Satellite-Based Continuous-Variable Quantum Communications: State-of-the-Art and a Predictive Outlook

Nedasadat Hosseinidehaj, Zunaira Babar, Robert Malaney, Soon Xin Ng, *Senior Member, IEEE,* and Lajos Hanzo, *Fellow, IEEE*

***Abstract*—The recent launch of the Micius quantum-enabled satellite heralds a major step forward for long-range quantum communication. Using single-photon discrete-variable quantum states, this exciting new development proves beyond any doubt that all of the quantum protocols previously deployed over limited ranges in terrestrial experiments can in fact be translated to global distances via the use of low-orbit satellites. In this paper we survey the imminent extension of space-based quantum communication to the continuous-variable regime—the quantum regime perhaps most closely related to classical wireless communications. The continuous variable regime offers the potential for increased communication performance, and represents the next major step forward for quantum communications and the development of the global quantum Internet.**

***Index Terms*—Quantum key distribution, free space optical, satellite communication, continuous variable quantum.**

I. Motivation and Introduction

MOORE'S Law has remained valid for half-a-century! As a result, contemporary semi-conductor technology is approaching nano-scale integration. Hence nano-technology is about to enter the realms of quantum physics, where many of the physical phenomena are rather different from those of classical physics. Hence this treatise contributes towards completing the 'quantum jig-saw puzzle' by paving the way from classical wireless systems to their perfectly secure quantum-communications counterparts, as heralded in [1] and [2].

- *The Inspiration:* In order to circumvent the specific limitations of the classical wireless systems detailed in [1], we set out to bridge the separate classical and quantum worlds into a joint universe, with the objective of contributing to perfectly secure quantum-aided communications for anyone, anywhere, anytime across the globe, as indicated by the stylized vision of the near-future quantum communications scenario seen in Fig. 1.
- *The Reality:* However, quantum processing is far from being flawless - it has substantial challenges, as detailed in this contribution. Nonetheless, at the time of writing long-range quantum communications via satellites has become a reality.

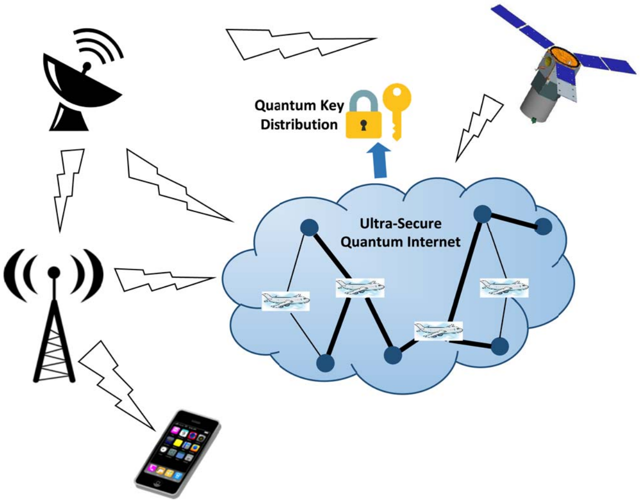


Fig. 1. Stylized vision of future global quantum communications unifying the separate classical and quantum systems into a joint secure universe for anyone, anywhere, anytime.

Amongst its numerous intriguing attributes, quantum communication has the potential to achieve secure communications at confidence levels simply unattainable in classical communications settings. This is due to the fact that quantum physics introduces a range of phenomena which have no counterpart in the classical domain, such as quantum entanglement and the superposition of quantum states.[1] The exploitation of such effects, both before and after the transmission of information in the quantum domain, can in effect lead to communications possessing 'unconditional' security.

Manuscript received December 27, 2017; revised June 22, 2018; accepted August 4, 2018. Date of publication August 20, 2018; date of current version February 22, 2019. This work was supported in part by EPSRC under Project EP/Noo4558/1 and Project EP/PO34284/1, and in part by the European Research Council's Advanced Fellow Grant QuantCom. *(Corresponding author: Lajos Hanzo.)*

N. Hosseinidehaj and R. Malaney are with the School of Electrical Engineering and Telecommunications, University of New South Wales, Sydney, NSW 2052, Australia.

Z. Babar, S. X. Ng, and L. Hanzo are with the School of Electronics and Computer Science, University of Southampton, Southampton SO17 1BJ, U.K. (e-mail: lh@ecs.soton.ac.uk).

Digital Object Identifier 10.1109/COMST.2018.2864557

[1] The superposition of a logical one and zero may be viewed as a coin spinning in a box, where we cannot claim to show its state being 'head' or 'tail'. When we stop spinning the coin, and lift the lid of the box, the superposition-based quantum state collapses back into the classical domain as a consequence of us observing it.

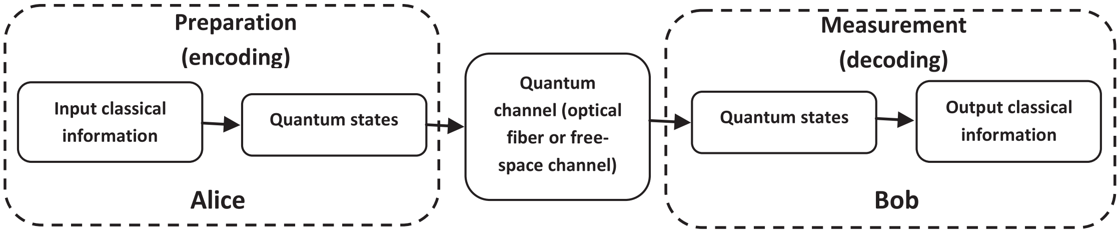

Preparation
(encoding)
Input classical information
Quantum states
Alice
Quantum channel (optical fiber or free-space channel)
Measurement
(decoding)
Quantum states
Output classical information
Bob

Fig. 2. Basic quantum communications schematic for transmitting classical information over a secure quantum channel. **Preparation**: Encoding classical information into quantum states. **Channel**: Secure quantum transmission using optical fiber or free space optical. **Measurement**: Decoding the received quantum states, yielding classical information.

Quantum communication entails the transfer of quantum states from one place to another via a quantum channel. In a generic form, quantum communication consists of three steps: (i) the preparation of quantum states - where the original classical information is encoded into quantum states; (ii) the transmission of the prepared quantum states over a quantum channel such as optical fiber or a free-space optical (FSO) channel - where the states are transmitted from a transmitter, held by Alice, to a receiver, named Bob; and (iii) detection - where the received states are decoded using quantum measurement resulting in some output classical information. A schematic including these three steps is shown in Fig. 2.

A key motivation for quantum communication of Fig. 2 is that the quantum information, mapped for example to the polarization of a photon, can be shared more securely than classical information. The well-known example of this is quantum key distribution (QKD) [3], whose unconditional security has been theoretically proved (classical cryptography schemes are not proved to be secure). We also note the close connection between quantum communication and quantum entanglement. A pair of quantum states are said to be entangled if, for example, changing the polarization of a photon results in an instantaneous polarization change for its entangled pair. Einstein referred to this as a 'spooky action at a distance.' Important quantum communication protocols utilizing entangled states include QKD, quantum teleportation [4]–[6], and entanglement swapping (teleportation of entanglement) [7].

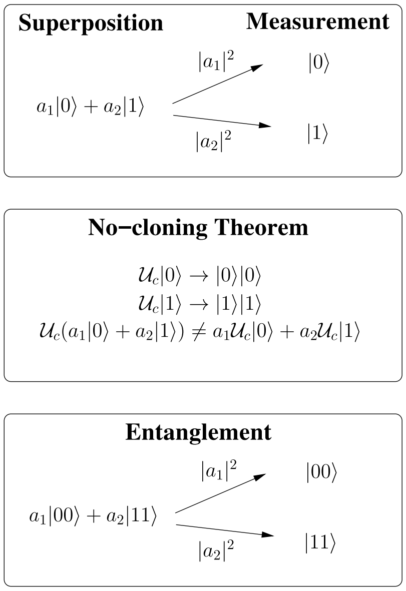

Superposition
Measurement
$a_1|0\rangle + a_2|1\rangle$
$|a_1|^2$
$|a_2|^2$
$|0\rangle$
$|1\rangle$
No−cloning Theorem
$\mathcal{U}_c|0\rangle \rightarrow |0\rangle|0\rangle$
$\mathcal{U}_c|1\rangle \rightarrow |1\rangle|1\rangle$
$\mathcal{U}_c(a_1|0\rangle + a_2|1\rangle) \neq a_1\mathcal{U}_c|0\rangle + a_2\mathcal{U}_c|1\rangle$
Entanglement
$a_1|00\rangle + a_2|11\rangle$
$|a_1|^2$
$|a_2|^2$
$|00\rangle$
$|11\rangle$

Fig. 3. Fundamental characteristics of qubits: (a) **Superposition & Measurement**: A qubit exists in superposition of the states $|0\rangle$ and $|1\rangle$. However, when measured, it collapses to the state $|0\rangle$ with a probability of $|a_1|^2$ and the state $|1\rangle$ with a probability of $|a_2|^2$. Hence, measurement of the qubit perturbs its coherent superposition. (b) **No-cloning Theorem**: An arbitrary quantum state cannot be cloned. Assume a hypothetical cloning operator $\mathcal{U}_c$, it is straightforward to show that cloning of a state $|\psi\rangle$ is not equivalent to cloning the constituent basis states, hence a quantum cloning operator $\mathcal{U}_c$ does not exist. (c) **Entanglement**: Qubits are said to be entangled, if measuring one qubit reveals information on the value of the other. In the example given, if the first qubit is found to be in the state $|0\rangle$ (or $|1\rangle$) upon measurement, then the second qubit also exists in the state $|0\rangle$ (or $|1\rangle$), hence a mysterious relation exists between the two entangled qubits.

In terms of representing the quantum states in quantum communications, discrete-variable (DV) and continuous-variable (CV) descriptions have been used [8], [9]. In the former, information is mapped to discrete features such as the polarization of single photons [3]. The detection of such features would then be realized by single-photon detectors. In DV technology information is mapped to two (or to a finite number of) basis states. The standard unit of DV quantum information in the two basis form is the quantum bit, also known as the 'qubit.' In a qubit, information is carried as a superposition of two orthogonal quantum states which can be represented mathematically as:

$$|\psi\rangle = a_1|0\rangle + a_2|1\rangle \tag{1}$$

with $|a_1|^2 + |a_2|^2 = 1$, where the complex numbers a_1 and a_2 can be considered as probability amplitudes. The notation $|.\rangle$ is used to indicate that the object is a vector.[2] Explicitly, the superimposed state of Eq. (1) implies that the qubit concurrently exists in the states $|0\rangle$ and $|1\rangle$. However, it collapses to one of the two states upon measurement. Fig. 3 summarizes the fundamental attributes of qubits, which makes quantum communication absolutely secure.

As an alternative approach, CV encoding has also been introduced [10], [11], and it is this type of encoding that forms the focus of this work. Such encoding is

[2] Note we have utilised the standard quantum mechanical notation for a vector in a vector space, i.e., $|\psi\rangle$, where ψ is a label for the vector (any label is valid). The entire object $|\psi\rangle$ is sometimes called a 'ket'. Note also that $\langle\psi|$ is called a 'bra' which is the Hermitian conjugate or adjoint of the ket $|\psi\rangle$. In quantum mechanics, bra-ket notation is a standard notation for describing quantum states.

more appropriate for quantum information carriers such as laser light. In CV technology, information is usually encoded onto the quadrature variables of the optical field [10]–[15], which constitute an infinite-dimensional Hilbert space. Detection of these variables is normally realized by high-efficiency homodyne (or heterodyne) detectors, which are capable of operating at a faster transmission rate than single-photon detectors [16]–[18]. The field's quadrature components (representing the quantum state) can be considered as related to the amplitude and phase of the laser light. Hence, CV states can be generated and detected using off-the-shelf state-of-the-art optical hardware [10]–[15]. In quantum mechanics, the quadrature components can also be considered as corresponding to the position and momentum of a harmonic oscillator.

There are generally three quantum communication scenarios, namely, the use of optical fibers, the use of terrestrial FSO channels, and the use of FSO channels to satellites. These scenarios are complementary and all may be expected to play a role in the emerging global quantum communication infrastructure. Fiber technology has the key advantage that once in place, an unperturbed channel from A to B exists. In fact, in fiber links the photon transfer is hardly affected by external conditions such as background light, the weather or other environmental obstructions. However, fiber suffers both from optical attenuation and polarization-preservation problems, which therefore limit its attainable distance to a few hundred kilometers [19]–[30]. These distance limitations may be overcome by the development of suitable quantum repeaters [31]. Losses in fiber are due to inherent random scattering processes, which increase exponentially with the fiber length. Explicitly, the transmissivity determining the fraction of energy received at the output of a fiber link of length L is given by $\tau = 10^{-\alpha_{\text{fiber}} L/10}$, where the value of α_{fiber} is highly dependent on the wavelength. Losses are minimised at the wavelength of 1550 nm, where for silicon fiber $\alpha_{\text{fiber}} \simeq 0.2$ dB/km.

Replacing the fiber channel with a FSO channel has the immediate advantage of lower losses [32]–[35], largely because the atmosphere provides for low absorption. The atmosphere also provides for almost unperturbed propagation of the polarization states. Additionally, FSO channels offer convenient flexibility in terms of infrastructure establishment, with links to moving objects also feasible [36]–[38]. However, terrestrial FSO quantum communications remain ultimately distance-limited, due to (amongst other issues) the curvature of the Earth, potential ground-dwelling line-of-sight (LoS) blockages, as well as atmospheric attenuation and turbulence.

FSO quantum communication via satellites [39]–[69] has the additional advantage that communications can still take place, even when there is no direct free-space LoS from A to B. That is, assuming that LoS paths from a satellite to two ground stations exist, satellite-based FSO communication can still proceed. The range of satellite-based communication is also potentially much larger than that allowed by direct terrestrial FSO connections, since the former circumvents the terrestrial horizon limit and there are lower photonic losses at high altitudes. In satellite-based FSO communications, only a small fraction of the propagation path (less than 10 km) is through the atmosphere - meaning most of the propagation path experiences no absorption and no turbulence-induced losses. The utilisation of satellites also allows for fundamental studies on the impact of relativity on quantum communications [39]. The key disadvantage of satellite-based quantum communications is, however, atmospheric turbulence-induced loss. The above discussions are summarized in Fig. 4.

The quantum communication system of Fig. 4 has given rise to new security paradigms. At the time of writing most of the classical cryptography schemes are based on the Rivest-Shamir-Adleman (RSA) protocol [70] in which the encryption key is public. These cryptography schemes are based on the concept of one-way functions, i.e., on functions which are easy to compute but extremely difficult to invert. Hence, the grade of security of these schemes cannot be irrevocably proved in principle. In fact, the security of these schemes is not unconditional, since they are based on certain computational power assumptions. Thus, if quantum computers were available today with a substantial amount of parallel computational power, RSA cryptography schemes could be broken. However, unconditional security is indeed possible using the so-called one-time pad scheme of [71], where a symmetric, random secret key is shared between the transmitter and receiver. To elaborate, in the one-time pad scheme, the transmitter (Alice) encodes the message by applying modulo addition between the plaintext bits and an equal number of random bits of the shared secret key. At the receiver, Bob decodes the received message by applying the same modulo addition between the received ciphertext and the shared secret key. If Alice and Bob never reuse their key, the one-time pad scheme of [71] cannot be broken, in principle. However, the main problem of this scheme is the generation of the secret key - a key which is as long as the message itself and must be used only once. This problem becomes severe, when a large amount of information has to be securely transmitted. Partially because of this limitation, public-key cryptography is more widely used than the one-time pad scheme. However, QKD, which is based on the laws of quantum physics, allows Alice and Bob to generate secret keys that can later be used to communicate with unconditional information-theoretic security, regardless of any future advances in computational power. Explicitly, the security of QKD is based on some of the fundamental principles of quantum physics. From an attacker's perspective, the ultimate goal is to have a perfect copy of the quantum state sent by Alice to Bob. However, it is impossible to acquire this owing to the no-cloning theorem mentioned in Fig. 3, which states that it is impossible to create an identical copy of an arbitrary unknown quantum state, while keeping the original quantum state intact [72], [73]. This simple, but crucial, observation can be traced back to the fact that quantum mechanics is a linear theory.

Fig. 5 shows the schematic of a QKD system, which can be divided into two main stages. Firstly, a quantum communication part where a pair of distant and trusted parties, Alice and Bob, generate two sets of correlated data through the transmission of a significant number of quantum states over an

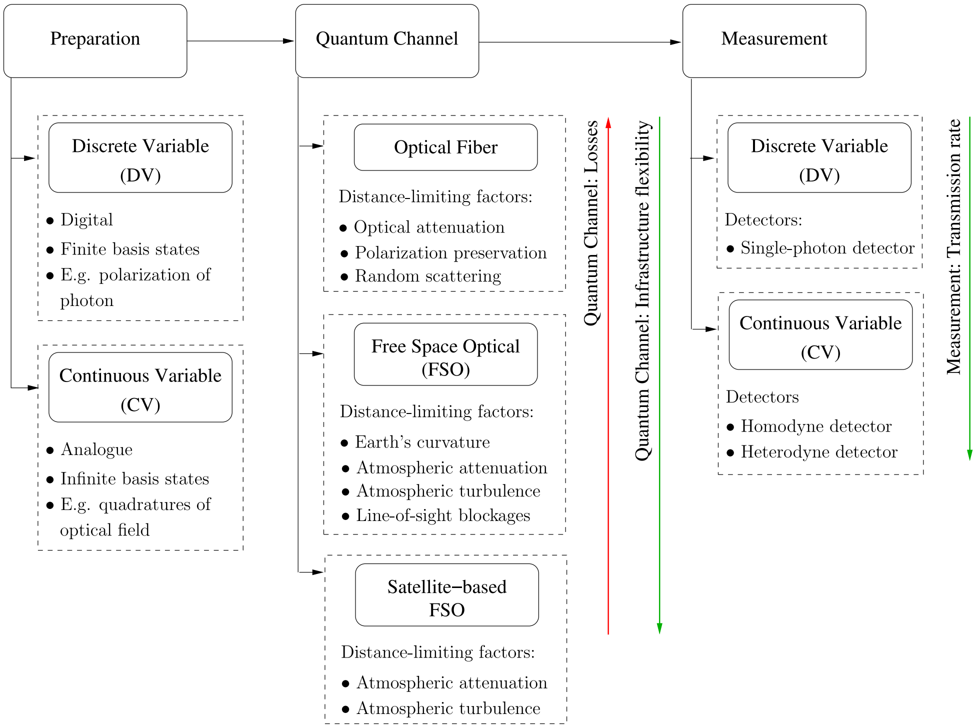


Fig. 4. Insights into the quantum communications system of Fig. 2.

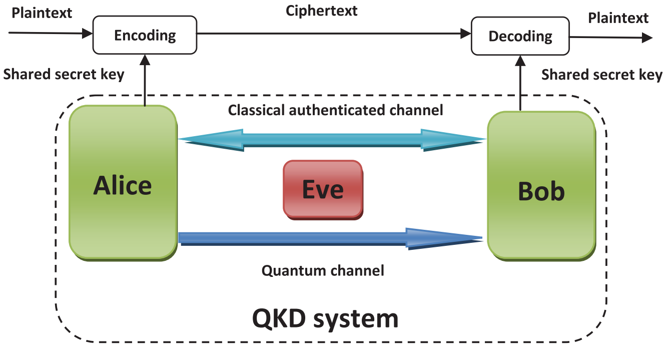


Fig. 5. A schematic of a QKD system: Alice and Bob are connected by a quantum channel, to which Eve has full access without any limitation (other than those constrained by the laws of physics). They are also connected by an authenticated classical channel, which Eve can only monitor. The final shared key between Alice and Bob, which is unconditionally secure, can then be used to transmit (encode and decode) secret messages.

insecure quantum channel.[3] Secondly, by the use of a classical post-processing protocol [74], [75] operated over a public but authenticated (meaning that the transferred data is known to be unaltered) classical channel, Alice and Bob extract from their correlated data a secret key that is unknown to a potential eavesdropper, Eve. The final key, which is unconditionally secure can then be used to transmit secret messages [76], [77]. Note that in QKD the quantum channel is open to any possible manipulation by Eve, which means that Eve has full access to the quantum channel without any computational (classical or quantum) limitation other than those imposed by the laws of quantum physics. However, Eve can only *monitor* the public classical channel, without *modifying* the messages (since the channel is authenticated).

In line with the quantum communication system of Fig. 4, there are two main techniques of implementing QKD, namely DV-QKD and CV-QKD. As the name implies, DV-QKD maps the key information to a single photon's phase or polarization [3], [78], [79], and invokes single-photon detectors. By contrast, CV-QKD maps the key information to the quadrature variables of the optical field and exploits homodyne (or heterodyne) detection [10]–[15], which can be implemented using off-the-shelf optical hardware. Hence, CV-QKD may be viewed as a specialized application of classic optical communications. More precisely, CV-QKD is one of the few quantum applications, which rely on state-of-the-art communications technology, hence ensuring a relatively smooth transition from the classical to the ultra-secure quantum regime. Motivated by this, we set out to survey and characterise the capabilities of CV quantum technology, in particular the family of satellite-based quantum communications solutions, which is essential for realizing our vision of the global quantum communications system encapsulated in Fig. 1. Since CV entanglement has been widely relied upon as a basic resource for CV-QKD [80], our survey is focused on satellite-based CV quantum communication in the context of CV entanglement distribution and its application to CV-QKD. A brief comparison of this survey to other published surveys on topics related to CV quantum communication is presented in Table I, which are mostly targeted towards the specialized quantum fraternity. By contrast, we have adopted a slow-paced tutorial approach for bridging

[3] The term 'insecure' here indicates the presence of an eavesdropper. However, please note that an eavesdropper cannot make a copy of the transmission, since quantum channel is intrinsically protected against copying owing to the no-cloning theorem. An eavesdropper can only 'listen to', or more specifically 'measure', the quantum information.

TABLE I
COMPARISON OF THIS STUDY WITH AVAILABLE SURVEYS

Approach	Satellite-based quantum communication	Atmospheric fading quantum channels	CV quantum systems	Quantum communication protocols	QKD			Gaussian CV quantum communication	Non-Gaussian CV quantum communication	CV quantum teleportation	CV entanglement swapping
					DV-QKD	CV-QKD	Security analysis				
Braunstein and van Loock [9]			✓	✓		✓		✓		✓	✓
Pirandola and Mancini [81], and Pirandola *et al* [82]			✓	✓				✓		✓	✓
Adesso and Illuminati [83]			✓					✓	✓		
Gisin and Thew [84]				✓	✓						
Scarani *et al* [76]			✓	✓	✓	✓	✓	✓			
Andersen *et al* [85]			✓	✓		✓		✓		✓	
Wang *et al* [86]			✓	✓		✓	✓	✓		✓	✓
Weedbrook *et al* [87]			✓	✓		✓	✓	✓		✓	
Lo *et al* [88], and Diamanti *et al* [89]			✓	✓	✓	✓					
Bedington *et al* [40]	✓			✓	✓						
This survey	✓	✓	✓	✓		✓	✓	✓	✓		✓

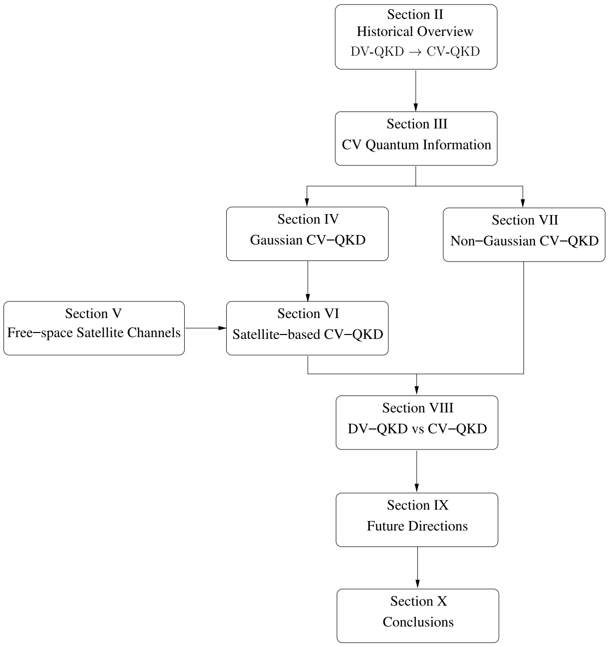


Fig. 6. Paper rationale.

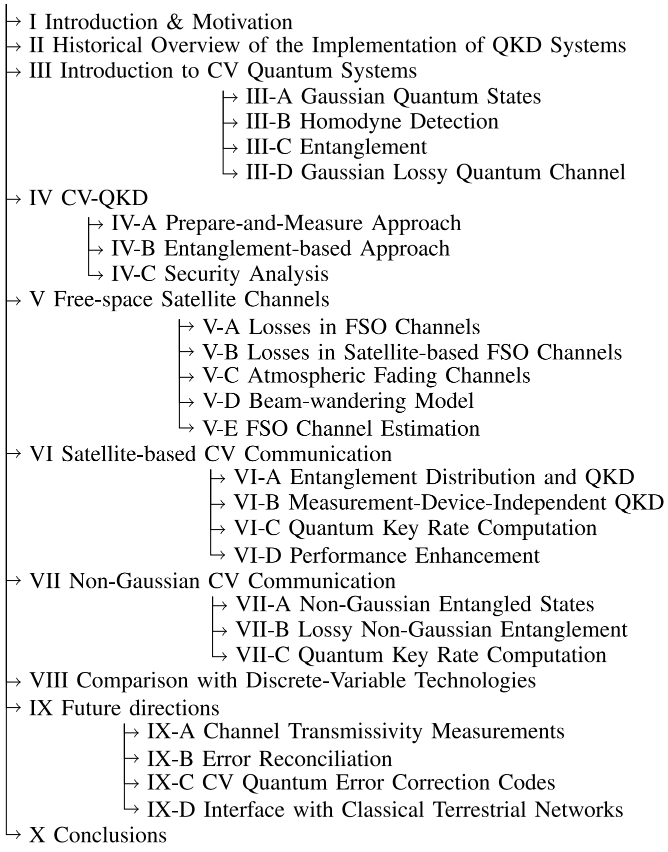
the classical as well as the quantum working groups. For the readers' convenience, the rationale of this paper is captured in Fig. 6, while a detailed paper outline is given in Fig. 7.

II. Historical Overview of the Implementation of Quantum Key Distribution Systems

In this section, we survey the major milestones achieved in the implementation of free-space QKD systems, which are chronologically arranged in Table II.

QKD constitutes the most studied quantum communication protocol, and has been deployed over both fiber and FSO channels. Indeed, the implementation of QKD over optical fibers has already been commercialised [90]–[92]. Terrestrial FSO quantum communications have been successfully deployed over very long distances [32]–[35]. In 2007, entanglement-based QKD and decoy-state QKD were realized over a 144 km FSO link between the Canary Islands of La Palma and Tenerife [78], [79], [93]. In addition to QKD, long-distance terrestrial FSO experiments have also been carried out to implement both entanglement distribution [93], [94] and quantum teleportation [95], [96]. The above long-distance FSO quantum communication experiments have been implemented at night. However, in a recent experiment FSO terrestrial QKD over 53 km has also been demonstrated during the day by choosing an appropriate wavelength, spectrum filtering and spatial filtering [97]. Nonetheless, in both fiber and FSO QKD implementations, the increasing levels of channel attenuation and noise tend to limit the maximum distance of successful key distribution to a few hundred kilometers.

A promising way of extending the deployment range of QKD is through the use of satellites. Indeed, it is widely anticipated that the reliance on satellites will assist in the expansion of quantum communication to global scales [39]–[69]. Full-scale verifications of satellite-based QKD have been reported in [36] (by demonstration of QKD between an aeroplane and a ground station), in [37] (by demonstration of QKD using a moving platform on a turntable, and a floating platform on a hot-air balloon), and in [38] (by demonstration of QKD from a stationary transmitter to a moving receiver platform traveling at an angular speed equivalent to a 600 km altitude satellite). Furthermore, several satellite-based quantum communication projects have been reported in [41]–[46]. In [47]–[49], a



- I Introduction & Motivation
- II Historical Overview of the Implementation of QKD Systems
- III Introduction to CV Quantum Systems
  - III-A Gaussian Quantum States
  - III-B Homodyne Detection
  - III-C Entanglement
  - III-D Gaussian Lossy Quantum Channel
- IV CV-QKD
  - IV-A Prepare-and-Measure Approach
  - IV-B Entanglement-based Approach
  - IV-C Security Analysis
- V Free-space Satellite Channels
  - V-A Losses in FSO Channels
  - V-B Losses in Satellite-based FSO Channels
  - V-C Atmospheric Fading Channels
  - V-D Beam-wandering Model
  - V-E FSO Channel Estimation
- VI Satellite-based CV Communication
  - VI-A Entanglement Distribution and QKD
  - VI-B Measurement-Device-Independent QKD
  - VI-C Quantum Key Rate Computation
  - VI-D Performance Enhancement
- VII Non-Gaussian CV Communication
  - VII-A Non-Gaussian Entangled States
  - VII-B Lossy Non-Gaussian Entanglement
  - VII-C Quantum Key Rate Computation
- VIII Comparison with Discrete-Variable Technologies
- IX Future directions
  - IX-A Channel Transmissivity Measurements
  - IX-B Error Reconciliation
  - IX-C CV Quantum Error Correction Codes
  - IX-D Interface with Classical Terrestrial Networks
- X Conclusions

Fig. 7. Paper structure.

satellite-to-ground single-photon downlink was simulated by reflecting weak laser (coherent) pulses (emitted by the ground-based station) off a low-Earth-orbit (LEO) satellite. In addition to experimental demonstrations, quantum communications with orbiting satellites have also been investigated by a growing number of feasibility studies [39], [50]–[61]. Recently, the in-orbit operation of a photon-pair source aboard a nano-satellite has been reported, which demonstrates photon-pair generation and polarization correlation under space conditions [64].

Quantum communication via satellites has very recently been given an enormous boost with the launch of the world's first quantum satellite, Micius, by China [66]. Building on the previously mentioned experiments, this new LEO satellite creates entangled photon pairs, sending them down to Earth for subsequent processing in a diverse range of communication scenarios. For example, using Micius, satellite-based distribution of entangled photon pairs in the downlink to two terrestrial locations separated by 1203 km has been demonstrated [67]. Quantum teleportation of single-photon qubits from a ground station to Micius through an uplink channel has also been demonstrated [68]. Extensions of this technology to significantly smaller satellites has just been reported for a Japanese micro-satellite and an optical ground station [65].

All of the previous FSO quantum communication systems referred to above have been focussed on DV technologies [32]–[69], [78], [79], [93]–[97]. They are based on single-photon technology and use single-photon detectors. Such detectors are impaired by background light, and involve spatial, spectral and/or temporal filtering in order to reduce this noise [97]. By contrast, in CV quantum communication, homodyne detection (in which the signal field is mixed with a strong coherent laser pulse, called the "local oscillator") is used for determining the field quadratures of light. Homodyne detectors offer better immunity to stray light [16], since the local oscillator is also capable of assisting in both spatial and spectral filtering. Also, such homodyne detectors are more efficient than single-photon detectors, since the p-i-n (PIN) photodiodes used in them offer higher quantum efficiencies than the avalanche photodiodes of single-photon detectors. Hence, CV-QKD can generally be considered to be more robust against background noise than DV-QKD.

In [16] and [98] the feasibility of a point-to-point CV-QKD (with coherent polarization states of light) has been demonstrated over a 100 m FSO link. In [99]–[101] the non-classical properties of CV quantum states propagating through the turbulent atmosphere have been analysed. Gaussian[4] entanglement distribution through a single point-to-point atmospheric channel and its applicability to CV-QKD have been studied in [102]. The entanglement properties of quantum states in the turbulent atmosphere have also been studied in [103] and [104]. Satellite-based CV quantum communication in the context of Gaussian and non-Gaussian entanglement distribution, and its application to CV-QKD, have been investigated in detail in [105]–[109]. The results presented in [105]–[109] apply for both a single point-to-point atmospheric channel, and in combined satellite-based atmospheric channels where the satellite acts as a relay. Recently, a point-to-point CV quantum communication experiment relying on the coherent polarization states of light has been established over a 1.6 km FSO link in an urban environment [110]. The distribution of polarization squeezed states[5] of light through an urban 1.6 km FSO link has also been demonstrated [111]. Recently, an experiment has been carried out relying on homodyne detection at a ground station of optical signals transmitted from a geostationary satellite [112]. This experiment is important in that it clearly demonstrates the feasibility and potential of satellite-based CV-QKD implementations.

III. Introduction to CV Quantum Systems

Any isolated physical system is associated to a Hilbert space, i.e., a complex vector space with inner product. The system is completely described by its state vector, which is a unit vector in the system's Hilbert space.

The simplest quantum mechanical system is a qubit, which has a two-dimensional Hilbert space. Supposing $|0\rangle$ and $|1\rangle$

[4] Gaussian quantum states are CV states with field quadratures exhibiting a Gaussian probability distribution.

[5] In quantum optics, there is an uncertainty relationship for the quadrature components of the light field, stating that the product of the uncertainties in both quadrature components is at least some quantity times Planck's constant. Hence, the uncertainty relationship dictates some lowest possible noise (i.e., uncertainty) amplitudes for the quadrature components of the light. In squeezed light, a further reduction in the noise amplitude of one quadrature component is carried out by squeezing the uncertainty region of that quadrature component, which is at the expense of an increased noise level in the other quadrature component.

TABLE II
MAJOR ACHIEVEMENTS IN THE IMPLEMENTATION OF FREE-SPACE QUANTUM COMMUNICATIONS

Discrete		**Continuous**
Free-space entanglement distribution over 7.8 km [33] and 13 km [32] in dense urban environment	**2005**	
10-hr long entanglement-based QKD demonstrated over 1.5 km [34]		
Entanglement-based QKD and decoy-state QKD realized over 144 km [78], [79], [93]		
Long-distance entanglement distribution using terrestrial FSO [93], [94]		Point-to-point CV-QKD over a 100 m FSO link [16], [98]
	2010	
Long-distance teleportation using terrestrial FSO [95], [96]		
Full-scale verification of satellite-based QKD [36]–[38]		
		Point-to-point CV quantum communication over a 1.6 km FSO link in urban environment [110], [111]
	2015	
Day-time FSO terrestrial QKD over 53 km [97], World's first quantum satellite Micius launched [66], Satellite-based entanglement distribution using Micius over 1203 km [67], Teleportation using Micius over 1400 km [68], quantum transmission using a 48-kg micro-satellite [65]		Homodyne detection using a geostationary satellite demonstrating the feasibility of satellite-based CV-QKD [112]

form an orthonormal[6] basis for this Hilbert space, an arbitrary state vector in the Hilbert space can be written as $|\psi\rangle = a_1|0\rangle + a_2|1\rangle$, where a_1 and a_2 are complex numbers. The normalization condition for state vectors (or the condition that $|\psi\rangle$ be a unit vector), $\langle\psi|\psi\rangle = 1$, is equivalent to $|a_1|^2 + |a_1|^2 = 1$.[7] When we measure a qubit in the basis $\{|0\rangle, |1\rangle\}$ we obtain either the result $|0\rangle$, with probability $|a_1|^2$, or the result $|1\rangle$, with probability $|a_2|^2$.

Now we can extend a two-dimensional Hilbert state to an arbitrary-dimensional Hilbert state (even infinite-dimensional). A quantum state with finite-dimensional Hilbert space is called discrete-variable quantum state, and a quantum state with infinite-dimensional Hilbert space is called continuous-variable quantum state. In an arbitrary-dimensional Hilbert space the arbitrary quantum state $|\psi\rangle$ can be expanded in an arbitrary orthonormal basis as $|\psi\rangle = \sum_i \psi_i|v_i\rangle$, where the complex number ψ_i is $\psi_i = \langle v_i|\psi\rangle$. By definition the basis is complete (i.e., $\sum_j |v_j\rangle\langle v_j| = I$, with *I* the identity operator) and orthonormal (i.e., $\langle v_i|v_j\rangle = \delta_{ij}$).

Now let us consider the quantum measurement of an arbitrary quantum state $|\psi\rangle$. Quantum measurements are described by operators[8] $\hat{M}_m$, where the index *m* refers to the measurement result. Note that the measurement operators satisfy the completeness equation $\sum_m \hat{M}_m^\dagger \hat{M}_m = I$. Considering the initial quantum state $|\psi\rangle$, the probability that outcome *m* occurs as a result of the quantum measurement $\hat{M}_m$ upon the state $|\psi\rangle$ is given by $p_m = \langle\psi|\hat{M}_m^\dagger \hat{M}_m|\psi\rangle$, and the state of the system after the measurement collapses onto $\frac{1}{\sqrt{p_m}}\hat{M}_m|\psi\rangle$. Due to the completeness of the measurement operators we have $\sum_m p_m = 1$.

A projective measurement is described by an observable $\hat{M}$. Each observable quantity is associated with a Hermitian operator whose eigenvalues correspond to the possible values of the observable. The observable has a spectral decomposition $\hat{M} = \sum_m \lambda_m \hat{P}_m$, where $\hat{P}_m = |u_m\rangle\langle u_m|$. The vectors $|u_m\rangle$ are the orthonormal set of eigenvectors of the observable $\hat{M}$ with real-valued eigenvalues λ_m which satisfy $\sum_m |u_m\rangle\langle u_m| = I$. The probability for obtaining the measurement result λ_m upon measuring the state $|\psi\rangle$ is given by $p_m = |\langle u_m|\psi\rangle|^2$. Hence, the probability p_m is determined by the size of the component of $|\psi\rangle$ in direction of the eigenvector $|u_m\rangle$. When the measurement result λ_m is obtained, the quantum state $|\psi\rangle$ collapses onto $\frac{1}{\sqrt{p_m}}\hat{P}_m|\psi\rangle$.

One form of a CV quantum system is that represented by *N* bosonic modes, such as those corresponding to *N* quantized radiation modes of the electromagnetic field [9], [83], [85]–[87], [113], [114]. A single photon has four degrees of freedom, helicity (polarization) and the three components of the momentum vector. In principle, quantum information can be encoded into any one of these degrees of freedom. A single 'mode' of an electromagnetic field refers to a specific combination of these photonic degrees of freedom. In many circumstances different modes can be simply represented by different frequencies (since frequency is related to momentum). For a beam of photons, the *number* of photons in the beam constitutes another means to encode quantum information. Quantum information encoded into the quadratures of the electromagnetic field (formally defined below) are related to an encoding in this additional degree of freedom. Since the quadrature operators have continuous spectra, we can describe the values of such operators as CV variables.

A single mode of a CV system can be described as a single quantum harmonic oscillator of a specific frequency, where the electric and magnetic fields play the 'roles' of the position and momentum [115]. It will be useful to further illustrate this concept. Consider the case of a single-frequency radiation field confined to a one-dimensional cavity with walls that are perfectly conducting. Assume the *z*-axis is parallel to the length of the cavity and the cavity walls are located at $z = 0$ and $z = L$. The electric field within the cavity will form a standing wave. Without loss of generality, we can take the electric field to be polarized perpendicular to the *z*-axis, and in the positive *x*-direction (we take the *x* and *z* coordinates to

[6] A set of vectors $|i\rangle$ is orthonormal if each vector is a unit vector, and distinct vectors are orthogonal, i.e., $\langle i|j\rangle = \delta_{ij}$, where δ_{ij} is the Kronecker delta function.

[7] Note that the overlap $\langle\varphi|\psi\rangle$ indicates the inner product between the vectors $|\psi\rangle$ and $\langle\varphi|$ (the adjoint of the vector $|\varphi\rangle$) in the Hilbert space.

[8] The operator serves as a linear function which acts on the states of the system. While quantum states correspond to vectors in a Hilbert space, operators can be regarded as matrices.

be in same plane and the *y* plane perpendicular to the *x* plane). In terms of the distance vector *r* and time *t*, the electric field can then be written as $E(r,t) = e_x E_x(z,t)$, where e_x is a unit-length polarization vector. Given our boundary conditions, and assuming a radiation source-free cavity, the electric field satisfying Maxwell's equations can be written as [115]

$$E_x(z,t) = \sqrt{\left(\frac{2\omega^2}{V_o \varepsilon_0}\right)} \quad q(t)\sin(kz), \tag{2}$$

where $k = \omega/c$ is the wave number (ω is the frequency of the mode and *c* is the speed of light in vacuum), ε_0 is the vacuum permittivity, *q*(*t*) is a time-dependent factor having the dimension of length (meters), and V_o is the effective volume of the cavity.[9] For the present purposes we will assume the frequency is one of those allowed by the boundary conditions, namely, $\omega_n = c(n\pi/L)$, where $n = 1, 2, \ldots$.

Similarly, the magnetic field can be written $B(r,t) = e_y B_y(z,t)$, where e_y is a unit-length polarization vector, and [115]

$$B_y(z,t) = \frac{\mu_0 \varepsilon_0}{k}\sqrt{\left(\frac{2\omega^2}{V_o \varepsilon_0}\right)}\ p(t)\cos(kz). \tag{3}$$

Here $p(t) = \dot{q}(t)$, where the dot denotes the time derivative, and μ_0 is the vacuum permeability. Based on these equations it is then straightforward to show that the Hamiltonian, H_o, of the electromagnetic field can be written as [115]

$$H_o = \frac{1}{2}\int dV_o \left(\varepsilon_0 E_x^2(z,t) + \frac{1}{\mu_0}B_y^2(z,t)\right). \tag{4}$$

Substituting $E_x(z,t)$ and $B_y(z,t)$ in H_o from Eq. (2) and Eq. (3) respectively and exploiting that $\sin^2(\frac{\omega}{c}z) + \cos^2(\frac{\omega}{c}z) = 1$ the Hamiltonian of the single-mode electromagnetic field can be written as

$$H_o = \frac{1}{2}\left(p^2 + (\omega q)^2\right). \tag{5}$$

This equation can be compared with the Hamiltonian of the classical harmonic oscillator for a particle of mass *m* viz., $H_o = \frac{1}{2}(p^2/m + (m\omega q)^2)$, where we have taken the generalised coordinate $q = x$ and set $p = m\dot{x}$, *x* being the position. Comparing these two Hamiltonians, it can be seen that a single-mode electromagnetic field is formally equivalent to a harmonic oscillator of unity mass, where the electric and magnetic fields play roles similar to that of the position and momentum of a particle.[10]

In quantum systems we replace variables, such as *q*, *p*, *E*, *B* and *H* of the classical system, by their corresponding operator[11] equivalents, e.g., $\hat{q}$, $\hat{p}$, $\hat{E}$, $\hat{B}$ and $\hat{H}$. Then the Hamiltonian of the single-mode electromagnetic field becomes $\hat{H}_o = \frac{1}{2}(\hat{p}^2 + (\omega\hat{q})^2)$. As such, we can now see how a single mode of a CV system can indeed be described as a single quantum harmonic oscillator. Furthermore, note that the operators $\hat{q}$ and $\hat{p}$ are Hermitian (or self-adjoint). In quantum physics Hermitian operators correspond to observable quantities, where an observable is an operator that corresponds to a physical quantity, such as position or momentum, that can be measured.

However, it will be useful to introduce non-Hermitian operators $\hat{a}$ (the annihilation operator) and $\hat{a}^\dagger$ (the creation operator). These can be written as,

$$\hat{a} = (2\hbar\omega)^{(-1/2)}(\omega\hat{q} + i\hat{p}), \tag{6}$$

$$\hat{a}^\dagger = (2\hbar\omega)^{(-1/2)}(\omega\hat{q} - i\hat{p}), \tag{7}$$

where $\hbar = h/2\pi$, with *h* being Planck's constant. These bosonic field operators satisfy the commutation relation $[\hat{a}, \hat{a}^\dagger] = 1$, where the commutator between two operators $\hat{x}$ and $\hat{y}$ is defined to be $[\hat{x}, \hat{y}] = \hat{x}\hat{y} - \hat{y}\hat{x}$. Note that since the annihilation and creation operators are non-Hermitian, they correspond to *non-observable* quantities.

It can be easily shown that our new non-Hermitian operators have a time dependence, under free evolution, which can be expressed as $\hat{a} = \hat{a}(0)\exp(-i\omega t)$ and $\hat{a}^\dagger = \hat{a}^\dagger(0)\exp(i\omega t)$. As such, the electric field operator can then be re-written as

$$\hat{E}_x(z,t) = \sqrt{\left(\frac{\hbar\omega}{V_0\varepsilon_0}\right)}\sin(kz)\Big[\hat{a}\exp(-i\omega t) + \hat{a}^\dagger\exp(i\omega t)\Big]. \tag{8}$$

Removing the time dependence in the creation and annihilation operators by re-setting $\hat{a} = \hat{a}(0)$ and $\hat{a}^\dagger = \hat{a}^\dagger(0)$, we can in turn define the *quadrature operators* (see later discussion on the freedom to choose the specific form of these)

$$\hat{X}_1 = \frac{1}{2}\left(\hat{a} + \hat{a}^\dagger\right), \tag{9}$$

$$\hat{X}_2 = \frac{1}{2i}\left(\hat{a} - \hat{a}^\dagger\right). \tag{10}$$

In terms of the quadrature operators we can then re-write $\hat{E}_x(z,t)$ as

$$\hat{E}_x(z,t) = 2\sqrt{\left(\frac{\hbar\omega}{V_0\varepsilon_0}\right)}\sin(kz)\Big[\hat{X}_1\cos(\omega t) + \hat{X}_2\sin(\omega t)\Big]. \tag{11}$$

As such, we can see that the quadratures $\hat{X}_1$ and $\hat{X}_2$ can be considered as the amplitudes of the electric field's time-dependent cos and sin components, respectively. Clearly, these components are 90° out of phase with each other - hence the name, quadratures. The quadratures satisfy the commutation relation $[\hat{X}_1, \hat{X}_2] = i/2$.[12]

A CV system of *N* modes follows a similar description to that we have just given for a single mode, except of course the Hilbert space containing the multimode system is larger. The *N*-mode system may be described by a Hilbert space given by the tensor product $\mathcal{H} = \otimes_{k=1}^{N}\mathcal{H}_k$, where $\mathcal{H}_k$ is a single-mode Hilbert space associated with the *k*-th mode. The

[9] To apply this formalism to the free field we calculate the physical observables we are interested in and then simply take the limit $V_0 \to \infty$.

[10] We emphasize that the terms 'position' and 'momentum' here simply refer to the similar roles played by the field quadratures and position and momentum of a particle - e.g., the 'position quadrature' does not in any manner refer to the position of a photon.

[11] Note that operators can be regarded as matrices. In fact, the operator and matrix viewpoints turn out to be completely equivalent [8].

[12] This can be derived from the constraint imposed by quantum mechanics that $[\hat{q}, \hat{p}] = i\hbar$. Note, that in contrast to classical physics where any two observables commute, i.e., their commutator is zero (which means it is possible to know precisely the value of both observables at the same time), in quantum mechanics the quadrature observables of the electromagnetic field do not commute.

creation and annihilation operators for each mode then satisfy the commutation relationships

$$[\hat{a}_k, \hat{a}_{k'}] = \left[\hat{a}_k^\dagger, \hat{a}_{k'}^\dagger\right] = 0, \quad \left[\hat{a}_k, \hat{a}_{k'}^\dagger\right] = \delta_{kk'}, \qquad (12)$$

where $\delta_{kk'}$ is the Kronecker delta function.

Consider again the single-mode Hilbert space $\mathcal{H}_k$. This is spanned by the Fock, or number-state basis, $\{|n\rangle_k\}_{n=0}^{\infty}$, where the Fock state $|n\rangle_k$ is the eigenstate of the number operator $\hat{n}_k = \hat{a}_k^\dagger \hat{a}_k$, i.e., $\hat{n}_k|n\rangle_k = n|n\rangle_k$. Put simply, $|n\rangle_k$ represents the state of the electromagnetic field containing exactly *n* photons (quanta) of frequency ω_k. Note that for each mode *k* there exists a *vacuum* state which contains *no* quanta of the field, namely, $|0\rangle_k$, satisfying $\hat{a}_k|0\rangle_k = 0$. The action of the bosonic field operators over the Fock states is given by [9], [87]

$$\hat{a}_k|n\rangle_k = \sqrt{n}|n-1\rangle_k, \quad \hat{a}_k^\dagger|n\rangle_k = \sqrt{n+1}|n+1\rangle_k. \quad (13)$$

Having now formally defined the vacuum state, it is probably useful to note for the unwary that some *apparent* inconsistency lies lurking in the literature (including the many references of this work). This applies to both the constant value applied to $\hbar$, as well as the nomenclature itself. We note that our quadrature operators, as defined thus far, can be used to form $\hat{q} = \sqrt{2\hbar/\omega}\hat{X}_1$ and $\hat{p} = \sqrt{2\hbar\omega}\hat{X}_2$; from which we can easily show consistency with $[\hat{q}, \hat{p}] = i\hbar$. In many works we will find that $\hat{q}$ and $\hat{p}$ written in this form (and also in 'dimensionless' form with, say, $\hbar = \omega = 1$) are also referred to as the 'quadratures.' Also, in many works the cofactor of 1/2 in front of our definitions of $\hat{X}_1$ and $\hat{X}_2$ is replaced by some other constant, e.g., $1/\sqrt{2}$ or 1-allowable re-definitions of course. It is straightforward to determine the vacuum expectation value for any well-defined operator (or function of that operator), e.g., $\langle 0|\hat{X}_1^2|0\rangle = 1/4$, and $\langle 0|\hat{q}^2|0\rangle = \hbar/(2\omega)$. It is common to set $\hbar$ to some numerical constant, usually 1/2, 1 or 2. However, no consistency exists in the literature on this either. Setting $\hbar = 2$ has the convenience of setting the vacuum-state variance of the $\hat{q}$ and $\hat{p}$ operators to 1 (when ω is set to unity).[13]

Bearing in mind the above discussion of inconsistency in nomenclature, we adopt henceforth that $\hbar = 2$ and $\omega = 1$ (unless stipulated otherwise). We also redefine the 'quadrature' operators to be $\hat{q}_k$ and $\hat{p}_k$, now given by the simpler form $\hat{q}_k = \hat{a}_k + \hat{a}_k^\dagger$ and $\hat{p}_k = i(\hat{a}_k^\dagger - \hat{a}_k)$. This will make the notation to follow less cluttered.

Defining the vector of quadrature operators for *N* modes as $\hat{R} = (\hat{q}_1, \hat{p}_1, \ldots, \hat{q}_N, \hat{p}_N)$, the commutation relationship between the quadrature operators can be written as $[\hat{R}_i, \hat{R}_j] = 2i\Omega_{ij}$, where $\hat{R}_i$ ($\hat{R}_j$) is the *i*-th (*j*-th) element of the vector $\hat{R}$, and Ω_{ij} is the element of the matrix

$$\mathbf{\Omega} = \bigoplus_{k=1}^{N} \mathbf{\Omega}_0, \ \mathbf{\Omega}_0 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \qquad (14)$$

Since a Hermitian operator has an orthogonal set of eigenvectors with real-valued eigenvalues, the quadrature operator $\hat{q}$ ($\hat{p}$) (which is Hermitian) is an observable with continuous eigenspectra, i.e., $\hat{q}|q\rangle = q|q\rangle$ ($\hat{p}|p\rangle = p|p\rangle$), with orthogonal eigenvectors or eigenstates $|q\rangle$ ($|p\rangle$) having continuous eigenvalues $q \in \mathbb{R}$ ($p \in \mathbb{R}$). Note that the two sets of eigenstates $|q\rangle$ and $|p\rangle$ identify two different bases (i.e., two different sets of orthogonal and complete eigenstates), and each set constitutes a common basis for CV quantum information. A CV quantum state can be defined as a continuous-valued superposition of the field's eigenstates.

All the physical information about a quantum system is contained in its quantum state, represented by a density operator $\hat{\rho}$, which is a trace-one positive operator. A pure quantum state (i.e., the state of an isolated physical system which does not have any interaction with the environment) is described by a unit vector $|\psi\rangle$ in Hilbert space, and its density operator is given by $\hat{\rho} = |\psi\rangle\langle\psi|$.

Unlike pure states, mixed states cannot be described by a single vector in the Hilbert space, because the knowledge about the state preparation is incomplete. In fact, a mixed state is a statistical mixture of pure states, and is described by its associated density operator. The density operator describing a mixed state is in the form of $\hat{\rho} = \sum_i p_i|\psi_i\rangle\langle\psi_i|$, where the pure quantum state $|\psi_i\rangle$ in which the system is prepared occurs with probability p_i. A quantum state $\hat{\rho}$ is said to be a pure state, when we have $\hat{\rho}^2 = \hat{\rho}$. In fact, for pure states we have $\mathrm{Tr}(\hat{\rho}^2) = 1$, and for mixed states we have $\mathrm{Tr}(\hat{\rho}^2) < 1$, where Tr denotes trace.

For a general mixed quantum state $\hat{\rho} = \sum_i p_i|\psi_i\rangle\langle\psi_i|$ the mean value of the observable $\hat{M}$ is given by $\langle\hat{M}\rangle = \sum_i p_i\langle\psi_i|\hat{M}|\psi_i\rangle = \mathrm{Tr}(\hat{\rho}\hat{M})$, where $\langle . \rangle$ denotes the mean value, and the variance of the observable $\hat{M}$ is given by $V(\hat{M}) = \langle\hat{M}^2\rangle - \langle\hat{M}\rangle^2$, where $V(.)$ is the variance. Note that the fluctuations in the quadrature operators (i.e., $\hat{q}$ and $\hat{p}$) of the electromagnetic field can be characterized by the variance of these observables, or by the standard deviation (i.e., the square root of the variance) of these observables denoted by $\Delta(.)$, which is sometimes referred to as the uncertainty of the quadrature operators. Note also that for non-commuting operators $\hat{A}$ and $\hat{B}$ where $[\hat{A}, \hat{B}] = \hat{C}$, we have $\Delta(\hat{A})\Delta(\hat{B}) \geq \frac{1}{2}|\langle\hat{C}\rangle|$. Since the quadrature operators of the electromagnetic field do not commute ($[\hat{q}, \hat{p}] = i\hbar$), there exists an uncertainty relation for the uncertainty of the quadrature operators, called the Heisenberg uncertainty principle. In a *N*-mode CV system the Heisenberg uncertainty principle is defined for the quadrature operators of each mode *k*, and is given by $V(\hat{q}_k)V(\hat{p}_k) \geq 1$ (recall again $\hbar = 2$). According to the uncertainty principle if we prepare a large number of quantum systems in identical states, and then measure the quadrature $\hat{q}$ of some of those states, and measure the quadrature $\hat{p}$ of others, then the variance of the $\hat{q}$ results times the variance of the $\hat{p}$ is at least one. Note again, that the quadrature variance of the vacuum state of a single mode is one, i.e., we have $V(\hat{q}) = V(\hat{p}) = 1$, which is the lowest possible variance reachable symmetrically by the $\hat{q}$ and $\hat{p}$ quadratures according to the uncertainty relationship.

A quantum state $\hat{\rho}$ of a *N*-mode CV system can also be described in terms of a characteristic function $\chi_c(\xi) = \mathrm{Tr}(\hat{\rho}\hat{\mathrm{D}}(\xi))$, where $\hat{D}(\xi) = \exp(i\hat{R}\mathbf{\Omega}\xi)$ is the Weyl operator [9], [87], and $\xi \in \mathbb{R}^{2N}$. The quantum state $\hat{\rho}$ can also be

[13] Note the variance of $\hat{q}$ in the vacuum state is just $\langle 0|\hat{q}^2|0\rangle$ since the vacuum expectation of $\hat{q}$ is zero (variance $= \langle 0|\hat{q}^2|0\rangle - \langle 0|\hat{q}|0\rangle^2$). Similar is the case for $\hat{p}$.

described in terms of a Wigner function (quasi-probability distribution), which is given by the Fourier transform of the characteristic function χ_c as [9], [87]

$$W(R) = \int_{\mathbb{R}^{2N}} \frac{d^{2N}\xi}{(2\pi)^{2N}} \exp(-iR\boldsymbol{\Omega}\xi)\chi_c(\xi), \tag{15}$$

where $R = (q_1, p_1, \ldots, q_N, p_N)$ is the vector of quadrature variables, with the real-valued variables q and p being the eigenvalues of the quadrature operators. Note that for a single-mode quantum state the probability distribution of a quadrature measurement (marginal distribution) is obtained from the Wigner function of the quantum state by integration over the conjugate quadrature.

The CV quantum states can be visualized using their Wigner function in a phase-space representation, where the axes are defined by a pair of conjugate quadrature variables q and p. In such a phase space, a classical optical field is represented by a single point corresponding to its complex-valued field amplitude. However, the quantum states of light cannot be represented by a single point, since conjugate quadrature variables cannot be measured simultaneously with arbitrary precision due to the Heisenberg uncertainty relationship. Hence the Wigner function is utilized to represent the quantum states in the phase space [9], [85]–[87].

A. Gaussian Quantum States

Gaussian quantum states (for a detailed review, see [86], [87], [114]) are completely characterized by the first moment (or the mean value) of the quadrature operators $\langle \hat{R} \rangle$ and a covariance matrix $\boldsymbol{M}$, i.e., a matrix of the second moments of the quadrature operators defined as

$$M_{ij} = \frac{1}{2}\langle \hat{R}_i\hat{R}_j + \hat{R}_j\hat{R}_i \rangle - \langle \hat{R}_i \rangle \langle \hat{R}_j \rangle. \tag{16}$$

The covariance matrix of a N-mode quantum state is a ($2N \times 2N$) real symmetric matrix, which must satisfy the uncertainty principle, *viz.*, $\boldsymbol{M} + i\boldsymbol{\Omega} \geq 0$. By definition, a Gaussian state having N modes is a CV state whose Wigner function is a Gaussian distribution of the quadrature variables given by

$$W(R) = \frac{\exp\Big(-\frac{1}{2}(R - \langle R \rangle)\, \boldsymbol{M}^{-1}\, (R - \langle R \rangle)^T\Big)}{(2\pi)^N \sqrt{\det(\boldsymbol{M})}}. \tag{17}$$

Some important examples of Gaussian states are vacuum states [9], [86], [87], [115], coherent states [9], [86], [87], [115], thermal states [9], [86], [87], [115] and squeezed states [9], [86], [87], [115]. We discuss some of these Gaussian states further.

1) Vacuum State: The Wigner function of the vacuum state with respect to the conjugate quadrature variables q and p is shown in Fig. 8(a), in which the Wigner function is centered at (0, 0), which means that the vacuum state has a zero mean. The covariance matrix of the vacuum state is the identity matrix, which means that a vacuum state has a symmetric distribution of the quadrature components (see Fig. 8(a)) with both the quadrature components having noise variance of one. This noise is usually termed the vacuum noise or quantum shot noise.

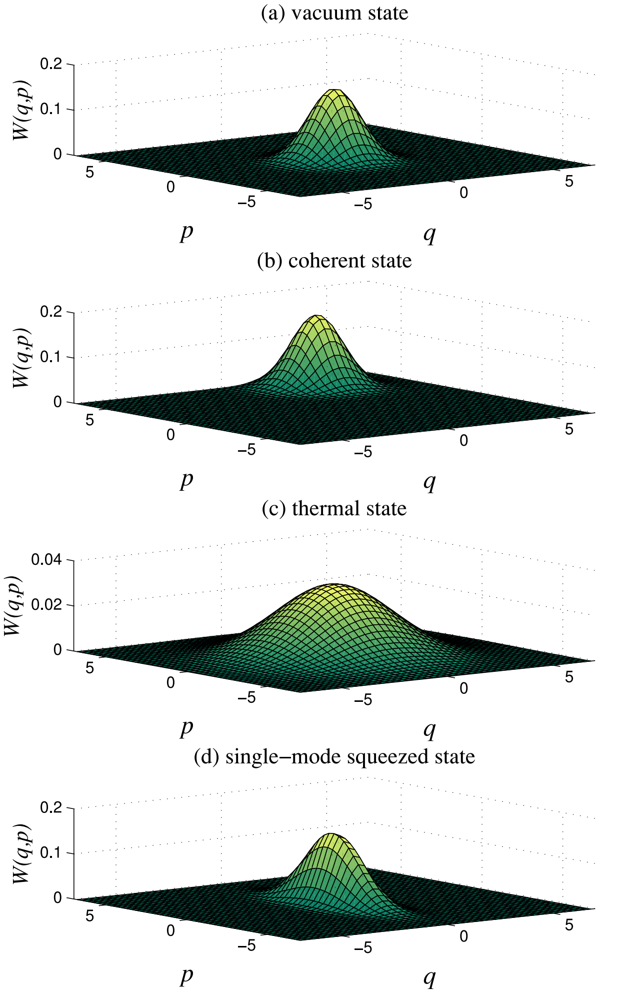
2) Coherent State: A coherent state is generated by applying the displacement operator $\hat{D}$ to the vacuum state formulated as $|\alpha\rangle = \hat{D}(\alpha)|0\rangle$, where $\hat{D}(\alpha) = \exp(\alpha\hat{a}^\dagger - \alpha^*\hat{a})$ is the displacement operator and $\alpha = (q + ip)/2$ is the complex amplitude. Since the displacement operator does not change the variance of the quadratures, coherent states - similarly to vacuum states - exhibit the lowest possible variance reachable symmetrically by the $\hat{q}$ and $\hat{p}$ quadratures. The coherent state is the eigenstate of the annihilation operator, which is formulated as $\hat{a}|\alpha\rangle = \alpha|\alpha\rangle$. To elaborate a little further, this state has a mean value of $\langle \hat{R} \rangle = (q, p)$, and the covariance matrix is equal to the identity matrix, which means that a coherent state has a symmetric distribution of the quadrature components with both the quadrature components having noise variance equal to one. This symmetric distribution can be seen in Fig. 8(b), where the Wigner function of the coherent state with a mean value of (3, 5) (which is the centre of the Wigner function) is shown with respect to the conjugate quadrature variables q and p. Note that coherent states are much easier to generate in the laboratory than any other Gaussian state. For example, the laser field is in a coherent state. As an important application in the context of quantum communication, coherent states are used to distribute secret keys in Gaussian CV-QKD protocols [13], [14], [116], [117].

3) Thermal State: Thermal states can be described as a mixture of coherent states. The thermal state has a zero mean and a covariance matrix $\boldsymbol{M_{th}} = v_t\boldsymbol{I}$ associated with $v_t = 2\bar{n} + 1$, where v_t is the noise variance of each quadrature component, $\bar{n}$ >0 is the average number of photons and $\boldsymbol{I}$ is the (2×2)-element identity matrix. This form of the covariance matrix means that a thermal state has a symmetric distribution of the quadrature components, which can be seen in Fig. 8(c) where the Wigner function of the thermal state with $v_t = 5$ is shown with respect to the conjugate quadrature variables q and p. Note that in the generic form of quantum communication the quantum noise of the channel is in a thermal state, called thermal noise.

4) Single-Mode Squeezed Vacuum State: According to the Heisenberg uncertainty relationship, the lowest possible variance reachable symmetrically by the $\hat{q}$ and $\hat{p}$ quadratures is one, i.e., the noise variance of the vacuum state. A reduction in the variance of the $\hat{q}$ (or $\hat{p}$) quadrature below the vacuum noise is possible by *squeezing*. In squeezing, the variance of one continuous variable is in fact decreased below the vacuum noise, while the variance of the conjugate variable is increased. For instance, in a $\hat{q}$-squeezed light, the variance of the $\hat{q}$ quadrature is reduced below the vacuum noise, while the variance of the $\hat{p}$ quadrature is increased above the vacuum noise. A single-mode squeezed vacuum state is generated by applying the single-mode squeezing operator of $\hat{S}_s(r_s) = \exp[r_s(\hat{a}^2 - \hat{a}^{\dagger 2})/2]$ [9], [86], [87], [115] to the vacuum state, where $r_s \in [0, \infty)$ represents the single-mode squeezing parameter.[14] Such a squeezed state has zero mean and a covariance matrix of $\boldsymbol{M} = diag[\exp(-2r_s), \exp(2r_s)]$

[14] Note, in general, squeezing parameters are complex numbers. For simplicity (and to be consistent with most of the literature) we limit them here to real numbers.

when the quantum fluctuations of the $\hat{q}$ quadrature have been squeezed. In this case for the single-mode squeezing represented by $r_s > 0$ we have $V(\hat{q}) < 1$ and $V(\hat{p}) > 1$. This means that a single-mode squeezed state does not have a symmetric distribution of the quadrature components, since the variance of one of the quadratures is reduced by squeezing at the expense of an increase in the variance of the conjugate quadrature by the counterpart operation of anti-squeezing. Note, the state still obeys the Heisenberg uncertainty relationship. Such an asymmetric distribution of quadrature components can be seen in Fig. 8(d), where the Wigner function of the single-mode squeezed vacuum state with $r_s = 0.5$ is shown. Here, the $\hat{q}$ quadrature is squeezed. In terms of applications in quantum communications, single-mode squeezed vacuum states are also utilized to distribute secret keys in Gaussian CV-QKD protocols [12], [118]. Note that for $r_s = 0$, the single-mode squeezed state corresponds to the vacuum state.


(a) vacuum state

(b) coherent state

(c) thermal state

(d) single−mode squeezed state

Fig. 8. The Wigner function of the important single-mode Gaussian states including vacuum state, coherent state with a mean value of (3, 5), thermal state with $v_t = 5$, and single-mode squeezed vacuum state with $r_s = 0.5$ and with $\hat{q}$ quadrature being squeezed.

5) Two-Mode Squeezed Vacuum State: A two-mode squeezed vacuum (TMSV) state is generated by applying the two-mode squeezing operator of $\hat{S}_t(r) = \exp\left[r(\hat{a}_1\hat{a}_2 - \hat{a}_1^\dagger\hat{a}_2^\dagger)/2\right]$ [9], [86], [87], [115] to a pair of vacuum states $|0\rangle|0\rangle$, where $r \in \mathbb{R}$ is the two-mode squeezing parameter, and the indices 1 and 2 represent the two modes. A TMSV state is described in the Fock basis as [9], [86], [87], [115]

$$|\text{TMSV}\rangle = \sum_{n=0}^{\infty} q_n |n\rangle_1 |n\rangle_2, \text{ where}$$
$$q_n = \sqrt{1-\lambda^2}\lambda^n, \tag{18}$$

and $\lambda = \tanh(r)$. The two-mode squeezing in dB is given by $-10\log_{10}[\exp(-2r)]$. Such a squeezed state has a zero mean, and a covariance matrix in the following form [9], [86], [87], [115]

$$\boldsymbol{M} = \begin{pmatrix} v\,\boldsymbol{I} & \sqrt{v^2-1}\,\boldsymbol{Z} \\ \sqrt{v^2-1}\,\boldsymbol{Z} & v\,\boldsymbol{I} \end{pmatrix}, \tag{19}$$

where $v = \cosh(2r)$ is the quadrature variance of each mode, and $\boldsymbol{Z} = diag(1, -1)$. Note that the two-mode squeezing operator $\hat{S}_t$ cannot be factorised into the product of the two single-mode squeezing operators $\hat{S}_s$. Hence, the TMSV state is not a product of the two single-mode squeezed vacuum states. In fact, the squeezing (anti-squeezing) operation applied to the quantum fluctuations does not squeeze (anti-squeeze) the variance of the individual modes, but rather that of the superposition of the two modes, so that we have $V(\hat{q}_-) = V(\hat{p}_+) = \exp(-2r)$ and $V(\hat{q}_+) = V(\hat{p}_-) = \exp(2r)$, where $\hat{q}_- = (\hat{q}_1 - \hat{q}_2)/\sqrt{2}$, $\hat{p}_+ = (\hat{p}_1 + \hat{p}_2)/\sqrt{2}$, $\hat{q}_+ = (\hat{q}_1 + \hat{q}_2)/\sqrt{2}$, and $\hat{p}_- = (\hat{p}_1 - \hat{p}_2)/\sqrt{2}$. For a two-mode squeezing operation with $r > 0$, we have $V(\hat{q}_-) = V(\hat{p}_+) < 1$ and $V(\hat{q}_+) = V(\hat{p}_-) > 1$. The correlations between the quadratures of the two modes are known as Einstein-Podolski-Rosen (EPR) correlations, which indicate the presence of bipartite entanglement. Hence, for the two-mode squeezing operation with $r > 0$ the two modes are entangled, where the entanglement increases upon increasing r. The TMSV state associated with $r > 0$ is the most commonly used Gaussian entangled state [9], [83], [86], [87], [113], [114]. In the limit of $r \to \infty$ we have a maximally entangled state having perfect correlations, yielding $\hat{q}_1 = \hat{q}_2$ and $\hat{p}_1 = -\hat{p}_2$. Note that for $r = 0$ the TMSV state corresponds to two (non-entangled) vacuum states.

The Gaussian entangled squeezed states can be generated by parametric down conversion in a non-degenerate optical parametric amplifier [119]–[123], where a crystal having an optical nonlinearity is pumped by a bright laser beam. A photon of the incoming pumping beam spontaneously transfigures in the non-linear crystal into a lower-energy pair of photons, termed as the signal and the idler [119]–[123]. In Type-II parametric down conversion, which is known as a source of entangled states in the CV domain, the signal and idler are in orthogonal polarizations, forming a Gaussian entangled squeezed state [119]–[123]. In this process, the pump photons of frequency $2\omega_p$ are converted into pairs of entangled photons having a pair of different-frequency modes, namely modes 1 and 2 of frequency ω_1 and ω_2, where $2\omega_p = \omega_1 + \omega_2$. An alternative way of generating the Gaussian entangled squeezed state is by mixing two orthogonally single-mode squeezed vacuum states, where one of the states is squeezed in the $\hat{q}$

quadrature and the other one is squeezed in the $\hat{p}$ quadrature. This mixing can be achieved by a balanced (or 50:50) beam splitter. Note that the single-mode squeezed vacuum state can be generated by Type-I parametric down conversion in a degenerate optical parametric amplifier, where the pump photons of frequency $2\omega_p$ are split into pairs of photons having the same frequency and polarization [123].

Finally, note that by invoking local unitary operators the first moment of every two-mode Gaussian state can be set to zero and the covariance matrix can be transformed into the following standard form [86], [87], [114]

$$\boldsymbol{M_s} = \begin{pmatrix} \boldsymbol{A} & \boldsymbol{C} \\ \boldsymbol{C}^T & \boldsymbol{B} \end{pmatrix}, \tag{20}$$

where we have $\boldsymbol{A} = a\boldsymbol{I}$, $\boldsymbol{B} = b\boldsymbol{I}$, $\boldsymbol{C} = diag(c_+, c_-)$, $a, b, c_+, c_- \in \mathbb{R}$.

B. Homodyne Detection

The homodyne detection of Fig. 9(a) represents the most common measurement in CV quantum information processing [9], [86], [87]. This detection scheme can be used for determining or observing the quadrature operator $\hat{q}$ (or $\hat{p}$) of a mode. The scheme of Fig. 9(a) is experimentally implemented by combining the target mode (relying on the annihilation operator $\hat{a}$) with a local oscillator via a balanced beam splitter. The local oscillator is assumed to be in a bright coherent state $|\alpha_{LO}\rangle$. Since $|\alpha_{LO}\rangle$ is represented by a large number of photons, the local oscillator can be described by a classical complex amplitude α_{LO}. The two output modes of the beam splitter can then be approximated by $\hat{a}_1 = (\alpha_{LO} + \hat{a})/\sqrt{2}$ and $\hat{a}_2 = (\alpha_{LO} - \hat{a})/\sqrt{2}$.

The intensity of each outgoing mode is then measured using a photodetector, which converts the photons of the electromagnetic mode into electrons, and hence into an electric current - which is termed as the photo-current $\hat{i}$. The photo-current is proportional to the number of photons in the electromagnetic mode. Hence, the pair of photodetectors of the two output modes of the beam splitter generate the photo-currents of

$$\begin{aligned} \hat{i}_1 \propto \hat{n}_1 &= \hat{a}_1^\dagger \hat{a}_1 = \left(\alpha_{LO}^* + \hat{a}^\dagger\right)(\alpha_{LO} + \hat{a})/2, \\ \hat{i}_2 \propto \hat{n}_2 &= \hat{a}_2^\dagger \hat{a}_2 = \left(\alpha_{LO}^* - \hat{a}^\dagger\right)(\alpha_{LO} - \hat{a})/2. \end{aligned} \tag{21}$$

Then the difference between the photo-currents $\hat{i}_1$ and $\hat{i}_2$ is measured, or more specifically, $\hat{i}_1 - \hat{i}_2 \propto (\alpha_{LO}^* \hat{a} + \alpha_{LO} \hat{a}^\dagger)$ is measured. Considering a local oscillator associated with $\alpha_{LO} = |\alpha_{LO}| \exp(i\Theta)$, where $|\alpha_{LO}|$ and Θ are the magnitude and phase of the local oscillator respectively, the quadrature operator $\hat{q}$ ($\hat{p}$) can be measured by setting the local oscillator's phase as $\Theta = 0$ ($\Theta = \pi/2$).

In contrast to homodyne detection, heterodyne detection allows us to measure both the quadrature operators $\hat{q}$ and $\hat{p}$ of a mode simultaneously [9], [86], [87]. A heterodyne detector combines the target mode with a vacuum ancillary mode into a balanced beam splitter. Then, homodyne detection is applied to the conjugate quadratures of the two output modes, i.e., to $\hat{q}$ of one output mode and $\hat{p}$ of the other one, which are measured using homodyne detection. The 'price' to pay for this simultaneous detection is the introduction of an additional noise term into the measurements (due to the mixing into the signal of the vacuum state). The implementation of heterodyne detection is shown in Fig. 9(b).

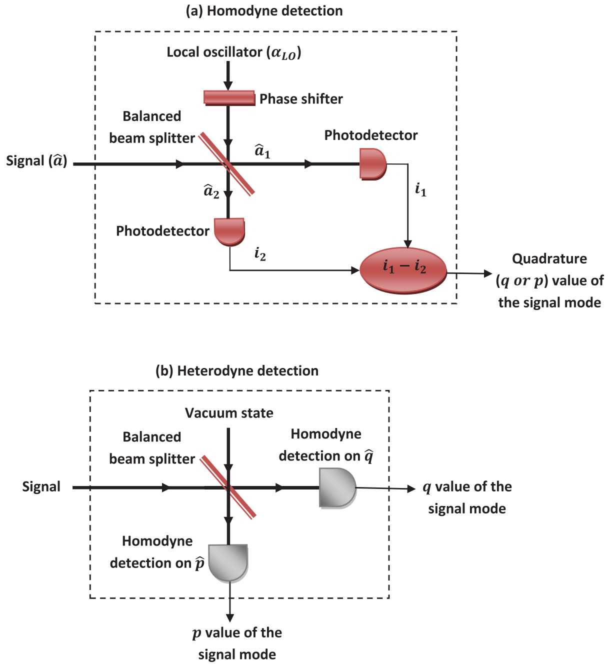


Fig. 9. (a) Homodyne detection: The signal mode is combined with the local oscillator in a balanced beam splitter. Each output mode of the beam splitter is then measured using a photodetector, which generates a photo-current proportional to the photon numbers of the output mode. By measuring the difference between the two photo-currents, the $\hat{q}$ (or $\hat{p}$) quadrature operator of the signal mode can be measured depending on the phase of the local oscillator. (b) Heterodyne detection: The signal mode interacts with a vacuum mode in a balanced beam splitter. By applying homodyne detection to the conjugate quadratures of the two output modes, both the quadrature operators of the signal mode can be measured simultaneously at the price of introducing an additional noise term into the measurements.

C. CV Entanglement

We have already discussed the notion of entanglement. Indeed, this property is one of the most important properties of quantum mechanics, and is widely recognized as a basic resource for quantum information processing and quantum communications (for review, see [83], [87], [113], [114]). We now attempt to quantify the entanglement property of CV states more carefully. We focus our attention on *bipartite* CV entanglement, which relies on the entanglement between two CV quantum systems. Let us consider the pair of CV quantum systems A and B having Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. The Hilbert space of the composite system is given by the tensor product $\mathcal{H}_A \otimes \mathcal{H}_B$. By definition, a bipartite quantum state $\hat{\rho}_{AB}$ relying on the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ is said to be separable, if it can be formulated as a probability distribution over a pair of uncorrelated states expressed as $\hat{\rho}_{AB} = \sum_i p_i \hat{\rho}_i^A \otimes \hat{\rho}_i^B$, where the quantum state $\hat{\rho}_i^A$ ($\hat{\rho}_i^B$) acts on the Hilbert space $\mathcal{H}_A$ ($\mathcal{H}_B$), $p_i \geq 0$, and $\sum_i p_i = 1$. If a quantum state $\hat{\rho}_{AB}$ is separable, then its partial transpose $\hat{\rho}_{AB}^{PT}$ with respect to either subsystem is positive [124]. The partial transposition of $\hat{\rho}_{AB}$ represents the transposition with respect to only one of the two subsystems, for example to system *B*. By definition, a state is stated to be entangled, when it is not separable in the above-mentioned sense.

The *grade* (or quantifiable measure) of entanglement in a *pure* bipartite quantum state $|\psi\rangle$ (with density operator $\hat{\rho}_{AB} = |\psi\rangle\langle\psi|$) can be quantified by the entropy of entanglement $E_v(|\psi\rangle)$. The entropy of entanglement stipulates the number of entangled qubits (measured in ebits)[15] that can be extracted from the state. It also can be considered as the amount of entanglement required to generate the state. The entropy of entanglement is given by the von Neumann entropy of the reduced density operators $\hat{\rho}_A$ or $\hat{\rho}_B$, where $\hat{\rho}_A = \mathrm{Tr}_B(\hat{\rho}_{AB})$ and $\hat{\rho}_B = \mathrm{Tr}_A(\hat{\rho}_{AB})$, with Tr_A and Tr_B denoting the partial trace [83], [87], [113], [114].

For a Gaussian state $\hat{\rho}$, the von Neumann entropy $S(\hat{\rho})$ is given by $S(\hat{\rho}) = \sum_k g(\nu_k)$, where we have $g(x) = [(x+1)/2]\log_2[(x+1)/2] - [(x-1)/2]\log_2[(x-1)/2]$, and ν_k are the symplectic eigenvalues[16] of the covariance matrix of the state. For a pure two-mode entangled state in the form of $|\psi\rangle = \sum_{n=0}^{\infty} q_n |n\rangle_1 |n\rangle_2$, the entropy of entanglement is given by $E_v(|\psi\rangle) = -\sum_{n=0}^{\infty} q_n^2 \log_2 q_n^2$.

Among the different quantifiable measures used as a grade of entanglement for a *mixed* bipartite quantum state $\hat{\rho}_{AB} = \sum_i p_i |\psi_i\rangle\langle\psi_i|$, the most well-known is perhaps the entanglement of formation [125], [126], E_f. This is defined as $E_f(\hat{\rho}_{AB}) = \min\limits_{\{p_i, |\psi_i\rangle\}} \sum_i p_i E_v(|\psi_i\rangle)$, where the minimum is taken over all the possible pure-state decompositions of the mixed state $\hat{\rho}_{AB}$. The entanglement of formation gives the minimal amount of entanglement of any ensemble of pure states realizing the given state $\hat{\rho}_{AB}$ - meaning it quantifies the minimum amount of entanglement needed to prepare the quantum state $\hat{\rho}_{AB}$ from a mix of pure entangled states. In fact, given an entangled state $\hat{\rho}_{AB}$, the entanglement of formation expresses the number of maximally entangled states we need to create $\hat{\rho}_{AB}$. In general, this measure of entanglement is difficult to calculate.

The distillable entanglement is another measure for entanglement, and is the amount of entanglement that can be distilled from a given mixed state [113]. This quantity is also hard to calculate in general, since it would require optimization over all possible distillation protocols. However, there is an entanglement measure which is easy to compute, and gives an upper bound on the amount of distillable entanglement. This measure is the so-called logarithmic negativity [127], [128].

The logarithmic negativity (LN) exhibits the following properties. (i) E_{LN} is a non-negative function, $E_{LN}(\hat{\rho}_{AB}) \geq 0$. (ii) If $\hat{\rho}_{AB}$ is separable, $E_{LN}(\hat{\rho}_{AB}) = 0$. (iii) $E_{LN}(\hat{\rho}_{AB})$ does not increase on average under local (quantum) operations and classical communications. The logarithmic negativity of a bipartite state $\hat{\rho}_{AB}$ is defined as [127]

$$E_{LN}(\hat{\rho}_{AB}) = \log_2[1 + 2N(\hat{\rho}_{AB})], \tag{22}$$

where $N(\hat{\rho}_{AB})$ is the negativity defined as the absolute value of the sum of the negative eigenvalues of $\hat{\rho}_{AB}^{PT}$. The logarithmic negativity quantifies as to what degree the quantum state fails to satisfy the positivity of the partial transpose condition.

In the special case of two-mode Gaussian states, we are able to determine the logarithmic negativity through the use of the covariance matrix [83], [87], [114]. Given a two-mode Gaussian state associated with a covariance matrix $\boldsymbol{M} = \{\boldsymbol{A}, \boldsymbol{C}; \boldsymbol{C}^T, \boldsymbol{B}\}$ where $\boldsymbol{A} = \boldsymbol{A}^T$, $\boldsymbol{B} = \boldsymbol{B}^T$, and $\boldsymbol{C}$ are 2 × 2 real matrices, the logarithmic negativity is given by [83], [87], [114]

$$E_{LN}(\boldsymbol{M}) = \max[0, -\log_2(\tilde{\nu}_-)], \tag{23}$$

where $\tilde{\nu}_-$ is the smallest symplectic eigenvalue of the partially transposed $\boldsymbol{M}$. This eigenvalue is given by [83], [87], [114]

$$\tilde{\nu}_-^2 = \left(\Delta - \sqrt{\Delta^2 - 4\det(\boldsymbol{M})}\right)/2, \tag{24}$$

where $\Delta = \det(\boldsymbol{A}) + \det(\boldsymbol{B}) - 2\det(\boldsymbol{C})$.

D. Gaussian Lossy Quantum Channel

Consider a fixed-attenuation channel described by a transmissivity of $0 \leq \tau \leq 1$ and thermal noise variance of $V_n \geq 1$. Note that in the optical frequency domain the average number of photons is very low even at room temperature (300K), hence the thermal noise has a negligible impact on the signal. In fact, in the optical frequency domain the noise variance is effectively unity, simply representing the vacuum noise. However, in the millimeter-wave domain the thermal noise exhibits a variance, V_n, which is much higher than unity. More specifically, we have $V_n = 2\bar{n} + 1$ with $\bar{n}$ being the average number of photons [129]–[132]. In order to suppress the thermal noise, the system has to be operated at very low temperatures, e.g., <100mK. The average number of photons for a single mode is given by [129]–[132] $\bar{n} = [\exp(hf/k_B T_b) - 1]^{-1}$, where f is the frequency of the mode, k_B is the Boltzmann's constant, and T_b is the temperature.

A fixed-attenuation channel is a Gaussian channel, which transforms the Gaussian input states into Gaussian states. For example, if a single-mode Gaussian quantum state is transmitted through a fixed-attenuation channel, it will remain Gaussian at the output of the channel even though it has experienced channel loss. We can model the impact of a fixed-attenuation channel of transmissivity τ and thermal noise variance V_n on the single-mode input Gaussian state $\hat{\rho}$ by a beam splitter transformation, with the transmissivity of the beam splitter being τ and reflectivity $1-\tau$. In this channel representation shown in Fig. 10 the Gaussian input state is

[15] An ebit (entanglement qubit) as the unit of bipartite entanglement is the amount of entanglement that is contained in a maximally entangled two-qubit state (Bell state). In fact, it is said that each of the Bell states contains one ebit of entanglement.

[16] For an arbitrary *N*-mode covariance matrix $\boldsymbol{M}$, there exists a symplectic matrix $\boldsymbol{S}$ such that $\boldsymbol{M} = \boldsymbol{S}\boldsymbol{M_d}\boldsymbol{S}^T$, where $\boldsymbol{M_d} = \bigoplus_{k=1}^{N} \nu_k \boldsymbol{I}$ is a diagonal matrix, and the N positive quantities ν_k are the symplectic eigenvalues of $\boldsymbol{M}$. Note that a symplectic matrix $\boldsymbol{S}$ is a matrix with real elements that satisfies the condition $\boldsymbol{S\Omega S}^T = \boldsymbol{\Omega}$ where $\boldsymbol{\Omega}$ is defined in Eq. (14) [87], [114]. For example, given a two-mode Gaussian state associated with a covariance matrix $\boldsymbol{M} = \{\boldsymbol{A}, \boldsymbol{C}; \boldsymbol{C}^T, \boldsymbol{B}\}$, where $\boldsymbol{A} = \boldsymbol{A}^T$, $\boldsymbol{B} = \boldsymbol{B}^T$, and $\boldsymbol{C}$ are 2 × 2 real matrices, the symplectic eigenvalues of $\boldsymbol{M}$ are given by $\nu_\pm^2 = (\Delta \pm \sqrt{\Delta^2 - 4\det(\boldsymbol{M})})/2$, where $\Delta = \det(\boldsymbol{A}) + \det(\boldsymbol{B}) + 2\det(\boldsymbol{C})$ [87], [114].

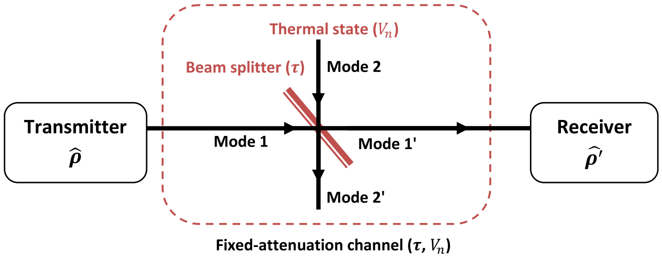


Fig. 10. The beam splitter representation of a fixed-attenuation channel with transmissivity τ and thermal noise variance V_n. In this channel representation, the transmitted signal mode is combined with a thermal mode of variance V_n in a beam splitter of transmissivity τ. In the case of a pure-attenuation channel (without thermal noise), the signal mode is simply combined with a vacuum mode of variance $V_n = 1$.

combined with the thermal noise in the beam splitter, such that one input mode of the beam splitter is the Gaussian input state $\hat{\rho}$ having the corresponding quadratures of $\hat{q}_1, \hat{p}_1$ and the second input mode is the thermal noise with corresponding quadratures of $\hat{q}_2, \hat{p}_2$. As a result of the beam splitter transformation we have the output modes $1'$ (corresponding to the received quantum state $\hat{\rho}'$ at the output of the channel) and $2'$ with corresponding quadratures of $\hat{q}_1', \hat{p}_1'$ and $\hat{q}_2', \hat{p}_2'$ respectively. These output quadratures can be described by [87]

$$\hat{R}_{out} = \begin{pmatrix} \sqrt{\tau}\boldsymbol{I} & \sqrt{1-\tau}\boldsymbol{I} \\ -\sqrt{1-\tau}\boldsymbol{I} & \sqrt{\tau}\boldsymbol{I} \end{pmatrix} \hat{R}_{in}, \tag{25}$$

where $\hat{R}_{in} = (\hat{q}_1, \hat{p}_1, \hat{q}_2, \hat{p}_2)$, and $\hat{R}_{out} = (\hat{q}_1', \hat{p}_1', \hat{q}_2', \hat{p}_2')$. As a result, the quadrature variance of the received quantum state at the output of the channel is given by $V(\hat{q}_1') = \tau V(\hat{q}_1) + (1-\tau) V_n$, and $V(\hat{p}_1') = \tau V(\hat{p}_1) + (1-\tau) V_n$.

Let us now use such a channel representation to analyse the evolution of a two-mode Gaussian quantum state over a fixed-attenuation channel (the general multimode case can be significantly more complex, e.g., [133]). We consider a TMSV state with zero mean and covariance matrix in the form of Eq. (19) as the input quantum state of the channel. There are two settings for the transmission of a two-mode quantum state between two parties, namely, the single-mode transfer and the two-mode transfer [134]. We discuss each of these in detail.

Single-mode transfer: In this setting, the TMSV source is placed at one of the parties' site. In this case, only one mode (mode 2) is transmitted through a fixed-attenuation channel, with the other mode (mode 1) remaining unaffected. The Gaussian output state has a zero mean and covariance matrix in the following form [87], [134]

$$\boldsymbol{M_{sm}} = \begin{pmatrix} v\boldsymbol{I} & \sqrt{\tau}\sqrt{v^2-1}\boldsymbol{Z} \\ \sqrt{\tau}\sqrt{v^2-1}\boldsymbol{Z} & (\tau v + (1-\tau) V_n)\boldsymbol{I} \end{pmatrix}, \tag{26}$$

where $v = \cosh(2r)$ is the quadrature variance of each mode in the input TMSV state (r being the two-mode squeezing parameter).

Two-mode transfer: In this setting, the TMSV source is placed somewhere between the two parties. In this case, one mode (mode 1) of the TMSV state is transmitted through a fixed-attenuation channel with transmissivity τ_1 and thermal noise variance V_{n1}, while the other mode (mode 2) being transmitted through another fixed-attenuation channel with transmissivity τ_2 and thermal noise variance V_{n2}. The Gaussian output state has a zero mean and covariance matrix in the following form [87], [134]

$$\boldsymbol{M_{tm}} = \begin{pmatrix} (\tau_1 v + (1-\tau_1) V_{n1})\boldsymbol{I} & \sqrt{\tau_1\tau_2}\sqrt{v^2-1}\boldsymbol{Z} \\ \sqrt{\tau_1\tau_2}\sqrt{v^2-1}\boldsymbol{Z} & (\tau_2 v + (1-\tau_2) V_{n2})\boldsymbol{I} \end{pmatrix}. \tag{27}$$

Here, we have assumed that the pair of fixed-attenuation channels are independent and that the two thermal noises are uncorrelated.

IV. Continuous Variable Quantum Key Distribution

CV-QKD protocols using Gaussian quantum states have been richly analysed in theory [12], [13], [15], [87], [118], [135], [136], and they have also been implemented experimentally [14], [20], [21], [23]–[25], [80], [137]–[140]. Among these contributions, the authors of [12]–[14], [20], [21], [23]–[25], [118], and [137]–[140] exploit the so-called prepare-and-measure (PM) scheme, where Alice prepares CV quantum states and encodes the key information onto the quantum states, which are then transmitted over an insecure quantum channel to Bob. At the output of the channel Bob receives the quantum states and measures them using classical homodyne or heterodyne detectors. As a result, correlated, but non-identical, data is created between Alice and Bob. Each PM scheme of CV-QKD can be represented by an equivalent entanglement-based (EB) scheme [15], [80], [87], [118], [135], [136], where Alice generates a two-mode entangled state,[17] with one mode being held by Alice and the other mode being transmitted through an insecure quantum channel to Bob. Again, Alice and Bob then proceed by measuring/observing their own modes using classical homodyne or heterodyne detectors in order to create correlated but non-identical data. Following the generation of the correlated data, Alice and Bob proceed with classical post-processing over a public, but authenticated, classical channel (in both the PM scheme and EB scheme), so as to generate a key, which remains secret even in the presence of Eve.

A. Prepare-and-Measure Approach

The PM CV-QKD is derived from the classic DV BB84 protocol of [3]. Hence, for the sake of enhancing readability, we commence by detailing the DV BB84 protocol before delving deeper into the specific instantiations of PM CV-QKD.

The DV BB84 protocol, conceived in 1984, is named after its inventors Bennett and Brassard. It derives it's strength from the two fundamental laws of quantum physics, namely the 'no-cloning theorem' and the 'measurement' of Fig. 3. Table III lists an example of the DV BB84 protocol, which proceeds as follows:

1) Alice generates a string of random bits, called the 'raw key', which is much longer than the desired length of the key.

[17] Please refer to Section III-C for CV entanglement.

TABLE III

PREPARE-AND-MEASURE DISCRETE VARIABLE BB84 QKD EXAMPLE (IN THE ABSENCE OF EVE AND NOISE). (1) RANDOM BINARY KEY GENERATED. (2) RECTILINEAR OR DIAGONAL POLARIZATION RANDOMLY SELECTED. (3) QUANTUM STATE PREPARED BY ENCODING THE BINARY KEY OF STEP (1) USING THE POLARIZATIONS OF STEP (2). (4) MEASUREMENT BASIS RANDOMLY SELECTED. INSTANCES WHERE THE PREPARATION AND MEASUREMENT BASIS MATCH ARE MARKED IN GREEN. (5) RECEIVED STATES MEASURED USING THE BASIS OF STEP (4). (6) DETECTED STATES MAPPED ONTO BITS. INSTANCES WHERE THE DETECTED AND RAW KEY BITS DIFFER ARE MARKED IN RED. (7) ONLY THOSE BITS RETAINED, WHICH HAVE THE SAME PREPARATION AND MEASUREMENT BASIS. (8) ERROR RATE ESTIMATED FOR DETECTING THE PRESENCE OF EVE. (9) INFORMATION RECONCILIATION CORRECTS ERRORS IN THE SIFTED KEY. (10) CORRECTED KEY FURTHER SHORTENED USING PRIVACY AMPLIFICATION, HENCE REDUCING EVE'S INFORMATION ABOUT THE KEY

Alice													
1	Raw key	1	0	0	1	1	1	0	1	0	0	0	1
2	Preparation (or encoding) basis	+	+	×	×	+	×	+	+	×	×	+	×
3	Quantum state preparation	→	↑	↗	↘	→	↘	↑	→	↗	↗	↑	↘
Bob													
4	Measurement basis	+	×	×	+	×	×	+	×	×	+	+	+
5	Quantum state detected	→	↘	↗	→	↗	↘	↑	↘	↗	→	↑	→
6	Detected key	1	1	0	1	0	1	0	1	0	1	0	1
Classical post-processing													
7	Sifted key	1		0			1	0		0		0	
8	Parameter (or error) estimation												
9	Information reconciliation												
10	Privacy amplification												

2) Alice exploits two conjugate pairs of states for encoding the classical raw key into photon polarizations (qubits). Specifically, the states within the pair are orthogonal, while the two pairs are the conjugates of each other. In our example, we consider the rectilinear polarization ($+$ in Table III), which maps bit 0 and 1 onto the vertical ($\uparrow$) and horizontal ($\rightarrow$) polarizations, respectively, and the diagonal polarization ($\times$ in Table III), which maps bit 0 and 1 onto the 45° ($\nearrow$) and 135° ($\searrow$) polarizations, respectively. Alice randomly chooses either the rectilinear or diagonal polarization for the action termed as state preparation.
3) Alice encodes the raw key of Step (1) seen in Table III based on the randomly chosen polarizations of Step (2) in Table III using $+$ or $\times$ and sends the resultant qubits to Bob over an insecure quantum channel.
4) Neither Bob nor Eve knows the encoding basis of Step (2) in Table III used by Alice. Therefore, Bob randomly chooses either the rectilinear ($+$) or the diagonal ($\times$) basis for measuring the received qubits. Bob's chosen basis are listed in Step (4) of Table III. Since both Alice and Bob randomly choose the polarization basis, they will end up choosing the same basis roughly half of the time. These instances have been marked in green in Steps (2) and (4) of Table III.
5) If Bob measures the qubits received in the same basis as they were prepared in Step (2) of Table III, then he detects the transmitted bit correctly, provided that the quantum channel is noiseless and there is no eavesdropper. By contrast, if the measurement basis is not the same as the preparation basis, then there is only a 50% chance that Bob will detect the bit correctly. For example, let us consider the second bit of Table III having the value 0, which is encoded in the rectilinear basis ($+$), but measured in the diagonal basis ($\times$). A bit value 0 in the rectilinear basis may also be expressed as a function of the diagonal basis:

$$|\uparrow\rangle \equiv \frac{1}{\sqrt{2}}|\nearrow\rangle + \frac{1}{\sqrt{2}}|\searrow\rangle. \tag{28}$$

Consequently, when $\uparrow$ is measured in the diagonal basis, it is equally likely to collapse either to the state $|\nearrow\rangle$ (bit 0) or the state $|\searrow\rangle$ (bit 1).
6) The detected polarizations of Step (5) may be decoded by invoking the same classical-to-quantum mapping as the encoding operation at the transmitter. Bob detects the bit correctly approximately 75% of the time. All incorrect instances of bit detection are marked in red in Steps (1) and (6) of Table III. Hence, Alice and Bob acquire a correlated key through Steps (1) to (6).
7) Alice and Bob then communicate over an authenticated classical channel for further processing the correlated key they possess, hence termed as 'classical post-processing'. This post-processing commences with 'bit sifting' during which Alice shares the basis used for preparation in Step (2) of Table III, while Bob shares the basis of Step (5) in Table III used for measurement. Both Alice and Bob discard the specific bits whose preparation basis and measurement basis differ, because these instances may result in incorrect detection, which are marked in red in Step (6) of Table III and statistically represent about 25% of the bits. This in turn ensures that both Alice and Bob possess the same secret key in the absence of Eve, provided that the quantum channel is noiseless. The length of this key is approximately half of that of the raw key, in which about half of the basis were different.
8) Recall that qubits cannot be cloned. Therefore, if Eve is listening to the insecure quantum channel, she cannot acquire a copy of the quantum information. Furthermore, Eve unaware of the specific basis in which Alice maps the classical bits onto the qubits, until Alice reveals this information during the classical post-processing stage. Consequently, similar to Bob, Eve chooses a random basis for measurement, while listening to the quantum-domain session between Alice and Bob. This in turn introduces errors in the shared key. Hence, for the sake of determining the presence of Eve, Alice and Bob share a subset of the key and

estimate the fraction of errors. If the resultant error ratio is higher than a pre-determined threshold, the transmission is considered 'insecure' and hence aborted.

9) By contrast, if the transmission is found to be secure, the process termed as 'information reconciliation' is invoked for correcting the dependencies between Alice's and Bob's key, which may include for example the dependencies arising from errors inflicted by a realistic imperfect quantum channel as well as those due to measurements by Eve. Let us now briefly elaborate on the effect of channel errors. Consider the first bit of Table III, which is prepared and measured in the same basis. As shown in Table III, Alice transmits the quantum state $|\rightarrow\rangle$ corresponding to the classical bit 1. Let us consider the scenario where a channel error is inflicted on Alice's quantum state during transmission, so that Bob receives the erroneous state $|\uparrow\rangle$. Now even if Bob measures the received quantum state in the same basis as it was prepared, his detected output will be incorrect. Explicitly, Bob will detect bit 0 upon measurement in the rectilinear basis $(+)$, while Alice transmitted bit 1. Hence, channel errors also introduce dependencies between Alice's and Bob's keys.

10) Eve may acquire information about the secret key by measuring a subset of the key as well as by listening to the public classical information shared during the error reconciliation process. For the sake of reducing this information, the technique of 'privacy amplification' is invoked. Explicitly, privacy amplification generates a shorter key from the corrected key of Step (9), hence reducing Eve's information about the shared key.

In contrast to the PM DV-QKD scheme of Table III, which transmits qubits, a Gaussian PM CV-QKD scheme exploits Gaussian CV quantum states, as shown in Fig. 11.

Explicitly, the CV quantum states prepared by Alice are Gaussian states (squeezed states or coherent states) which are modulated by Gaussian distributions [12]–[14], [20], [21], [24], [25], [118], [135], [137], [138], [140]. In fact, Alice encodes a classical random variable drawn from a Gaussian distribution onto a Gaussian quantum state, which is transmitted to Bob, and then measured by him, thus extracting a classical random variable which is correlated with Alice's. Furthermore, in contrast to the discrete measurement operations of Table III, the measurements of the received quantum states are made by Gaussian measurements, namely by classical homodyne or heterodyne detection. Hence, Alice and Bob share correlated Gaussian data in contrast to the correlated binary stream of PM DV-QKD. The resultant correlated Gaussian distributed random variable (rv) is then processed classically for the sake of generating a virtually error free and secure binary key.

We may notice in Fig. 11 that four different variants of a Gaussian PM CV-QKD protocol exist, since we have two types of Gaussian quantum states, i.e., squeezed and coherent states, and two types of detectors, i.e., homodyne and heterodyne detectors, which are detailed in Section III. In the succeeding subsections, we provide further insights into each of these four variants with the aid of slow-paced quantitative examples.

1) PM CV-QKD Relying on Squeezed States & Homodyne Detection: Table IV gives an example of CV-QKD protocol using squeezed states and homodyne detection [12], which proceeds as follows:

1) Alice generates a real random Gaussian-distributed variable a with zero mean $\mu = 0$ and variance $\sigma^2 = v_m$, as exemplified in Step (1) of Table IV.
2) Alice then decides to encode the Gaussian variable a into either a *p*-squeezed or a *q*-squeezed vacuum state by randomly choosing the $\hat{p}$ or $\hat{q}$ quadrature component for squeezing. More specifically, Alice generates a binary random variable *u* for choosing the $\hat{p}$ or $\hat{q}$ quadrature for squeezing. The chosen quadratures are listed in Step (2) of Table IV.
3) Alice next proceeds with quantum state preparation. Explicitly, Alice prepares a single-mode squeezed vacuum state having the covariance matrix $\boldsymbol{M} = diag(1/v, v)$, where $v = \exp(2r_s)$, and r_s is the single-mode squeezing. The prepared squeezed state is then modulated (displaced) by an amount a of Step (1) in Table IV, where the modulation variance satisfies $v_m = v - 1/v$. Specifically, depending on the quadratures chosen in Step (2) of Table IV, Alice either sends a *q*-squeezed state having a first moment of $(a_q, 0)$, $a_q = a$, or a *p*-squeezed state associated with the first moment $(0,\ a_p)$, $a_p = a$, as illustrated in Step (3) of Table IV. For example, let us consider the first element of raw Gaussian key having the value of 0.9 in Step (1) of Table IV. Since $\hat{p}$ quadrature is chosen in Step (2) of Table IV for preparing the first quantum state, Alice prepares a *p*-squeezed state having the first moment (0, 0.9). The prepared and modulated squeezed states are then transmitted over an insecure quantum channel to Bob.
4) For each incoming quantum state, Bob randomly chooses either the $\hat{q}$ or the $\hat{p}$ quadrature for detection depending on his own binary random variable u', as shown in Step (4) of Table IV.
5) Bob measures the received quantum state in either the $\hat{q}$ or the $\hat{p}$ quadrature using homodyne detection based on the chosen quadratures of Step (4). Note that in order to warrant security, Alice and Bob choose different basis for preparation and measurement (in a random fashion). Consequently, when the preparation and measurement basis are the same, which are marked in green in Steps (2) and (4) of Table IV, Bob accurately detects the transmitted quantum state, provided that the transmission channel is noiseless and there is no eavesdropper. For example, Bob chooses $\hat{p}$ quadrature for the first element of Gaussian key, as shown in Step (4) of Table IV. Since the first element was also prepared in the same quadrature, Bob correctly detects a $\hat{p}$-squeezed state having the first moment (0,0.9). By contrast, if the preparation and detection quadratures do not match, Bob detects a modified version of the transmitted state, which are marked as blank red cells in Table IV.
6) Finally, Bob obtains a real variable $b_q = b$ or $b_p = b$ corresponding to the $\hat{q}$ or the $\hat{p}$ detection quadratures.

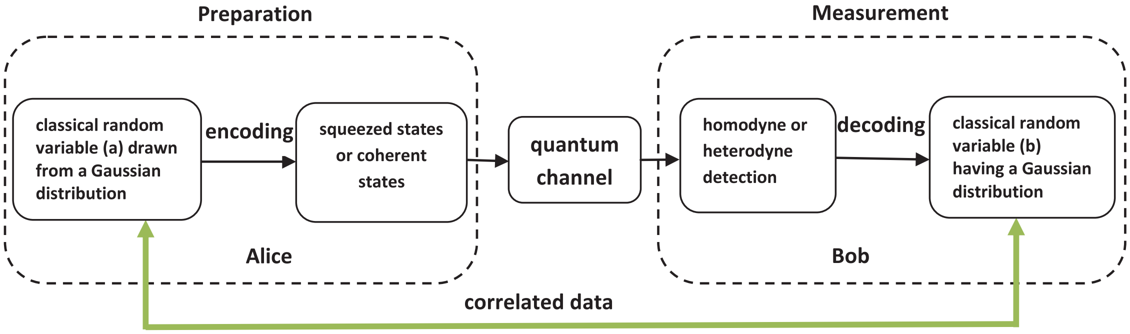

Preparation
Measurement
classical random variable (a) drawn from a Gaussian distribution
encoding
squeezed states or coherent states
quantum channel
homodyne or heterodyne detection
decoding
classical random variable (b) having a Gaussian distribution
Alice
Bob
correlated data

Fig. 11. The quantum communication stage of Gaussian CV-QKD protocol in a PM scheme, which consists of three steps; preparation, transmission, and detection. In a full-Gaussian protocol Alice encodes a classical Gaussian-distributed random variable (*a*) onto Gaussian quantum states (squeezed or coherent states). The prepared states are transmitted through an insecure quantum channel to Bob. In the detection step, received quantum states are measured using Gaussian measurements (homodyne or heterodyne detection) to obtain a classical Gaussian-distributed random variable (*b*), which is correlated with Alice's random variable (*a*).

TABLE IV

Prepare-and-Measure CV-QKD Example Relying on Squeezed States and Homodyne Detection (in the Absence of Eve and Noise). (1) Real Random Variable *a* Generated Using a Gaussian Distribution Having Mean $\mu = 0$ and Variance $\sigma^2 = v_m$. (2) $\hat{p}$ or $\hat{q}$ Quadrature Randomly Chosen for Squeezing. (3) Squeezed State Prepared Having the First Moment (*a*, 0), if $\hat{q}$ Quadrature Is Chosen in Step (2) and the Moment (0, *a*), If $\hat{p}$ Quadrature Is Chosen in Step (2). (4) $\hat{p}$ or $\hat{q}$ Detection Quadrature Randomly Selected. Instances Where the Preparation and Detection Quadratures Match Are Marked in Green. (5) Received States Detected Using the Quadratures of Step (4). The Detection Outcome Is Noisy (or Corrupted), When the Preparation and Detection Basis Do Not Match, Hence Are Marked in Red. (6) Detected States Mapped Onto Gaussian Key. (7) Only Those Key Values Are Retained, Which Have the Same Preparation and Measurement Quadrature

Alice													
1	Raw Gaussian key ($\mu = 0$, $\sigma^2 = v_m$)	0.9	2.4	1.3	2.1	0.5	4.1	1.1	0.3	3.6	0.2	1.7	2.8
2	Preparation (or encoding) quadrature	$\hat{p}$	$\hat{p}$	$\hat{q}$	$\hat{q}$	$\hat{p}$	$\hat{q}$	$\hat{p}$	$\hat{p}$	$\hat{q}$	$\hat{q}$	$\hat{p}$	$\hat{q}$
3	Squeezed state preparation (first moment)	$(0, 0.9)$	$(0, 2.4)$	$(1.3, 0)$	$(2.1, 0)$	$(0, 0.5)$	$(4.1, 0)$	$(0, 1.1)$	$(0, 0.3)$	$(3.6, 0)$	$(0.2, 0)$	$(0, 1.7)$	$(2.8, 0)$
Bob													
4	Detection quadrature	$\hat{p}$	$\hat{q}$	$\hat{q}$	$\hat{p}$	$\hat{q}$	$\hat{q}$	$\hat{p}$	$\hat{q}$	$\hat{q}$	$\hat{p}$	$\hat{p}$	$\hat{p}$
5	Squeezed state detected (first moment)	$(0, 0.9)$	🟥	$(1.3, 0)$	🟥	🟥	$(4.1, 0)$	$(0, 1.1)$	🟥	$(3.6, 0)$	🟥	$(0, 1.7)$	🟥
6	Detected Gaussian key	0.9		1.3			4.1	1.1		3.6		1.7	
Classical post-processing													
7	Sifted Gaussian key	0.9		1.3			4.1	1.1		3.6		1.7	

The resulting variables constitute the detected Gaussian key, as shown in Step (6) of Table IV.

7) Following the measurement of all incoming states by Bob, classical post-processing over the public channel commences via a sifting operation. In this operation, Alice and Bob reveal to each other which of the two randomly selected quadratures they used for preparing (Alice) and measuring (Bob) the information, discarding non-tallying random bit pairs (i.e., $u \neq u'$). A natural way of achieving this is that Alice reveals for each Gaussian rv the specific value of u (i.e., whether she displaced the $\hat{q}$ or the $\hat{p}$ quadrature), and Bob only retains those, where he measured the relevant tallying quadrature (i.e., $u = u'$), as shown in Step (7) of Table IV.

Let us now consider the second variant of Fig. 11.

2) PM CV-QKD Relying on Squeezed States & Heterodyne Detection: Another squeezed-state protocol was developed in [118], in which Bob uses heterodyne detection rather than homodyne detection and measures both the $\hat{q}$ and $\hat{p}$ quadratures for obtaining (b_q, b_p). In the sifting step of this protocol, Bob then disregards one of his quadrature measurements, depending on Alice's specific choice of quadrature preparation. This protocol can be seen as a noisy version of the protocol with squeezed states and homodyne detection, since the heterodyne detection imposes vacuum noise on the measurement. When Bob's Gaussian rv are the reference of error correction (see below) in the classical post-processing, the heterodyne detection protocol exhibits a better robustness against the channel noise than the protocol associated with homodyne detection [118]. Let us now focus our attention on the third variant of Fig. 11.

3) PM CV-QKD Relying on Coherent States & Homodyne Detection: Table V gives an example of the PM CV-QKD protocol using coherent states and homodyne detection [13], [14], [116], which can be described as follows:

1) Alice generates random real numbers a_q chosen from an independent Gaussian distribution of variance v'_m.

TABLE V

Prepare-and-Measure CV-QKD Example Relying on Coherent States and Homodyne Detection (in the Absence of Eve and Noise). (1) Real Random Gaussian Variable a_q Generated. (2) Real Random Gaussian Variable a_p Generated. (3) Coherent State Prepared Having a Mean Value of (a_q, a_p). (4) $\hat{p}$ or $\hat{q}$ Detection Quadrature Randomly Selected. (5) Received States Detected Using the Quadratures of Step (4). (5) Detected States Mapped Onto Gaussian Key. (6) Alice Retains a_q or a_p Depending on Bob's Detection Quadratures. The Retained Key Values Are Marked in Green in Steps (1) and (2)

Alice											
1	Raw Gaussian key (a_q)	0.9	2.4	1.3	2.1	0.5	4.1	1.1	0.3	3.6	0.2
2	Raw Gaussian key (a_p)	1.2	0.9	5.1	2.7	1.5	3.1	0.6	4.3	2.8	0.1
3	Coherent state preparation (mean)	$(0.9, 1.2)$	$(2.4, 0.9)$	$(1.3, 5.1)$	$(2.1, 2.7)$	$(0.5, 1.5)$	$(4.1, 3.1)$	$(1.1, 0.6)$	$(0.3, 4.3)$	$(3.6, 2.8)$	$(0.2, 0.1)$
Bob											
4	Detection quadrature	$\hat{p}$	$\hat{p}$	$\hat{q}$	$\hat{p}$	$\hat{q}$	$\hat{q}$	$\hat{p}$	$\hat{q}$	$\hat{q}$	$\hat{p}$
5	Detected Gaussian key	1.2	0.9	1.3	2.7	0.5	4.1	0.6	0.3	3.6	0.1
Classical post-processing											
6	Sifted Gaussian key	1.2	0.9	1.3	2.7	0.5	4.1	0.6	0.3	3.6	0.1

2) Alice also generates another set of random real numbers a_p, which are also chosen from an independent Gaussian distribution of variance v_m'.
3) Alice then prepares a coherent state, which is modulated (displaced) by the amounts of a_q and a_p generated previously in Steps (1) and (2), so that the resulting coherent state has a mean value of (a_q, a_p). For example, $a_q = 0.9$ and $a_p = 1.2$ are chosen for the first element of key in Steps (1) and (2), respectively. Consequently, Alice prepares a coherent state having a mean value of (0.9,1.2). The prepared coherent states transmitted over an insecure quantum channel to Bob.
4) Bob generates a random variable u' for each incoming state and chooses either the $\hat{q}$ or the $\hat{p}$ quadrature for detection depending on the value of u'.
5) Finally, Bob measures either the $\hat{q}$ or the $\hat{p}$ quadrature component using homodyne detection depending on the chosen quadratures of Step (4), hence obtaining a real variable b_q or b_p, respectively. For example, as can be seen in Table V, $\hat{p}$ quadrature is chosen in Step (4) for detecting the first element of the key. Consequently, when Bob measures the first received coherent state using the $\hat{p}$ quadrature, he obtains a value of 1.2.
6) When the quantum communication phase is completed and all the incoming states have been measured by Bob, classical post-processing over a public channel is commenced by applying sifting, where Bob reveals for each Gaussian rv the specific value of u' (i.e., whether he measured the $\hat{q}$ or the $\hat{p}$ quadrature), and Alice retains a_q or a_p depending on the value of u'. Note that in this protocol only one of the two real random variables generated by Alice is used for the key after the sifting stage. For example, Alice only retains $a_p = 1.2$ for the first element of key, since Bob measured the received state in the $\hat{p}$ quadrature. The retained key values are marked in green in Steps (1) and (2) of Table V.

Finally, we now consider the fourth variant of Fig. 11.

4) PM CV-QKD Relying on Coherent States & Heterodyne Detection: Another coherent-state protocol was developed in [117], where Bob uses heterodyne detection rather than homodyne detection and measures both the $\hat{q}$ and $\hat{p}$ quadrature components for obtaining (b_q, b_p) at the cost of imposing vacuum noise on the measurement. In this protocol, sifting is no longer needed, since both of the real random variables generated by Alice are used for the generation of the key, hence potentially resulting in higher secret key rates.

All the four CV-QKD protocols discussed above in the context of Fig. 11 yield a correlated Gaussian key between Alice and Bob. Please note that the Gaussian key generated in the examples above is the same for both Alice and Bob. However, when Eve is present or in the inevitable presence of noise, Bob's key will be a noisy version of Alice's key. Hence, Bob and Alice will possess correlated but unidentical Gaussian keys. Analogous to the PM DV-QKD of Table III, parameter estimation is then performed (in the classical post-processing stage, following the sifting step), where the two parties reveal a randomly chosen subset of their correlated but unidentical Gaussian key. This allows them to estimate the parameters of the channel, such as the channel's transmissivity and the level of channel noise, as well as to limit the maximum amount of information Eve can infer about their values. This step is followed by an information reconciliation procedure, which involves quantizing Alice's and Bob's correlated Gaussian data into binary keys as well as performing error correction, hence resulting in a near-error-free binary key. As discussed further later, this procedure normally relies on the employment of low density parity check (LDPC) codes [20]. QKD can be operated in two reconciliation scenarios, namely direct reconciliation [141] and reverse reconciliation [13], [14]. In the direct reconciliation protocol Alice's Gaussian data constitute the reference and she sends classical correction information to Bob which may be overheard by Eve. Then Bob corrects his key elements to arrive at the same values as Alice. By contrast, in the reverse reconciliation protocol Bob's Gaussian data constitute the reference and must be estimated by Alice (also by Eve) [13], [14]. Based on the upper bound on Eve's information estimated during the parameter estimation stage, Alice and Bob apply a privacy amplification protocol, which produces a shorter binary key in the spirit of expurgating Eve's information about the shared key, hence Eve's information about the key is substantially reduced.

Whilst in Fig. 11 we had four variants, now there are eight protocol choices for characterising Gaussian CV-QKD in a PM scheme. Explicitly, this is because we must consider

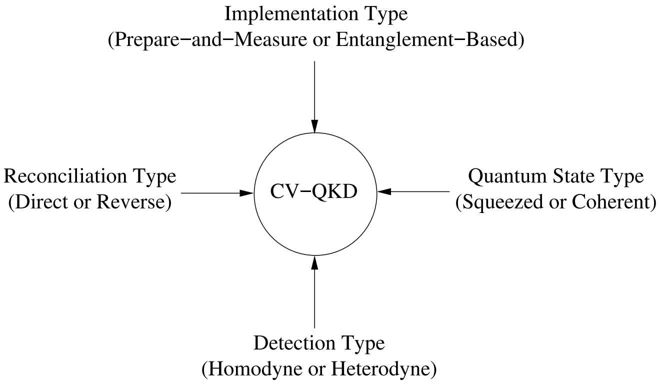


Fig. 12. Gaussian CV-QKD implementation parameters.

both the type of quantum state (squeezed states or coherent states) which Alice prepares, and also the type of detection (homodyne or heterodyne detection) which Bob applies to the received states, as well as the specific type of reconciliation (direct reconciliation or reverse reconciliation). However, recall that all PM schemes have an equivalent EB scheme. Hence, different variants of CV-QKD may be implemented using the parameters summarized in Fig. 12. Next we discuss the entanglement-based approach for implementing CV-QKD protocols.

B. Entanglement-Based Approach

All the Gaussian PM protocols can be described in an unified way using the EB scheme [87], [135] shown in Fig. 13. Here Alice generates a TMSV state, which we refer to as $\hat{\rho}_{AB}$. She keeps mode *A*, and sends mode *B* to Bob. At some time later, Alice and Bob use an unbalanced beam splitter of transmissivity (T_A at Alice's side and T_B at Bob's side), to carry out *generalized heterodyne* detections. If Alice applies homodyne detection ($T_A = 1$), the prepared state should be a squeezed state and if Alice makes a heterodyne detection ($T_A = 1/2$), the prepared state should be a coherent state. The security of the CV-QKD protocols is mostly analysed using their equivalent EB scheme, where a two-mode entangled state is shared between Alice and Bob before their detection observations. Note, in the security analysis of CV-QKD discussed next we will assume that the number of exchanges between Alice and Bob is considered to be infinite (the asymptotic regime). This assumption is adopted in most QKD security analyses since the ability to estimate some quantities (e.g., average values) exactly in the infinite sample-limit, greatly simplifies the analyses.

C. CV-QKD Security Analysis

The most powerful, and most general, attack that Eve can implement against QKD is known as a coherent attack [87], [135]. In this attack, Eve prepares her ancillary system in a global quantum state, which means she prepares an arbitrary joint (entangled) state of the ancillae. After the interaction of the global ancillary system with the signals sent by Alice, the output ancillary system is stored in a quantum memory. Once the classical post-processing relying on the public channel is finished, Eve applies an optimal joint measurement over the ancillary system stored in the quantum memory to maximize her knowledge on the quantum information of the trusted parties. The security analysis of CV-QKD in the face of coherent attacks is very complex. However, under some trivial constraint imposed on the classical post-processing protocol, collective attacks are just as detrimental as coherent attacks [142]. In a collective attack against QKD Eve prepares her ancillary system in a product state of identically prepared ancillae. After interaction of each ancilla with a single signal sent by Alice, the output ancilla is stored in a quantum memory. Once the classical post-processing is completed, Eve applies an optimal joint measurement over the ensemble of ancillae in the quantum memory.

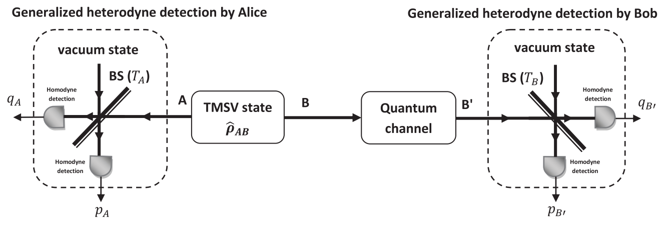


Fig. 13. The quantum communication stage of Gaussian CV-QKD protocol in an EB scheme. Alice generates a Gaussian two-mode entangled state (TMSV state) $\hat{\rho}_{AB}$. She keeps mode *A*, and sends mode *B* through an insecure quantum channel to Bob. If Alice applies homodyne detection, i.e., $T_A = 1$ (heterodyne detection, i.e., $T_A = 1/2$) to mode *A*, she remotely projects the other mode of the entangled state onto a squeezed state (coherent state). Similar to the PM scheme, Bob measures the received state using a Gaussian measurement (homodyne detection, i.e., $T_B = 1$ or heterodyne detection, i.e., $T_B = 1/2$). As a result of their measurements, Alice and Bob end up with two sets of classical Gaussian-distributed random variables which are correlated to each other.

For a realistic reconciliation algorithm, the asymptotic CV-QKD key rate (bits per pulse) against collective attacks is given by [87] and [135] $K = \xi I_{AB} - I_E$, where I_{AB} is the mutual information between Alice and Bob (i.e., between Alice's variable, *a*, as well as Bob's variable, *b*), and 0< ξ <1 is the reconciliation efficiency. This efficiency reflects that in a realistic reconciliation algorithm, Alice and Bob acquire not all of the maximum attainable mutual information. Note that for a perfect reconciliation algorithm we will have $\xi = 1$. Furthermore, I_E is the Holevo bound defined in [87] and [135] as an upper bound on the quantum information stolen by Eve. In the reconciliation step, if we assume that Alice's data represents the reference, then $I_E = I_{AE}$ is the Holevo bound on the mutual information between Eve's quantum memory and Alice's variable. By contrast, if we assume that Bob's data is the reference, then $I_E = I_{BE}$ is the Holevo bound on the mutual information between Eve's quantum memory and Bob's variable. Note that I_{AB} remains the same, regardless of whose data represents the reference of reconciliation. It was also shown [143] that in the family of collective attacks, Gaussian attacks based on Gaussian operations[18] are

[18] Gaussian operations are linear operations with respect to the quadrature amplitudes. Such operations maintain the Gaussian character of Gaussian states.

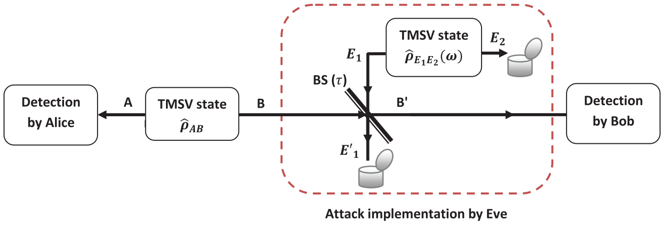

Detection by Alice
A
TMSV state $\hat{\rho}_{AB}$
B
BS (τ)
E_1
TMSV state $\hat{\rho}_{E_1E_2}(\omega)$
E_2
B'
E'_1
Detection by Bob
Attack implementation by Eve

Fig. 14. Implementation of optimal collective Gaussian attack (entangling-cloner attack) by Eve, in which Eve prepares an entangled state, $\hat{\rho}_{E_1E_2}$, interacts mode E_1 with the signal sent from Alice in a beam splitter (with the same transmissivity as the channel transmissivity). The output mode, mode B', is transmitted to Bob through a perfect quantum channel. The other output, mode E_1', and the other arm of Eve's entangled state, mode E_2, are stored in Eve's quantum memory, to be collectively measured at the end of the classical post-processing.

the optimal attacks Eve can implement so as to minimize the secret key rate K.[19]

Let us consider a Gaussian CV-QKD protocol in the EB scheme, where Alice generates a TMSV state $\hat{\rho}_{AB}$, and keeps mode A while sending mode B to Bob over an insecure quantum channel. In the optimal collective Gaussian attack (which is also referred to as the entangling-cloner attack [14]) shown in Fig. 14, Eve models the quantum channel (with transmissivity of $0 \leq \tau \leq 1$ and thermal noise variance of $\omega \geq 1$) by a TMSV state $\hat{\rho}_{E_1E_2}$ having a quadrature variance of ω and a beam splitter of transmissivity τ. In fact, the quadrature variance of $\hat{\rho}_{E_1E_2}$ and the transmissivity of the beam splitter in Fig. 14 are tuned in order to inject the same noise and to impose the same attenuation as in the original channel, respectively. In this beam splitter Eve combines the signal mode gleaned from Alice (mode B) with one mode (mode E_1) of the TMSV state. The first output of the beam splitter (mode B') which is the quantum signal received by Bob is given by $\hat{q}_{B'} = \sqrt{\tau}\hat{q}_B + \sqrt{1-\tau}\hat{q}_{E_1}$, and $\hat{p}_{B'} = \sqrt{\tau}\hat{p}_B + \sqrt{1-\tau}\hat{p}_{E_1}$. The second output of the beam splitter (mode E_1') and mode E_2 of the TMSV state $\hat{\rho}_{E_1E_2}$ are stored by Eve in a quantum memory. Once the classical post-processing over the public channel is completed, this quantum memory is detected by means of an optimal joint measurement which estimates Alice's data (in direct reconciliation) or Bob's data (in reverse reconciliation). Note that in a Gaussian CV-QKD protocol, the asymptotic key rate against optimal collective Gaussian attacks can be calculated through the equivalent EB scheme based on the covariance matrix of the two-mode entangled state shared between Alice and Bob before their detection observations [87], [135], [136].

V. Free-Space Channels to and From Satellites

A. Sources of Loss in FSO Channels

The main sources of loss in FSO communication are diffraction, absorption, scattering and atmospheric turbulence [144]–[148], as encapsulated in Fig. 15. As will be discussed in this section, Diffraction-induced beam-spreading and turbulence-induced beam-wandering as well beam-spreading are dominant in good weather conditions, while absorption, scattering and scintillation are known to be relatively minor issues in good weather conditions.

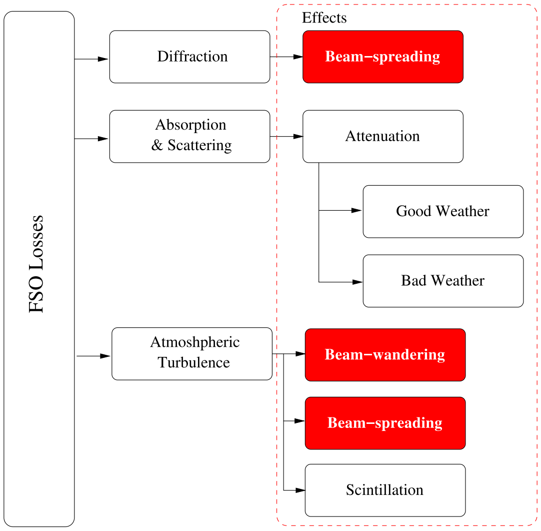


Fig. 15. Sources of losses in FSO channels and their effects on optical signal. Diffraction-induced beam-spreading and turbulence-induced beam-wandering as well beam-spreading dominate in good weather conditions.

Diffraction: Diffraction is a ubiquitous form of the natural wave propagation phenomenon experienced by light beams, and leads to beam-spreading (beam-broadening). Consequently, a certain fraction of the transmitted beam may not be collected by the receiver, since the diameter of the received beam is longer than the receiver's aperture, hence resulting in divergence loss, which increases upon increasing the length of the link. This loss may be mitigated by increasing the receiver's aperture as well as by reducing the transmission wavelength. However, a suitable compromise between the divergence loss, receiver size and cost as well as other transmission losses must be struck. Furthermore, a narrow beam is desirable to reduce diffraction losses, but this makes the link more sensitive to any misalignment between the transmitter and receiver.

Absorption and scattering: Absorption and scattering are imposed by the constituent gases and particles of the atmosphere. Both absorption as well as scattering impose attenuation on an optical wave. Explicitly, absorption is the phenomenon where the energy of optical wave is absorbed by the atmospheric particles, while scattering results in redistribution of the optical energy in arbitrary directions. Furthermore, both effects are strongly wavelength-dependent and become more pronounced when the transmission wavelength is comparable to the size of the atmospheric particles. Both scattering and absorption can be neglected, since they can be substantially mitigated by an appropriate choice of the communication wavelength. Explicitly, there is a negligible absorption at the visible wavelengths spanning from 0.4 to 0.7 mm. For these reasons, scattering and absorption was also neglected in [18], [54], [100]–[102], [110], and [149]–[151]. However, adverse weather conditions, for example fog, rain and snow,

[19] Gaussian collective attacks are as strong as coherent attacks in the limit of an infinite number of quantum states exchanged, however, it is not known this is the case for a realistic finite-length key protocols.

may severely limit the transmissivity of atmospheric channels, as discussed below:

- Fog includes particles having dimensions comparable to the transmission wavelength, hence it is the main source of atmospheric absorption and scattering. More specifically, dense fog may ultimately make optical transmission infeasible [152]. The impact of fog is generally quantified in terms of atmospheric visibility and the associated attenuation per unit length in dB/km. Explicitly, visibility is defined as the distance traversed by a parallel beam of light until its intensity drops to 2% of the original value [153], while the specific attenuation of fog in dB/km, denoted as α_{fog}, may be represented using the popular empirical Mie scattering model [147]:

$$\alpha_{\text{fog}}(\lambda) = \frac{3.91}{V}\left(\frac{\lambda}{550}\right)^{-p}, \tag{29}$$

  where *V* is the visibility range in km, λ is the operating wavelength (550 nm is used as a reference wavelength for visibility range) and *p* is the size distribution coefficient of scattering obtained from the Kim or Kruse model [153]. Specifically, the Kim model gives [154]:

$$p = \begin{cases} 1.6 & V > 50 \\ 1.3 & 6 < V < 50 \\ 0.6V + 0.34 & 1 < V < 6 \\ V - 0.5 & 0.5 < V < 1 \\ 0 & V < 0.5, \end{cases} \tag{30}$$

  while the Kruse model gives [155]:

$$p = \begin{cases} 1.6 & V > 50 \\ 1.3 & 6 < V < 50 \\ 0.585V^{\frac{1}{3}} & V < 0.6. \end{cases} \tag{31}$$

- From the detrimental effects of fog, rain and snow, rain has the least impact, because the size of rain droplets is large as compared to the transmission wavelength. The specific attenuation due to rain my be predicted using [147]:

$$\alpha_{\text{rain}} = k_1 R^{k_2}, \tag{32}$$

  where R is the rain rate in mm/hr, while k_1 and k_2 are modeling parameters, whose value depends on both the size of rain droplets and on the temperature.

- The attenuation due to snow is higher than that of rain, but less than that of fog. However, heavy snow may severely reduce the link's availability, making it comparable to that of fog. The specific attenuation of snow is given by [147]:

$$\alpha_{\text{snow}} = aS^b, \tag{33}$$

  where *S* is the snow rate in mm/hr, while the constants *a* and *b* are set to:

$$a = 5.42 \times 10^{-5} + 5.49, \quad b = 1.38 \tag{34}$$

  in dry snowy conditions and to:

$$a = 1.02 \times 10^{-4} + 3.78, \quad b = 0.72 \tag{35}$$

  in wet snowy conditions.

Hence, adverse weather conditions may significantly attenuate the optical signal, hence substantially degrading the availability of the FSO link. The transmission wavelength should be judiciously chosen to minimize these losses. Furthermore, sufficient link margin should be maintained for the sake of enhancing the link's availability.

Atmospheric turbulence: Atmospheric turbulence arises due to random fluctuations in the refractive index caused by stochastic variations of temperature. The atmosphere contains turbulent random inhomogeneities of various scales - also referred to as turbulent eddies [145]. They range from a large-scale (the outer scale of turbulence) to a small-scale (the inner scale of turbulence). These eddies affect optical wave-propagation through the atmosphere in different ways, depending on their size. In general, large scale eddies produce refractive effects and hence predominately distort the phase of the propagating wave, while small scale eddies are mostly diffractive in nature and therefore distort the amplitude of the wave [144], [145]. The most important effects resulting from the atmospheric eddies are beam-wandering, beam-spreading and beam-scintillation [144]–[146], [148]. We describe each of these three effects in more detail: (i) Random deviation of the beam from its original path is referred to as beam-wandering, which is caused by large-scale turbulent eddies, whose size is large compared to the beam-width. Beam-wandering causes time-varying power fades [54], [145], [146], [148]. (ii) Atmospheric turbulence results in a randomly fluctuating beam-width in the receiver's aperture plane. The broadening of the beam-width (when averaged over time) beyond that due to diffraction is termed as turbulence-induced beam-spreading [54], [57], [101], [145], [148], [156]. (iii) We define scintillation by fluctuations in the received irradiance (intensity) within the beam's cross section. Scintillation includes the temporal variation in the received irradiance and spatial variation within the receiver's aperture. Scintillation is mainly caused by small-scale turbulent eddies [144]–[146], [148].

B. Sources of Loss in FSO Channels to and From Satellites

In satellite-based quantum communications, the uplink and downlink channels are very different, since the atmospheric turbulence layer only occurs near the transmitter on an uplink, and only near the terrestrial receiver on a downlink. In the following, we briefly highlight how these two channels are affected by the above-mentioned turbulence-induced effects.

Uplink channels: For typical dimensions of the aperture size embedded in the ground station, the uplink optical beam first propagates through the turbulent atmosphere and its beam-width is much narrower than the size of the large-scale turbulent eddies [54], [145], [146], [148]. This makes beam-wandering the dominant effect in the uplink [54], [145], [146], [148]. Turbulence-induced beam-spreading also occurs to some extent in the uplink [54], [145]. As a result, the beam received by the satellite (when averaged over time) is wider than that associated with diffraction [54], [145]. Fig. 16 illustrates these two atmospheric effects, namely beam-wandering

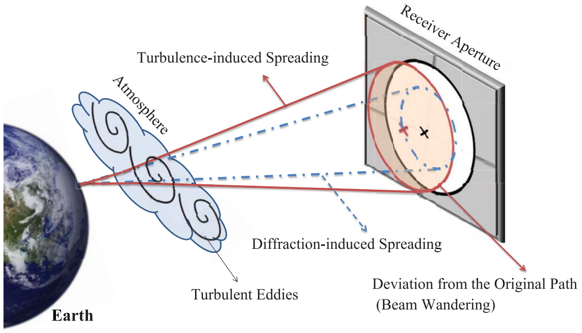

Receiver Aperture
Turbulence-induced Spreading
Atmosphere
Diffraction-induced Spreading
Turbulent Eddies
Deviation from the Original Path
(Beam Wandering)
Earth

Fig. 16. Illustration of beam-wandering (i.e., random deviation of the beam from its original path) and beam-spreading (including spreading induced by diffraction and spreading induced by turbulence) in uplink channels.

and beam-spreading in the uplink. Scintillation is not dominant in the uplink [145], [148].

Downlink channels: In contrast to the uplink case, the downlink optical beam propagates through the turbulent atmosphere only in the final part of its path. Considering the typical aperture size of the optical system embedded in the satellite, the beam-width at its entry into the atmosphere is likely to be larger than the scale of the turbulent eddies. As such, beam-wandering in the downlink tends to be less important relative to uplink channels [54], [145], [146], [148]. The photonic losses in the downlink are likely to be dominated by diffraction effects [54], [57]. Scintillation can occur to some extent in the downlink [145], [148]. However, as a consequence of aperture averaging, the downlink scintillation effects imposed on the detector tend to be negligible, when the receiver includes a large-diameter (>0.5 m) telescope [144], [145], [148].

C. Atmospheric Fading Channels

In atmospheric channels the transmissivity, η_t, fluctuates due to turbulence-induced effects. These fading channels can be characterized by the probability distribution of the transmission coefficients, η (where $\eta = \sqrt{\eta_t}$), which is denoted by $p(\eta)$. For a fading channel associated with the probability distribution $p(\eta)$ the mean fading loss in dB is given by $-10\log_{10}(\int_0^{\eta_0} \eta^2 p(\eta)\, d\eta)$, where η_0 is the maximum value of η.

As discussed in Section V-B, beam-wandering is the dominant turbulence-induced effect in the uplink. As an aside, we note that beam-wandering is expected to dominate the fading contributions in many terrestrial atmospheric communication scenarios [100], [102], [110], [111], [150].

D. Beam-Wandering Model

Here, we describe the probability distribution of the channel coefficients when the channel effects are dominated by beam-wandering. In the first instance we will assume that the beam-width at the receiver's aperture is fixed. That is, initially we will ignore any fluctuations in the beam-width caused by atmospheric turbulence.

In practice, beam-wandering causes the beam-center to be randomly displaced (along the *x* and *y* coordinates) from the center of the receiver's aperture plane. More explicitly, the beam's center position (x_l, y_l) randomly fluctuates around a fixed point, (x_d, y_d), hence its two-dimensional Gaussian distribution is given by [100]

$$p(x_l, y_l) = \frac{1}{2\pi\sigma_b^2} \exp\left(-\frac{(x_l - x_d)^2 + (y_l - y_d)^2}{2\sigma_b^2}\right), \quad (36)$$

where σ_b is the beam-wandering standard deviation. Thus, the beam-deflection distance, $l = \sqrt{x_l^2 + y_l^2}$, i.e., the distance between the beam-center and the aperture-center at (0, 0) fluctuates according to the Ricean distribution [100]

$$p(l) = \frac{l}{\sigma_b^2} I_0\left[\frac{ld}{\sigma_b^2}\right] \exp\left(-\frac{l^2 + d^2}{2\sigma_b^2}\right), \quad (37)$$

where $d = \sqrt{x_d^2 + y_d^2}$ is the distance between the aperture-center and the fluctuation-center (x_d, y_d), while $I_0[.]$ is the modified Bessel function. Note that $d = 0$ means that the beam-center fluctuates around the aperture-center. In beam-wandering the channel transmission coefficient, η, is a function of the beam-deflection distance, *l*, and is given by [100]

$$\eta^2 = \eta_0^2 \exp\left(-\left(\frac{l}{S}\right)^{\gamma}\right), \quad (38)$$

where γ is the shape parameter, *S* is the scale parameter and η_0 is the maximum value of η. The latter three parameters are given by

$$\begin{aligned} \gamma &= 8h \frac{\exp(-4h) I_1[4h]}{1 - \exp(-4h) I_0[4h]} \left[\ln\left(\frac{2\eta_0^2}{1 - \exp(-4h) I_0[4h]}\right)\right]^{-1}, \\ S &= \beta \left[\ln\left(\frac{2\eta_0^2}{1 - \exp(-4h) I_0[4h]}\right)\right]^{-(1/\gamma)}, \\ \eta_0^2 &= 1 - \exp(-2h), \end{aligned} \quad (39)$$

where $I_1[.]$ is the modified Bessel function, and where $h = (\beta/W)^2$, with β being the receiver's aperture radius and *W* the beam-spot radius at the receiver's aperture. Note that both β and *W* have the same units (meter). A schematic illustration of beam-wandering is shown in Fig. 17. According to Eqs. (37) and (38), the probability distribution $p(\eta)$ can be described by the log-negative Weibull distribution [100]

$$\begin{aligned} p(\eta) = {} & \frac{2S^2}{\sigma_b^2 \gamma \eta} \left(2 \ln \frac{\eta_0}{\eta}\right)^{\left(\frac{2}{\gamma} - 1\right)} I_0\left[\frac{Sd}{\sigma_b^2} \left(2 \ln \frac{\eta_0}{\eta}\right)^{\frac{1}{\gamma}}\right] \\ & \times \exp\left(\frac{-1}{2\sigma_b^2}\left[S^2 \left(2 \ln \frac{\eta_0}{\eta}\right)^{\frac{2}{\gamma}} + d^2\right]\right) \end{aligned} \quad (40)$$

for $\eta \in [0, \eta_0]$, with $p(\eta) = 0$, otherwise. In some of the earlier literature, e.g., [157], the log-normal distribution was used. However, at the time of writing we are aware that the log-negative Weibull distribution more accurately describes the operationally important distribution tail [100]. In Fig. 18 the log-negative Weibull distribution is shown for fixed values of the beam-wandering standard deviation σ_b and the receiver's aperture radius β, and for different values of the beam-spot radius at the receiver's aperture *W* (the mean fading loss increases with increasing *W*). In Fig. 19 the log-negative

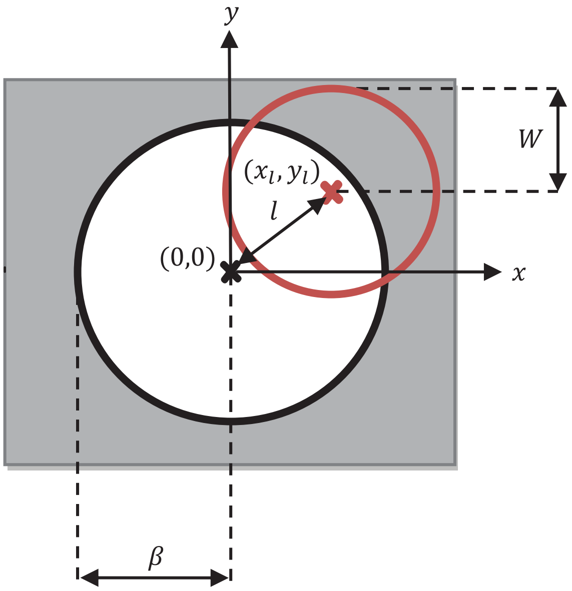


Fig. 17. A schematic illustration of beam-wandering in the receiver's aperture plane, where the beam-center (x_l, y_l) is randomly displaced (along the *x* and *y* coordinates) from the center of the receiver's aperture plane located at (0, 0).

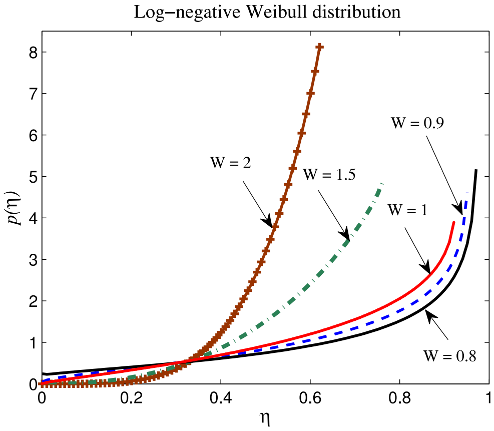


Fig. 18. The log-negative Weibull distribution for $\sigma_b = 0.7$, $\beta = 1$, and $d = 0$ with different values of *W*. For these parameters, $W = 0.8$ leads to a mean fading loss of 2.7 dB and $W = 2$ leads to a mean fading loss of 5.5 dB.

Weibull distribution is shown for the fixed values of W and β, with different values of σ_b (the mean fading loss increases with increasing σ_b).

Let us now we analyse the influence of beam-width fluctuations (caused by atmospheric turbulence) on the beam-wandering model just given. We refer to this effect as turbulence-induced beam-spreading. In doing this analysis, we will assume beam deformation does not occur - meaning the beam shape remains circular as it traverses the atmospheric channel (beam-deformation has been analysed in [101]). In turbulence-induced beam-spreading, the beam-spot radius W randomly changes in the receiver's aperture plane [101] with the probability distribution $p(W)$. Including this effect in our beam wandering model, the transmission coefficient of the channel, η, is now a function of the two random variables l and W according to Eqs. (38) and (39). We define a new variable Θ by setting $\Theta = 2\ln(\frac{W}{w_0})$, where w_0 is the initial beam-spot radius at the radiation source. This is useful since Θ randomly changes according to a normal distribution with the mean value $\langle\Theta\rangle$ and standard deviation σ_Θ [101]. Hence we have

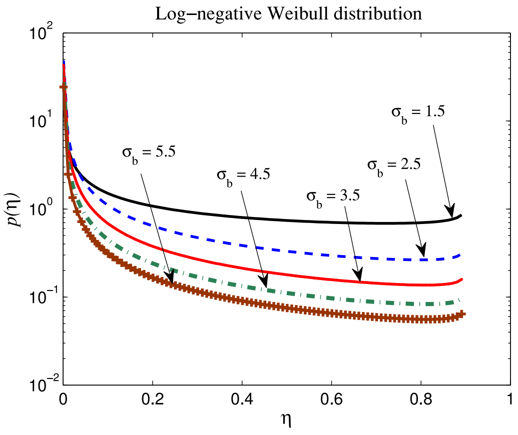


Fig. 19. The log-negative Weibull distribution for $W = 1.1$ and $\beta = 1$, and $d = 0$ with different values of σ_b. For these parameters, $\sigma_b = 1.5$ leads to a mean fading loss of 7.4 dB and $\sigma_b = 5.5$ leads to a mean fading loss of 17.8 dB.

$$p(\Theta) = \frac{1}{\sqrt{2\pi\sigma_\Theta^2}} \exp\left(-\frac{(\Theta - \langle\Theta\rangle)^2}{2\sigma_\Theta^2}\right). \tag{41}$$

With the inclusion of beam-width fluctuations in beam wandering, the calculation of a closed-form solution for $p(\eta)$ is not straightforward. However, given the knowledge of the probability distribution of $p(l)$ of Eq. (37) and $p(\Theta)$ of Eq. (41), we can calculate certain important quantities after averaging over all values of the channel's transmission coefficient. For instance, the mean fading loss in dB of a fading channel with the inclusion of beam-width fluctuations is now given by $-10\log_{10}(\int \eta^2(l,\Theta)p(l,\Theta)dld\Theta)$. Assuming that atmospheric turbulence is isotropic [101] and $d = 0$, the mean fading loss in dB of a fading channel (after the inclusion of beam-width fluctuations in the beam-wandering model) is given by $-10\log_{10}(\int \eta^2(l,\Theta)p(l)p(\Theta)dld\Theta)$. Note, with the inclusion of beam-width fluctuations, the maximum value of the channel's transmission coefficient η_0 is no longer fixed but rather randomly changes.

Optical losses in the downlink are usually orders of magnitude lower relative to uplinks [40], [66]–[68]. This means that if the "price" is paid in terms of placing the critical quantum technology on board the satellite (rather than the easier case of maintaining the quantum technology in ground stations), then much better quantum communication channels can be obtained. As alluded to earlier, the principal reason for this improvement is that in the downlink, diffraction of the beam is the main contributor to photon losses - not beam-wandering as in the uplink (see Fig. 20). The important fact is that by the time the downward-link beam hits the main turbulence-inducing layers of the atmosphere (this layer commences at about 20 km from ground level) the beam is much closer to its target and therefore any induced beam-wandering is less effective. Clearly, as opposed to most communication channels, there will be no directional reciprocity in channel

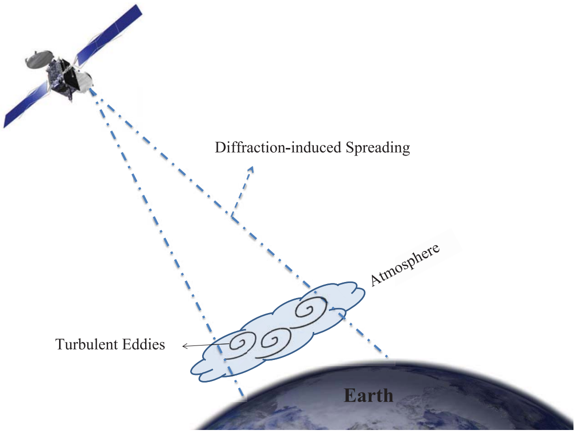


Fig. 20. Illustration of diffraction-induced beam-spreading as the main contributor to photon losses in downlink channels.

throughput for quantum communications with satellites. The recent experimental deployments of quantum communication in space have mostly exploited the more favourable downlink channel conditions [66], [67]. The losses in the downlink can then be modelled quite simply (to first order) through diffraction-only effects with the beam divergence following a λ/D scaling, where D is the diameter of the satellite telescope and λ is the transmission wavelength [40].

E. Estimation of a FSO Channel

Note that the rate of atmospheric fluctuations we consider are on the order of a few kHz, which is at least a thousand times slower than the typical transmission rates [145]. This means that the channel's transmission coefficient can be measured at the cost of additional (classical) transmission and receiver complexity [17], [149], [150], [158]. These channel measurements may be carried out using several schemes, e.g., by transmitting coherent (classical) light pulses that are intertwined with the quantum information [149], [150] or by transmitting a local oscillator (i.e., a strong coherent laser pulse which is mixed with the signal field in the homodyne detection and serves as a phase reference) [17]. In [17] measurement of the atmospheric channel's transmission coefficients was carried out in real time at the receiver by passing a local oscillator through the channel in a mode orthogonally polarized to the signal. The technique of measuring the atmospheric channel's transmission coefficient by an auxiliary classical laser beam was introduced in 2012 [149], and its practical employment was demonstrated for a one-way communication link in 2015 [150]. The same technique based on the intensity of the signal itself was realized in [158].

VI. Entanglement Distribution and CV-QKD Implementation Via Satellite

A. Entanglement Distribution and Standard QKD Protocols

In the context of satellite-based quantum communication we are faced with two different channels, namely, the uplink (ground-to-satellite) channels and the downlink (satellite-to-ground) channels. In the uplink, the ground station transmits signals to the satellite receiver, and in the downlink, the satellite transmits signals to the ground station receiver. Correspondingly, there are several possible architectures for implementing satellite-based quantum communication depending on the types of links utilized. Some of these configurations are illustrated in Fig. 21. Explicitly, the schemes (a) and (b) illustrate the uplink and downlink channels, respectively (both links have been demonstrated in the DV domain [65], [66], [68]). In scheme (c) of Fig. 21, the deployment of quantum technology at the satellite is minimized, since the satellite is utilized only in a reflector mode (i.e., a simple relay). As a proof of concept for the reflecting paradigm, we note the recent experimental tests of [47]–[49], where single photons (weak laser coherent pulses) emitted by the ground station were reflected (and subsequently detected on the ground) by a LEO satellite via the satellite's cube retroreflectors. In scheme (c) the complex quantum engineering components are limited to the ground stations, since the source of quantum states is located in one of the ground stations and the receiver of quantum states is located in the other ground station. Although satellite reflection towards another station

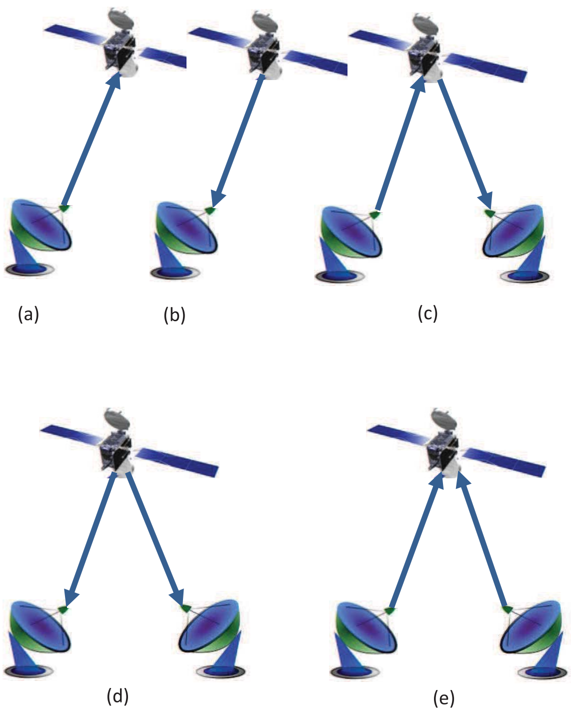


Fig. 21. Illustration of various architectures for implementing satellite-based quantum communication. In (a) ((b)) quantum states are transmitted from the ground station (satellite) to the satellite (ground station) over an uplink (a downlink) channel. In (c) quantum states are transmitted from one ground station over an uplink channel to the satellite, and then reflected at the satellite to the second ground station over a downlink channel. In (d) quantum states are generated on board the satellite, and then transmitted through different downlink channels to separate ground stations. In (e) quantum states are transmitted from two separate ground stations over two different uplinks to the satellite, at which quantum measurements are performed on the received quantum states, and the classical measurement results are communicated back to the ground stations.

constitutes a sophisticated engineering task in its own right, it does not require onboard generation of quantum communication information. There are many practical advantages in deploying quantum communication technology at the ground stations, such as lower-cost maintenance, and the ability to rapidly upgrade as new quantum technology matures. The other schemes, (d) and (e), in Fig. 21 can be considered as space-based high-complexity schemes, since they involve the deployment of quantum technology at the satellite. In scheme (d) (again already demonstrated for DV states [67]) the source of quantum states is located on board the satellite, with both ground stations acting as receivers. In scheme (e) the two ground stations transmit quantum states to the satellite. In the satellite, quantum measurements are performed on the received states and the classical measurement results are communicated back to the ground stations. Scheme (e) can be utilized in support of entanglement swapping and measurement-device-independent protocols so as to implement QKD between the two ground stations.

Let us reconsider the quantum communication architectures of Fig. 21 for CV entanglement distribution and for CV-QKD implementation. We assume that the source of quantum communication in the transmitter(s) is a two-mode entangled state associated with modes 1 and 2. In the scheme (a) (the scheme (b)) of Fig. 21, a two-mode entangled state is generated by Alice at the ground station (satellite) with one mode, mode 1, kept by Alice, while the other mode, mode 2, is transmitted to Bob located at the satellite (ground station) over the uplink (downlink). In the scheme (c) of Fig. 21, a two-mode entangled state is generated by Alice at the ground station transmitter with one mode, mode 1, held at the ground station transmitter and the other mode, mode 2, transmitted over the uplink to the relay satellite. The received mode is then reflected in the satellite and transmitted through the downlink to Bob at the ground station receiver. In the scheme (d) of Fig. 21, a two-mode entangled state is generated on board of the satellite with both modes then sent over the separate downlinks to Alice and Bob located at the separate ground stations. In the scheme (e) of Fig. 21, Alice and Bob are located in the separate ground stations, both initially possessing a two-mode entangled state. One mode of each entangled state is kept by a ground station transmitter and the second mode of each state is transmitted over the uplink to the relay satellite, in which on-board entanglement swapping is performed on the arriving modes. To elaborate a little further, entanglement swapping [7] is a standard quantum protocol conceived for establishing entanglement between distant quantum systems that have never interacted [159]–[162]. It is the central mechanism of quantum repeaters [31], enabling the distribution of entanglement over large distances. In the scheme (e) of Fig. 21, the received modes are swapped at the satellite via a CV Bell measurement [82], where the two modes are mixed through a balanced beam splitter. Explicitly, the $\hat{q}$ quadrature of one of the output modes of the beam splitter and the $\hat{p}$ quadrature of the output mode are separately measured by two homodyne detectors. This process is sometimes described by saying that the two output modes of the beam splitter are conjugately homodyned [82]. The classical outcome of the Bell measurement is then communicated to Alice and Bob so that they can optimally displace their modes, according to the measurement outcome, in order to maximize the resultant entanglement shared between the ground stations. This entanglement swapping scheme between two ground stations via satellite is shown more explicitly in Fig. 22.

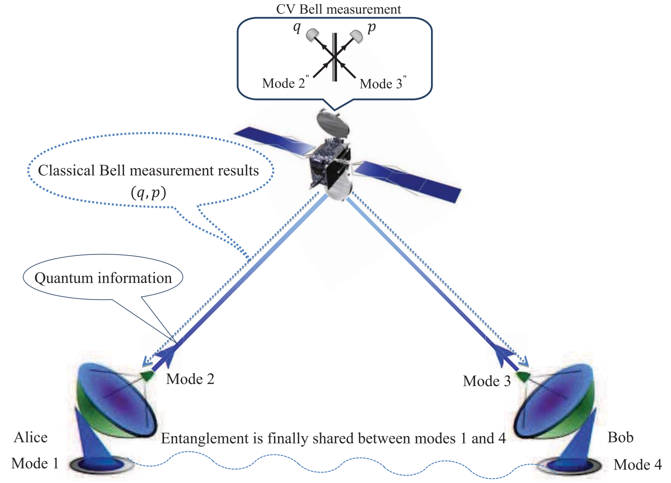


Fig. 22. Entanglement swapping between two ground stations via satellite: The two-mode entangled state of modes 1 and 2 (modes 3 and 4) is initially owned by Alice (Bob). Mode 1 (mode 4) is kept by Alice (Bob) and mode 2 (mode 3) is then transmitted over the uplink to the relay satellite. The received modes $2''$ and $3''$ (where the $''$ indicates that the modes have now incurred losses) are mixed through a balanced beam splitter and the $\hat{q}$ quadrature of one of the output modes and the $\hat{p}$ quadrature of the other one are measured by two homodyne detectors. The classical outcome of the Bell measurement is then communicated to Alice and Bob. As a result, there would exist an entangled state shared between modes 1 and 4.

As a result of the entanglement distribution in each quantum communication scheme of Fig. 21, there would exist an entangled state shared between Alice and Bob. Once the entangled states have been shared between the stations, for each scheme of Fig. 21, Alice and Bob are able to invoke CV-QKD protocols in the EB scheme by applying homodyne or heterodyne detection of their own modes. The level of entanglement produced by the quantum communication schemes considered here as well as the quantum key rates of the EB CV-QKD protocols in these schemes have recently been analyzed in [105]–[109].

In the schemes (a), (b), and (c) of Fig. 21 the entangled source originates from one of the trusted parties (Alice). However, in the scheme (d) of Fig. 21 the entangled source originates from the satellite, which in some circumstances may be controlled by the eavesdropper, Eve. In [136], it has been shown that in the context of the EB CV-QKD protocols Alice and Bob can still generate a secure key, even when Eve controls the entanglement source.

B. Measurement-Device-Independent QKD Protocols

In the scheme (e) of Fig. 21 the entangled source originates from both trusted parties (Alice and Bob), however, the Bell measurement at the satellite may be controlled by

Eve. In [163], it has been demonstrated that in CV-QKD protocols the secret key to be shared between the two trusted parties can be generated by the measurement of an untrusted intermediate relay. In measurement-device-independent (MDI) protocols of QKD [163]–[165], Alice and Bob are not connected by direct links, and an intermediate relay is used for completing the communication link. In MDI protocols the measurement device is the intermediate relay, whose operation may be controlled by an adversary. Fig. 22 is in fact one example of a scenario over which a MDI protocol may be implemented.

The security of CV-MDI protocols is usually analysed using EB schemes that invoke CV entanglement swapping at the relay similar to that shown in Fig. 22 Although CV-MDI protocols are practically implemented in a PM scheme (see below).

In the EB equivalent of the Gaussian MDI-QKD protocols, a pair of TMSV states associated with the quadrature variance of $v = \cosh\,(2r)$ (where r is the two-mode squeezing), is initially owned by Alice and Bob. One mode of each entangled state is held by Alice and Bob, while the second mode of each state is transmitted to the intermediate relay over the insecure channel. The received modes are swapped via a CV Bell measurement at the intermediate relay. The swapping process continues by the relay communicating the Bell measurement result through a classical public channel to Alice and Bob. After receiving the Bell measurement outcome, Bob displaces his mode, while Alice keeps her mode unchanged. Then Alice and Bob measure their modes by homodyne (or heterodyne) detectors to create correlated data. After the establishment of a sufficiently large amount of correlated data, Alice and Bob proceed with the classical post-processing over an authenticated public channel to create a secret key.

In the EB scheme of the Gaussian MDI-QKD protocols, if Alice and Bob apply a homodyne detection of their modes, the scheme becomes equivalent to the PM scheme, in which Alice and Bob prepare squeezed states, and if Alice and Bob apply a heterodyne detection of their modes, the scheme becomes equivalent to the PM scheme in which Alice and Bob prepare coherent states. We discus these PM schemes next.

The MDI implementation of Gaussian CV-QKD protocols in the PM scheme depends on whether the Gaussian resource is a squeezed or a coherent state. If a squeezed state, Alice prepares her mode in a squeezed state with the quadrature variance $v = \exp(2r_s)$, where r_s is the single-mode squeezing. Which one of the two quadratures is to be squeezed is based on a randomly generated bit. The chosen quadrature is then modulated by a random Gaussian-distributed variable with zero mean and variance v_m conditioned on $v_m = v-1/v$. The same procedure is applied independently at Bob's side. If the Gaussian resource is a coherent state, Alice prepares her coherent-state mode with each quadrature independently modulated by a random Gaussian-distributed variable having zero mean and variance of v'_m. Likewise Bob.

Following transmission to the satellite of the modes belong to Alice and Bob, and irrespective of the Gaussian resource used, the satellite makes a CV Bell measurement on each mode pair, announcing the results. Alice and Bob undertake some modification of their data based on these results and undergo some classical post-processing to end up with a shared key. More details of this process can be found in [108].

Note the modulation variance v'_m (in the protocol using coherent states) can reach very high values, e.g., $v'_m = 60$ [163]. With the use of squeezed states, however, achieving high values of squeezing reamins experimentally challenging. As such, quadrature variance v and of the modulation variance v_m are limited in the range of values attained. Note that $v = 5.05$ is equivalent to the two-mode squeezing of 10 dB [166]. Note also that vacuum squeezing at 15 dB is currently the highest obtainable in any experiment [167].

Previous contributions on MDI-QKD protocols have mainly been focussed on fixed-attenuation channels [30], [163], [168]–[177]. In [108], a MDI implementation has been investigated in order to establish Gaussian CV-QKD protocols between two ground stations, where the communication occurs between the ground stations via a LEO satellite over a pair of independent atmospheric channels. In this CV-MDI protocol the measurement device is the satellite itself, which can be controlled by an adversary. In [108], it has been demonstrated that while the CV-MDI protocol is only feasible for low-loss fixed-attenuation channels, the protocol is capable of achieving a beneficial secure key rate even for transmission over high-loss atmospheric channels. Note that in MDI-QKD the devices of Alice and Bob have to be trusted [30], [163], [168]–[177]. Nonetheless, it has recently been shown that QKD is possible even when the device of one of the parties is untrusted [178]–[180]. The security of this one-sided device-independent protocol using CV quantum states has recently been investigated both theoretically and experimentally [181], [182].

We note that MDI protocols represent a step closer to full device-independent protocols. These latter protocols are based on Bell violation measurements at the receivers, and represent the most robust form of QKD (the form that requires the least number of assumptions). Although some work has been carried out in relation to CV states in device independent QKD (e.g., [183]), practical progress is limited due to the very low key rates expected. CV MDI-QKD protocols, with their reduced assumptions on how the measurement device must operate, currently represent the most robust form of QKD that still lead to reasonable key rates. The MDI protocols remain unconditionally secure in their generation of keys - the best an adversary in charge of the measurement device can do is drive the key rate to zero (e.g., by broadcasting false Bell measurement results).

C. Entanglement Determination and Quantum Key Rate Computation

The evolution of quantum states as they prorogate through atmospheric fading channels can be considered in two different scenarios. In the first scenario, the transmission coefficient η of the atmospheric fading channel is unknown, while in the second scenario it is known. In this latter scenario, it is assumed that the transmission coefficient can be measured in real time at the receiver.

1) Scenario 1 (The Transmission Coefficient of the Fading Channel Is Unknown): Here, we consider the distribution of a two-mode entangled state over satellite-based atmospheric fading channels. In fact, we assume that the transmitter initially possesses a two-mode (mode 1 and mode 2) entangled state $\hat{\rho}$, with one (or more) of the modes transmitted to the receiving station(s) through atmospheric fading channels. This leads to two operational settings.

Single-mode transfer: In this setting we assume that mode 1 of $\hat{\rho}$ remains at the ground station (satellite), while mode 2 of $\hat{\rho}$ is transmitted to the satellite (ground station) over the fading uplink (downlink) characterized by the probability distribution $p(\eta)$ and the maximum transmission coefficient of η_0. The density operator of the two-mode state at the ground station and satellite for each realization of the transmission coefficient η is given by $\hat{\rho}'(\eta)$. Since η is a random variable, the elements of the total density operator of the resultant mixed state $\hat{\rho}'_t$ are calculated by averaging the elements of the density operator $\hat{\rho}'(\eta)$ over all possible transmission coefficients of the fading channel, giving the ensemble-averaged state of [107]

$$\hat{\rho}'_t = \int_0^{\eta_0} p(\eta)\hat{\rho}'(\eta)\, d\eta. \tag{42}$$

Now, let us consider the initial two-mode entangled state $\hat{\rho}$ at the transmitter being a Gaussian state [102], [103], [105], [106], [184]. In this case the resultant ensemble-averaged state $\hat{\rho}'_t$ is a non-Gaussian mixture of the Gaussian states $\rho'(\eta)$ obtained for each realization of η. Since the resultant ensemble-averaged state shared by the ground station and the satellite is a non-Gaussian state, it cannot be completely described by its first and second moments. Therefore, the final entanglement computed based on the covariance matrix of the resultant ensemble-averaged state will represent only the Gaussian entanglement between the ground station and the satellite, but not the total distributed entanglement [102], [103], [105], [184]. In order to calculate the total shared entanglement between the stations, the entanglement has to be computed based on the density operator of the resultant ensemble-averaged state [107].

Note that if we use the shared entanglement created for subsequent use in QKD, i.e., a EB CV-QKD protocols operating over atmospheric fading channels,[20] then the same concept (use of ensemble averaged states) is invoked when the quantum key rate is calculated. Note that when the quantum key rate is in fact calculated based on the covariance matrix of the resultant ensemble-averaged state $\hat{\rho}'_t$, the key rate computed is only related to the Gaussian component of $\hat{\rho}'_t$ [106].

Two-mode transfer: In this setting we assume that the satellite initially possesses a two-mode entangled state $\hat{\rho}$, with mode 1 transmitted to ground station 1 over a fading downlink obeying the probability distribution of $p_1(\eta_1)$ and having the maximum transmission coefficient of η_{01}, while mode 2 is transmitted to ground station 2 over a different fading downlink characterized by the probability distribution $p_2(\eta_2)$ and having the maximum transmission coefficient of η_{02}. Here, the two fading downlinks are assumed to be independent. The density operator of the two-mode state at the ground stations for each realization of the transmission coefficients η_1 and η_2 is given by $\hat{\rho}'(\eta_1, \eta_2)$. The elements of the total density operator of the resultant mixed state $\hat{\rho}'_t$ are calculated by averaging the elements of the density operator $\hat{\rho}'(\eta_1, \eta_2)$ over all possible transmission coefficients of the two separate fading channels, giving the ensemble-averaged state of [107]

$$\hat{\rho}'_t = \int_0^{\eta_{01}} \int_0^{\eta_{02}} p_1(\eta_1) p_2(\eta_2) \hat{\rho}'(\eta_1, \eta_2)\, d\eta_1 d\eta_2. \tag{43}$$

2) Scenario 2 (The Transmission Coefficient of the Fading Channel Can Be Measured): Let us now assume a modified scenario, in which the variable transmission coefficient of the atmospheric fading channel is measured with the aid of a separate coherent signal. For example, when a local oscillator in a polarized mode orthogonal to the signal is sent through the channel. Although this increases the complexity of the system, the grade of entanglement (and hence the quantum key rate of the EB CV-QKD protocols implemented based on this entanglement) generated between the stations will be increased.

When considering this scenario in the single-mode transfer setting where the transmission coefficient η is measured at the receiving station, the final entanglement can be calculated as [107]

$$E = \int_0^{\eta_0} p(\eta)\, E\big[\rho'(\eta)\big]\, d\eta, \tag{44}$$

where $E[\rho'(\eta)]$ is the grade of entanglement of a state received through the channel of transmission coefficient η.

In this scenario, when the initial two-mode entangled state $\hat{\rho}$ at the transmitter is a Gaussian state, the mixed states $\rho'(\eta)$ collected at the receiver during each transmission coefficient window remain Gaussian, because within each (small) fading bin we can assume that the transmission coefficient is constant and therefore the states during that particular bin remain Gaussian. In this case, the grade of entanglement of the mixed Gaussian state $\rho'(\eta)$, i.e., $E[\rho'(\eta)]$ can be calculated based on the covariance matrix of $\rho'(\eta)$, which results in E of Eq. (44) representing the total entanglement shared between the stations [107].

Considering this scenario in the EB CV-QKD protocols communicating over atmospheric fading channels, which are implemented based on the shared entangled states between the stations, the same concept is true when the quantum key rate is calculated. In fact, due to the relatively long coherence time of the atmospheric channel, it may be possible to devise a scheme, in which quantum key rates are derived for each realization of the fading (each fading bin realized), and summed [107]–[109], [186]. Indeed, the quantum key rate $K[\rho'(\eta)]$ resulting from the mixed Gaussian state $\rho'(\eta)$ can be calculated based on the covariance matrix of $\rho'(\eta)$, and then the total key rate shared between the stations is calculated by $K = \int_0^{\eta_0} p(\eta)\, K[\rho'(\eta)]\, d\eta$ [107]–[109].

[20] Note that in [185], a fast-fading channel has been considered where the users are only able to estimate the probability distribution of the channel's transmission coefficient but not its instantaneous values, while the eavesdropper has full control of the fast-fading channel, so that she chooses the instantaneous transmission coefficient of the channel.

Similarly, considering this scenario in the two-mode transfer setting, where the transmission coefficients η_1 and η_2 are measured at the two receiving stations, the final grade of entanglement can be calculated as [107]

$$E = \int_0^{\eta_{01}} \int_0^{\eta_{02}} p_1(\eta_1) p_2(\eta_2) E[\hat{\rho}'(\eta_1, \eta_2)] \, d\eta_1 \, d\eta_2, \quad (45)$$

where $E[\hat{\rho}'(\eta_1, \eta_2)]$ is the entanglement of a state that has traversed two channels having the transmission coefficients of η_1 and η_2 [107]–[109].

D. Enhancement of Quantum Communication Performance

Satellite-based communication channels tend to suffer from high uplink losses on the order of 25-30 dB (and beyond) for a LEO satellite receiver [40], [52], [145], while single downlink channels are anticipated to have losses of 5-10 dB for a LEO satellite transmitter [40], [52], [145]. Under such high losses, entanglement distribution and QKD via satellite will remain a fruitless endeavor without the beneficial intervention of the post-selection strategy [102] and entanglement distillation techniques [184] detailed below.

1) Post-Selection: Although atmospheric fading degrades both the entanglement and the quantum key rate, its effects may be mitigated. Post-selection of high transmission-coefficient windows, as introduced in [102] for the case of a single point-to-point fading channel, is capable of improving both the entanglement and the quantum key rate. To elaborate a little further, in the post-selection strategy, a subset of the channel transmittance distribution, namely that associated with the high transmission coefficient, is selected to contribute to the resultant post-selected state and to the post-selected key rate.

To elaborate on the post-selection strategy, in addition to the quantum states, coherent (classical) light pulses are transmitted through the channel in order to estimate the channel's transmission coefficient η at the receiver. The received quantum state is either retained or discarded, conditioned on the channel's transmission coefficient being higher or lower than the post-selection threshold η_{th}. Although this post-selection strategy can be invoked for enhancing the grade of entanglement and the quantum key rate between the transmitter and receiver, estimation of the channel's transmission coefficient will impose additional complexity on both the transmitter and receiver. The operation of this form of post-selection in the scheme (c) of Fig. 21 has been invoked in [105] for enhancing the grade of Gaussian entanglement and in [106] for increasing the quantum key rates between the ground stations.

2) Entanglement Distillation: The other strategy, which can be used in order to enhance the grade of entanglement between the transmitter and receiver is entanglement distillation that is based on quantum measurement techniques without relying on channel estimation. Entanglement distillation represents the protocol of extracting a subset of states with a higher degree of entanglement from an ensemble of entangled states [187]. In fact, entanglement distillation may be viewed as a purifying protocol that selects highly entangled pure states from a set of entangled states that have become mixed as a result of imperfect transmission [188]–[191]. It has been shown that if the entangled states are Gaussian, entanglement distillation cannot be performed using only Gaussian operations carried out by linear optical components, such as beam splitters and phase shifters, homodyne detection and classical communication [192]–[194]. However, when the Gaussian entangled states are transmitted through a fading channel, the state at the output of the channel is a non-Gaussian mixed state (a non-Gaussian mixture of Gaussian states), and therefore the aforementioned no-go theorem does not apply. In [184], a method has been proposed for distilling entanglement from (initially) Gaussian entangled states received over a single point-to-point fading channel. This is achieved by carrying out a weak measurement (based on a beam splitter and a homodyne detector) applied to the received non-Gaussian mixed state. The entanglement distillation is implemented at the receiver by extracting a small portion of the received mixed state using a tap beam splitter. A single quadrature (for instance, the $\hat{q}$ quadrature) is then measured by applying homodyne detection to the tapped beam. If the measurement outcome is above the threshold value q_{th}, then the remaining state is retained, otherwise it is discarded. The operation of this form of entanglement distillation in the scheme (c) of Fig. 21 has been invoked in [105] for enhancing the Gaussian entanglement between the ground stations (which consequently leads to an improvement in the quantum key rates of the EB CV-QKD protocols).

Note that when entangled states are conveyed over a fading channel, both the above-mentioned post-selection and entanglement distillation strategies act as "Gaussification" methods in the sense that the resultant conditioned states approach a Gaussian form due to the enhanced concentration of low-loss states in the final ensemble-averaged state. Note also that using the above-mentioned post-selection and entanglement distillation strategies, the entanglement established between the transmitter and receiver is only probabilistically increased.

Another entanglement distillation technique is based on applying an initial non-Gaussian operation to the Gaussian entangled states (that again increases the entanglement probabilistically), which is followed by a Gaussification step that iteratively drives the output non-Gaussian state towards a Gaussian state. Non-deterministic noiseless linear amplification has been identified as a method of distilling Gaussian entanglement [196] and [195], [197]–[203]. It has been shown that the non-deterministic noiseless linear amplification is capable of distilling improved CV entanglement [196], [199], [200] and enhancing CV-QKD performance [201]–[203], when applied after the lossy channel to the quantum states received. The non-Gaussian operations which result in the generation of non-Gaussian entangled states will be discussed in detail in the next section.

VII. Non-Gaussian CV Quantum Communication Over Atmospheric Channels

In the CV domain, previous efforts invested in entanglement distribution and QKD over atmospheric channels have been predominately focussed on Gaussian states [16], [98], [102], [103], [105], [106], [108], [110], [111]. Although Gaussian quantum states are well understood both from a theoretical and from an experimental perspective [86], [87], [114], the employment of CV non-Gaussian quantum states[21] for quantum communication has also garnered interest [204]–[224]. Non-Gaussian quantum states are valuable resource for a range of protocols, including teleportation [204]–[208], [212]–[214], cloning [222], [223] and CV-QKD protocols [219]–[221], [224]. For two important reasons, entangled non-Gaussian states are particularly interesting in the context of quantum communication via satellite. The first of these reasons is that the distillation of Gaussian entanglement is impossible using only Gaussian operations [192]–[194]. However, mixed non-Gaussian states can undergo entanglement distillation without any additional requirements. The second reason is that, relative to Gaussian entanglement, non-Gaussian entanglement can be shown in some circumstances to be more robust against decoherence [212], [217], [218].

A. Non-Gaussian Entangled States

CV non-Gaussian states are mostly generated by applying non-Gaussian operations, such as photon subtraction [204], [205], [207]–[210], [213], [214], photon addition [206], [207], [209], [211], [214] and photon replacement [212], [214] to incoming Gaussian states. We discuss here non-Gaussian entangled states which are created probabilistically by applying non-Gaussian operations to (i.e., at the receiver) Gaussian TMSV states. Note that a non-Gaussian operation can be applied to either a single mode, or to both modes, of the incoming Gaussian entangled state. Also note the non-Gaussian operation can be applied to the incoming mode at the sender (i.e., incoming from the local TMSV production site), or at the receiver side (after propagation through the atmosphere). Unless otherwise stated, we will consider the former process in the following.

For the generation of an entangled photon-subtracted squeezed (PSS) state [204], [205], [207]–[210], [213], [214], each mode of an incoming TMSV state interacts with a vacuum mode in a beam splitter. One of the outputs of each beam splitter feeds a photon number resolving detector. When both detectors simultaneously register k photons, which are considered to be non-Gaussian measurements, a pure non-Gaussian state is heralded with a probability of $0 < P_{sb} < 1$. This photon-subtraction operation is shown in Fig. 23(a) for $k = 1$. A PSS state can also be generated by applying the photon subtraction technique described above to a single mode of the TMSV state [214]. The generation of non-Gaussian states via photon subtraction as described above has been experimentally demonstrated in [225]–[227]. Note that in the photon-subtraction operation, other types of photon detectors such as on/off photon detectors (which only distinguish the presence and absence of photons, and are considered a non-Gaussian measurement) can also be used for generating a PSS state from a TMSV state [205], [208]. In this case the non-Gaussian output state is a mixed state.

An entangled photon-added squeezed (PAS) state [206], [207], [209], [211], [214] is generated by adding a single photon to each mode of a TMSV state. This single-photon addition is performed at a beam splitter, as shown in Fig. 23(b), with one of the outputs of each beam splitter being detected by an on/off photon detector. A pure non-Gaussian state is then generated (with a probability of 0< P_{ab} <1) when a vacuum state is registered in both detectors simultaneously. Note that the final creation probability of a PAS state is obtained by multiplying P_{ab} by the probability of creating the two additional photons required. A PAS state can also be generated by applying the photon addition technique described above to a single mode of the TMSV state [214]. Note that the addition of single photons to coherent states and to thermal states of light has been experimentally realized in [228] and [229].

By contrast, an entangled photon-replaced squeezed (PRS) state [212], [214] is generated according to Fig. 23(c), where each mode of a TMSV state interacts with a single photon in a beam splitter, with one of the outputs of each beam splitter being detected by a photon number resolving detector. When both detectors register a single photon simultaneously, a pure non-Gaussian state is heralded with a probability of 0< P_{rb} <1. The final creation probability of a PRS state is obtained by multiplying P_{rb} by the probability of creating the two additional photons required. A PRS state can also be generated by applying the photon replacement process described above to a single mode of the TMSV state [214].

B. Evolution of Non-Gaussian Entangled States Over a Lossy Channel

Unlike Gaussian states, the evolution of non-Gaussian states cannot be analysed solely through the covariance matrix. Previous contributions have analysed the evolution of non-Gaussian states for transmission over fixed-attenuation channels relying on the so-called Master equation approach of [215], the characteristic function approach of [212] or the Kraus operator approach of [217]. Here we discuss the general approach of Kraus representation [230] of the channel in order to directly analyze the evolution of the entangled states (Gaussian or non-Gaussian) through the channel. Considering a quantum state associated with the density operator $\hat{\rho}_{in}$ as the input of a trace-preserving[22] completely positive channel, the output density operator of the channel can be described in an operator-sum representation of the form $\hat{\rho}_{out} = \sum_{\ell=0}^{\infty} G_\ell \hat{\rho}_{in} G_\ell^\dagger$, where the Kraus operators G_ℓ satisfy $\sum_{\ell=0}^{\infty} G_\ell \, G_\ell^\dagger = I$, with I being the identity operator. In [230], the Kraus operators of a wide range of channels including a fixed-attenuation channel subject to vacuum noise (i.e., $V_n = 1$ in Fig. 10) are given. In [217], the Kraus operators of a fixed-attenuation channel subject to vacuum noise but with additional Gaussian noise is given. The results of [230] have been generalized to a fixed-attenuation channel subject to thermal noise (i.e., $V_n > 1$ in Fig. 10) in [132].

[21] Note that only pure states having a positive Wigner function are Gaussian states. However, the Wigner function of non-Gaussian pure states takes on negative values.

[22] In a trace-preserving channel, the trace of the density operator is preserved, which means the trace of the output density operator of the channel remains one.

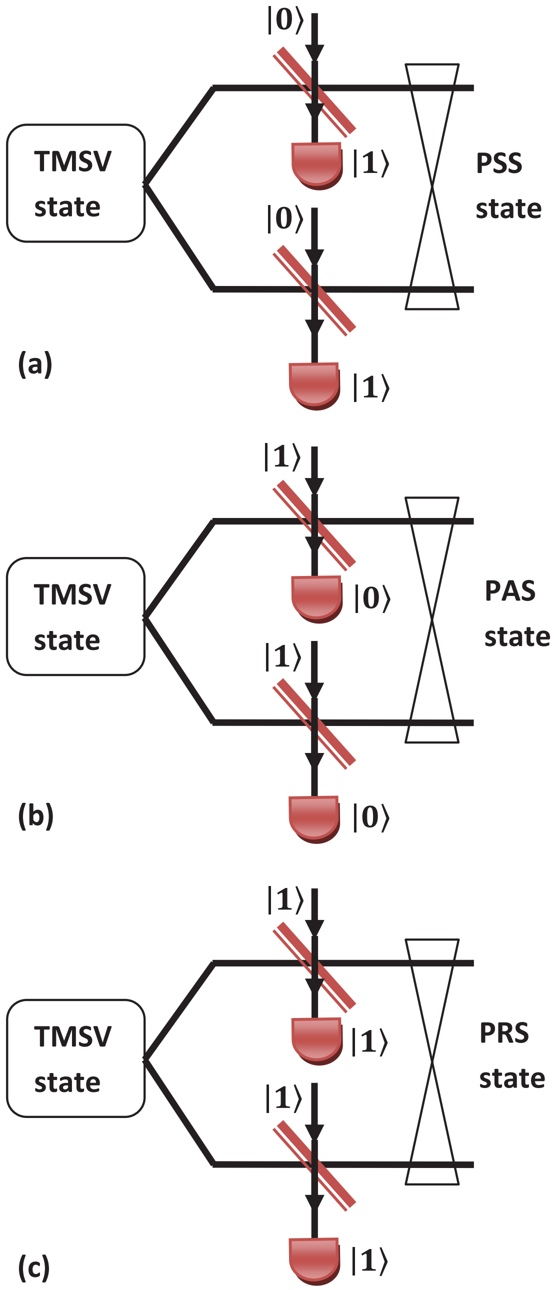


Fig. 23. Implementation of non-Gaussian operations on the Gaussian TMSV state. (a) Photon subtraction: each mode of the input TMSV state interacts with a vacuum mode in a beam splitter, with one output of the each beam splitter feeding a photon detector. If the two detectors simultaneously detect a single photon, a PSS state is heralded on the non-measured outputs. (b) Photon addition: each mode of the input TMSV state interacts with a single photon in a beam splitter, with one output of the each beam splitter feeding a photon detector. If the two detectors simultaneously detect vacuum state, a PAS state is heralded on the non-measured outputs. (c) Photon replacement: each mode of the input TMSV state interacts with a single photon in a beam splitter, with one output of the each beam splitter feeding a photon detector. If the two detectors simultaneously detect single photons, a PRS state is heralded on the non-measured outputs.

C. Entanglement Determination and Quantum Key Rate Computation

Following the evolution of pure non-Gaussian states over the lossy channel(s), the quantum state of the channel output is a non-Gaussian mixed state. In general it is not possible to analytically determine the total grade of entanglement of the mixed non-Gaussian states after transmission over a lossy channel. Since the grade of entanglement is determined by the output density operator $\hat{\rho}_{out}$, which possesses an infinite number of elements, a numerical method is required for approximating the matrix $\hat{\rho}_{out}$ by its truncated-dimensional version, as discussed in [107], [109], [132], and [205] whilst ensuring that the trace of the truncated matrix is close to 1.

Given the non-deterministic nature of the non-Gaussian operations, in the context of non-Gaussian entanglement distribution, there are two key performance indicators, namely the grade of entanglement E between two stations following the transmission of a pulse through the lossy channel(s), and the entanglement-generation rate R_E, where we have $R_E = P_c\, E$, with P_c being the creation probability of the initial non-Gaussian state. The evolution of a wide range of non-Gaussian entangled states in both single-mode and two-mode transfer over atmospheric fading channels has been investigated both when the transmission coefficient of the atmospheric fading channel is unknown and when it is estimated in real time [107]. The work of [107] considered operational scenarios where the non-Gaussian entangled states transmitted through the atmospheric channel are created "just-in-time" via non-Gaussian operations applied to the Gaussian entangled input states that would otherwise be transmitted directly over the communication channel. In this scenario transmitting the incoming Gaussian state directly over the atmospheric channel would be the best option in terms of maximizing the *entanglement-generation rate*. However, if the transmission rates of all the states through the channel could be equalized for example with the aid of quantum memory (see [107] for more details), some non-Gaussian states lead to enhanced *entanglement* transfer relative to that obtained by Gaussian state transfer.

The performance of CV-QKD protocols has been analysed in [109] for transmission over atmospheric fading channels, where the source is constituted by PSS states in the context of EB CV-QKD protocols. In [109], one mode of the PSS state remains at the ground station (satellite), while the other photon-subtracted mode is transmitted to the satellite (ground station) over the fading uplink (downlink) channel characterized by the probability distribution $p(\eta)$ and maximum transmission coefficient of η_0. When the transmission coefficient of the atmospheric channel can be measured in real time, after acquiring each realization of η, the key rate $K(\eta)$ is calculated based on the covariance matrix of the mixed non-Gaussian state at the output of the channel. The final key rate is then computed as $K = P_c \int_0^{\eta_0} K(\eta) p(\eta)\, d\eta$ in units of bits per pulse, with P_c being the creation probability of the initial non-Gaussian entangled state. The resultant key rate represents a lower bound on the actual key rate of the CV-QKD protocol. However, to determine the actual resultant key rates (not just its lower bounds), $K(\eta)$ must be computed based on the density operator of the mixed non-Gaussian output state.

In [107] and [109] the non-Gaussian operations are first applied to the initial Gaussian states, with the resultant non-Gaussian states being transmitted through the atmospheric fading channel. An alternative approach would be to transmit the initial Gaussian states through the atmospheric channel, and then apply the non-Gaussian operations after the atmospheric channel to the quantum states received. In [212], the distillation of CV entanglement using a coherent superposition-based non-Gaussian operation has been studied, where the non-Gaussian operation is the superposition of the photon subtraction and of the photon addition operations, and where the non-Gaussian operation is applied either before or after a fixed-attenuation channel.

VIII. Comparison With Discrete-Variable Technologies

The family of DV systems invoked for satellite-based quantum communications constitutes an alternative technology, which has been deployed in Micius [66]–[68]. In space-based deployment, a range of pragmatic issues comes into play when considering the pros and cons of DV *vs.* CV implementations. Perhaps the strongest argument in favour of DV systems in the space-based context is that photon losses have a less grave impact on quantum information processing in DV systems. In CV systems the photon losses in the channel introduce vacuum noise, leading to a reduction in the correlation between Alice and Bob's data. By contrast, in DV systems, photon losses reduce the communication efficiency, but they do not trigger a false single-photon detection event. A photon is either lost in the channel, in which case Bob does not register anything, or it is simply detected at Bob's detector. In high-loss scenarios, this effect can lead to advantages for DV systems. However, this benefit may by outweighed by other considerations, as discussed briefly below. More details on satellite-based DV quantum communication can be found elsewhere, for example in [40].

The performance of DV-QKD [231] is limited both by the difficulty of single-photon generation, as well as by the expense of single-photon detectors. It is a challenge to construct a true single-photon source owing to implementation challenges. Alternatively, single-photon sources can be approximated using an attenuated laser (weak coherent state pulses) [232], [233]. By contrast, CV-QKD systems rely on low-cost implementations and are potentially capable of supporting higher key rates than DV-QKD systems. Recall that CV-QKD can be implemented by modulating both the amplitude and phase quadratures of a coherent laser and can be subsequently measured in the receivers using homodyne detectors, which operate faster and more efficiently than the single-photon detectors. Moreover, CV-QKD systems are more compatible with standard telecommunication encoding, transmission and detection techniques. All these advantages potentially allow CV-QKD protocols to achieve higher secret key rates than DV-QKD systems.

Furthermore, the single-photon detectors of DV systems are very sensitive to background light sources. By contrast, the homodyne detectors used for CV systems offer beneficial robustness to background light. Indeed, an explicit advantage of using a local oscillator is that it has an 'automatic' spectral-domain filtering effect. Consequently, homodyne detectors remain to a large extent unimpaired in daylight conditions without the extra filtering that are needed by the single-photon detectors [16]. Furthermore, in CV systems, a tapped component of the local oscillator can be simply obtained and measured, thereby allowing for *direct* monitoring of atmospheric fluctuations effects, such as beam wandering (which can then be compensated for using adaptive optics [16], [98], [110]).

TABLE VI
Comparison of DV-QKD and CV-QKD

	DV-QKD	**CV-QKD**
Preparation	• Difficult to implement	• Low-cost implementation
Channel	• Photon losses do not trigger false detection events	•Photon losses introduce vacuum noise
Measurement	• Expensive • Sensitive to background light	•Low-cost implementation • Robust to background light • Efficient (high key rates) • Facilitates FSO channel estimation
Performance	• Generates higher key rates in high-loss channels	• Generates higher key rates in low-loss channels

Both DV and CV-QKD systems have protocols which are able to generate unconditional secure key [76]. However, the performance of QKD systems can be evaluated in terms of the generation "rate" of the final secure key. Due to the fact that the impact of photon losses on QKD performance is different for DV and CV systems (as discussed earlier), for low-loss channels where CV-QKD is secure (i.e., generates positive key rates), the key rate generated from CV-QKD can be higher than the key rate from DV-QKD [163] (due to the use of faster and more efficient transmission and detection technology in CV-QKD systems). However, for high-loss (and noisy) channels where CV-QKD is not secure (i.e., not able to generate positive key rates), DV-QKD can be secure, and generate positive key rates. Thus, the secure transmission range (or the maximum transmission distance) of DV-QKD systems can be higher than CV-QKD systems.

Table VI summarizes the pros and cons of DV-QKD and CV-QKD. Nonetheless, the issue of whether DV or CV systems should be deployed as the quantum information carrier in space-based quantum communications remains very much an open issue at the time of writing. Ultimately, it could well be that hybrid DV+CV architectures, accommodating time-variant atmospheric conditions, turn out to be the most beneficial in many circumstances. The employment of such hybrid architectures has been extensively studied for example in [234].

IX. Future Directions

Quantum communication via satellite is in its infancy. Building on the early work and verification studies (both experimental and theoretical) of many researchers, e.g., [16], [32]–[69], [78], [79], [93]–[112], [235], and [236] the pioneering experimental result of the Micius [66]–[68] collaboration has now provided us with the first glimpse of what is truly achievable via space-based platforms. However, there remains much to do before quantum communications via satellites can be considered mainstream. This is especially so in the CV quantum domain, where no space-based deployments have yet been achieved, despite the numerous theoretical studies, e.g., [16] and [98]–[111]. We briefly mention here some of the research topics within space-based CV quantum communications that we consider of particular interest to any multi-disciplinary engineering community.

A. Channel Transmissivity Measurements

The Micius [66]–[68] data provides us with our first real insight into the channel conditions experienced by quantum states, as they traverse through the turbulent atmosphere, to and from Earth. The measured photonic losses in the downlink [66], [67] and in the uplink [68] are now available (the losses in the latter case were a minimum of 41 dB). Leveraging this data for better understanding the channel conditions experienced by CV states as they travel to and from Earth would be an insightful, but costly endeavour. As discussed earlier in Section VIII, the loss of photons in the CV context fundamentally affects any subsequent information processing, as opposed to the DV case, where photons not received can be simply ignored. Ultimately, the study of how the CV states are affected by the atmosphere reduces to a determination of the statistical distribution of the channel transmissivity. Detailed knowledge of this distribution has wide ranging implications for studies pertaining to non-classical signatures of CV states traversing through atmospheric channels [104], as well as for a host of CV-based applications. The latter outcome is due to the fact that many applications are very sensitive to the channel's transmissivity [105]–[109]. As discussed previously, beyond the dominant effects of beam wandering and beam broadening, other more subtle effects induced by the atmosphere can play a non-negligible role. These effects include beam deformation, attenuation, absorption and scattering. Sophisticated theoretical studies of these effects are now becoming available, and in general these models are found to be consistent with terrestrial experiments carried out over a wide range of turbulence conditions [101], [237], [238]. Experimental confirmations of existing turbulence models in the realm of Earth-to-satellite (and vice versa) channels would be very important. Of particular importance would be a robust validation of the beam-wandering models used for the transmissivity statistics in the Earth-to satellite channels [100]–[102], and the validation of the beam-broadening models expected to dominate the satellite-to-Earth channels [57].

B. Error Reconciliation

The reconciliation phase of any QKD protocol is perhaps the area of quantum communications most closely associated with classical communications. In the DV scenario, long LDPC codes can be used to correct transmission errors. For scenarios, where DV quantum measurements are mapped directly to binary outcomes, the transmission of bits via a classical binary symmetric channel can be adopted as the underlying model. A range of high-performance LDPC codes which approach reconciliation factors close to 1 in the large key length limit are known for such channels [239]–[241]. However, in the CV setting the extraction of binary information is substantially more involved. Currently, there are two main techniques that are widely adopted in this regard, namely, slice reconciliation [20], [242], and multi-dimensional reconciliation [24], [243]. For the low signal to noise ratios (SNRs) routinely anticipated for satellite communications, the multi-dimensional reconciliation technique is likely to be more appropriate. In this context, multi-dimensional reconciliation via multi-edge LDPC codes is considered by many as the most appropriate path due to the high performance of such codes at low SNRs [24].

Nonetheless, numerous open research issues remain. Perhaps the most important of these is constituted by the finite key effects. Much of the work in formally determining the security of a key within QKD systems assumes having an infinite key length. However, in reality, this assumption is never satisfied and the consideration of the finite-length key effects must be analysed. This is an issue that affects both the DV [244] and CV security analyses [181], [245]–[248]. This problem is of particular concern for space-based QKD due to the short transit times of LEO satellites. Hence, the finite-length key processing invoked in the context of CV-QKD conceived for satellites has to be considered. Naturally, this analysis will be strongly dependent on the specific CV-QKD protocol adopted. Finite-length key based analyses of standard coherent state protocols [249], of MDI protocols [250], [251] and of full device-independent protocols [252] follow quite distinct paths.

Beyond the finite-length effects within the reconciliation decoding phase, the construction of near-capacity adaptive-rate LDPC codes for CV space-based implementations would be useful. Again, these issues are particularly relevant to satellite-based communication due to the time-variant properties of the channel. For LEO satellites we can expect the SNR to exhibit quite rapid variations versus time, as the satellite appears above the horizon and disappears again. Furthermore, for a given set of orbital parameters, we could anticipate the SNR's evolution versus time to be reasonably predictable. Adaptive-rate LDPC codes well suited for counteracting the SNR vs time evolution should be constructed. The employment of puncturing techniques [253] used for multi-edge LDPC codes appears to be an appropriate pathway to achieving this [254]. These studies are only in their early phases of development, hence further research into the design of adaptive-rate codes as a path to low-complexity CV-QKD via satellites is expected to be fruitful. An important focus of such future studies should be the maintenance of high reconciliation efficiencies over the anticipated range of SNRs [255].

Finally, we note that in principle other codes beyond LDPC codes could be used in the CV-QKD reconciliation phase. Currently, however, limited work has been reported in this area. Nonetheless, we do note some work on turbo codes [256] applied to the CV domain, as reported in [257] (for use of such codes in the DV domain see [258], [259]). Furthermore, polar codes [260] have recently been invoked for CV-QKD in [261]. These contributions suggest that further performance comparisons using various error correction codes for the CV-QKD reconciliation phase may become fruitful.

C. CV Quantum Error Correction Codes

Of special importance for CV quantum communications are the non-Gaussian operations that form the basis of quantum error correction. Such operations are required due to the no-go theorem, stipulating that Gaussian errors cannot be corrected by purely Gaussian operations [262]. It is possible to build a pathway from standard classical LDPC codes to qubit error correction codes, and then to CV error correction codes. Following on from the original CV error correction protocols of [263]–[265], there are several examples of CV quantum error correction codes appearing in [197] and [266]–[272]. However, in the context of space-based implementations there is evidence to suggest that direct non-Gaussian measurement at the receiver is likely to be the most fruitful pathway to CV error correction - at least in the short term.

In Section VII-A we have discussed a host of non-Gaussian operations in the form of photon subtraction and addition techniques that were used to form our non-Gaussian states, as seen in Fig. 23. Such operations can also be used for producing CV entanglement distillation - a form of quantum error correction for CV variables. Photon subtraction and addition techniques are becoming mainstream in laboratories throughout the world and the imminent integration of such techniques directly into future satellite communications is expected. In QKD implementations though, a balance must be struck between the relatively low probabilities of success for the subtraction/addition operations required and the resultant degradation of the key rates. More detailed studies of these design options for space-based communications are warranted.

D. The Interface With Classical Terrestrial Networks

Although fundamentally a breakthrough, the birth of space-based quantum communications can be seen from a more pragmatic perspective - it will allow for the creation of the global "Quantum Internet". This new Internet will interconnect a vast range of devices, from mobile devices all the way through to the much anticipated quantum computers. These devices will be able to transfer quantum information and communicate with each other in an unconditionally secure manner. Importantly, this new network will consist of not only quantum communication channels but also of classical communication channels. As such, consideration of how best to accommodate integration of the quantum information received via satellites into a wider integrated network will be required. Currently, very little detailed thought has been given to this ambitious enterprise, and therefore there is much opportunity for high-impact future research in the context of the integrated system-oriented vision of Fig. 1.

In the CV setting, perhaps the integration of CV quantum information into the microwave setting is the most important example. The implementation of quantum communication protocols in the optical frequency domain is usually preferred, which is an explicit benefit of the negligible background thermal radiation at optical frequencies, hence all of our discussions have been in this domain. However, the advent of super-conducting microwave quantum circuits have led to an increasing interest in the implementation of quantum communication protocols in the microwave regime [129]–[131], [273]–[279]. These interests are further fuelled by advances in macro electro-optomechanical resonators that are capable of coupling quantum information with the microwave-optical interface [276], [278], [279]. With the advent of this technology, quantum information created via super-conducting circuits may be readily upconverted to the optical regime for direct transfer to an overhead satellite. The satellite could then communicate that information optically to a second terrestrial receiver with subsequent conversion back to the microwave regime for storage, error correction or further information processing. Such a scenario could well represent how future quantum computers will share information globally through the quantum Internet. We also note that it is even possible to directly transmit quantum information via microwave carriers to nearby wireless receivers [132]. The development of such integration techniques for the quantum Internet is still in its infancy.

X. Conclusion

We have discussed the recent research advances that are most relevant to CV quantum communication via low-Earth-orbit satellites. Recent experimental results gleaned from the Micius satellite on a range of DV-based quantum communication protocols indicate that CV quantum communication via large distances over the ether has become entirely plausible. We have outlined many of the technical advances in the field of CV quantum communication encompasses and highlighted a range of technical challenges it faces. As compared to the DV technology, CV systems bring with them the compelling benefit of inherent compatibility with the state-of-the-art optical technology. Explicitly, while DV sources and detectors are difficult to implement and expensive, CV systems can be easily implemented with the aid of off-the-shelf lasers and homodyne (or heterodyne) detectors. Hence, the many advantages of this intriguing technology warrant its experimental deployment to make the vision of the perfectly secure future quantum-communications scenario portrayed in Fig. 1 a reality.

Our hope is valued Colleague that you would join this community-effort...

References

[1] L. Hanzo *et al.*, "Wireless myths, realities, and futures: From 3G/4G to optical and quantum wireless," *Proc. IEEE*, vol. 100, pp. 1853–1888, May 2012.

[2] P. Botsinis, S. X. Ng, and L. Hanzo, "Quantum search algorithms, quantum wireless, and a low-complexity maximum likelihood iterative quantum multi-user detector design," *IEEE Access*, vol. 1, pp. 94–122, 2013.

[3] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput. Syst. Signal Process.*, Bengaluru, India, 1984, pp. 175–179.

[4] C. H. Bennett *et al.*, "Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels," *Phys. Rev. Lett.*, vol. 70, no. 13, pp. 1895–1899, 1993.

[5] L. Vaidman, "Teleportation of quantum states," *Phys. Rev. A*, vol. 49, no. 2, pp. 1473–1476, 1994.

[6] A. Furusawa *et al.*, "Unconditional quantum teleportation," *Science*, vol. 282, no. 5389, pp. 706–709, 1998.

[7] P. van Loock and S. L. Braunstein, "Unconditional teleportation of continuous-variable entanglement," *Phys. Rev. A*, vol. 61, no. 1, 1999, Art. no. 010302.

[8] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge, U.K.: Cambridge Univ. Press, 2000.

[9] S. L. Braunstein and P. van Loock, "Quantum information with continuous variables," *Rev. Mod. Phys.*, vol. 77, no. 2, pp. 513–577, Jun. 2005.

[10] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Phys. Rev. Lett.*, vol. 68, no. 21, pp. 3121–3124, May 1992.

[11] T. C. Ralph, "Continuous variable quantum cryptography," *Phys. Rev. A*, vol. 61, Dec. 1999, Art. no. 010303(R).

[12] N. J. Cerf, M. Lévy, and G. Van Assche, "Quantum distribution of Gaussian keys using squeezed states," *Phys. Rev. A*, vol. 63, no. 5, 2001, Art. no. 052311.

[13] F. Grosshans and P. Grangier, "Reverse reconciliation protocols for quantum cryptography with continuous variables," in *Proc. 6th Int. Conf. Quantum Commun. Meas. Comput.*, 2002.

[14] F. Grosshans *et al.*, "Quantum key distribution using Gaussian-modulated coherent states," *Nature*, vol. 421, pp. 238–241, Jan. 2003.

[15] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, "Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables," *Quantum Inf. Comput.*, vol. 3, no. 7, pp. 535–552, 2003.

[16] D. Elser *et al.*, "Feasibility of free space quantum key distribution with coherent polarization states," *New J. Phys.*, vol. 11, no. 4, 2009, Art. no. 045014.

[17] A. A. Semenov, F. Töppel, D. Y. Vasylyev, H. V. Gomonay, and W. Vogel, "Homodyne detection for atmosphere channels," *Phys. Rev. A*, vol. 85, no. 1, 2012, Art. no. 013826.

[18] C. Croal *et al.*, "Free-space quantum signatures using heterodyne measurements," *Phys. Rev. Lett.*, vol. 117, no. 10, 2016, Art. no. 100503.

[19] P. A. Hiskett *et al.*, "Long-distance quantum key distribution in optical fibre," *New J. Phys.*, vol. 8, Sep. 2006, Art. no. 193.

[20] J. Lodewyck *et al.*, "Quantum key distribution over 25 km with an all-fiber continuous-variable system," *Phys. Rev. A*, vol. 76, no. 4, 2007, Art. no. 042305.

[21] B. Qi, L.-L. Huang, L. Qian, and H.-K. Lo, "Experimental study on the Gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers," *Phys. Rev. A*, vol. 76, no. 5, 2007, Art. no. 052323.

[22] D. Rosenberg *et al.*, "Practical long-distance quantum key distribution system using decoy levels," *New J. Phys.*, vol. 11, Apr. 2009, Art. no. 045009.

[23] Q. D. Xuan, Z. Zhang, and P. L. Voss, "A 24 km fiber-based discretely signaled continuous variable quantum key distribution system," *Opt. Exp.*, vol. 17, no. 26, pp. 24244–24249, 2009.

[24] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, "Experimental demonstration of long-distance continuous-variable quantum key distribution," *Nat. Photon.*, vol. 7, no. 5, pp. 378–381, 2013.

[25] D. Huang, P. Huang, D. Lin, and G. Zeng, "Long-distance continuous-variable quantum key distribution by controlling excess noise," *Sci. Rep.*, vol. 6, Jan. 2016, Art. no. 19201.

[26] H. Takesue *et al.*, "Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors," *Nat. Photon.*, vol. 1, no. 6, pp. 343–348, 2007.

[27] D. Stucki *et al.*, "High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres," *New J. Phys.*, vol. 11, no. 7, 2009, Art. no. 075003.

[28] H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nat. Photon.*, vol. 8, pp. 595–604, Jul. 2014.

[29] B. Korzh *et al.*, "Provably secure and practical quantum key distribution over 307 km of optical fibre," *Nat. Photon.*, vol. 9, no. 3, pp. 163–168, 2015.

[30] H.-L. Yin *et al.*, "Measurement-device-independent quantum key distribution over a 404 km optical fiber," *Phys. Rev. Lett.*, vol. 117, no. 19, 2016, Art. no. 190501.

[31] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, "Quantum repeaters: The role of imperfect local operations in quantum communication," *Phys. Rev. Lett.*, vol. 81, pp. 5932–5935, Dec. 1998.

[32] C.-Z. Peng *et al.*, "Experimental free-space distribution of entangled photon pairs over 13 km: Towards satellite-based global quantum communication," *Phys. Rev. Lett.*, vol. 94, no. 15, 2005, Art. no. 150501.

[33] K. J. Resch *et al.*, "Distributing entanglement and single photons through an intra-city, free-space quantum channel," *Opt. Exp.*, vol. 13, no. 1, pp. 202–209, 2005.

[34] I. Marcikic, A. Lamas-Linares, and C. Kurtsiefer, "Free-space quantum key distribution with entangled photons," *Appl. Phys. Lett.*, vol. 89, no. 10, 2006, Art. no. 101122.

[35] C. Erven, C. Couteau, R. Laflamme, and G. Weihs, "Entangled quantum key distribution over two free-space optical links," *Opt. Exp.*, vol. 16, no. 21, pp. 16840–16853, 2008.

[36] S. Nauerth *et al.*, "Air-to-ground quantum communication," *Nat. Photon.*, vol. 7, no. 5, pp. 382–386, 2013.

[37] J.-Y. Wang *et al.*, "Direct and full-scale experimental verifications towards ground-satellite quantum key distribution," *Nat. Photon.*, vol. 7, no. 5, pp. 387–393, 2013.

[38] J.-P. Bourgoin *et al.*, "Free-space quantum key distribution to a moving receiver," *Opt. Exp.*, vol. 23, no. 26, pp. 33437–33447, 2015.

[39] D. E. Bruschi, T. C. Ralph, I. Fuentes, T. Jennewein, and M. Razavi, "Spacetime effects on satellite-based quantum communications," *Phys. Rev. D*, vol. 90, no. 4, 2014, Art. no. 045041.

[40] R. Bedington, J. M. Arrazola, and A. Ling, "Progress in satellite quantum key distribution," *npj Quantum Inf.*, vol. 3, Aug. 2017, Art. no. 30.

[41] J. M. P. Armengol *et al.*, "Quantum communications at ESA: Towards a space experiment on the ISS," *Acta Astronautica*, vol. 63, nos. 1–4, pp. 165–178, 2008.

[42] T. Scheidl, E. Wille, and R. Ursin, "Quantum optics experiments using the international space station: A proposal," *New J. Phys.*, vol. 15, no. 4, 2013, Art. no. 043008.

[43] T. Jennewein *et al.*, "QEYSSAT: A mission proposal for a quantum receiver in space," in *Proc. SPIE*, vol. 8997. San Francisco, CA, USA, 2014, Art. no. 89970A.

[44] H. Xin, "Chinese academy takes space under its wing," *Science*, vol. 332, no. 6032, p. 904, 2011.

[45] R. Ursin *et al.*, "Space-quest, experiments with quantum entanglement in space," *Europhys. News*, vol. 40, no. 3, pp. 26–29, 2009.

[46] T. Jennewein and B. Higgins, "The quantum space race," *Phys. World*, vol. 26, no. 3, pp. 52–56, 2013.

[47] P. Villoresi *et al.*, "Experimental verification of the feasibility of a quantum channel between space and Earth," *New J. Phys.*, vol. 10, no. 3, 2008, Art. no. 033038.

[48] J. Yin *et al.*, "Experimental quasi-single-photon transmission from satellite to earth," *Opt. Exp.*, vol. 21, no. 17, pp. 20032–20040, 2013.

[49] G. Vallone *et al.*, "Experimental satellite quantum communications," *Phys. Rev. Lett.*, vol. 115, no. 4, 2015, Art. no. 040502.

[50] M. Er-Long *et al.*, "Background noise of satellite-to-ground quantum key distribution," *New J. Phys.*, vol. 7, no. 1, 2005, Art. no. 215.

[51] J. G. Rarity, P. R. Tapster, P. M. Gorman, and P. Knight, "Ground to satellite secure key exchange using quantum cryptography," *New J. Phys.*, vol. 4, no. 1, 2002, Art. no. 82.

[52] M. Aspelmeyer, T. Jennewein, M. Pfennigbauer, W. R. Leeb, and A. Zeilinger, "Long-distance quantum communication with entangled photons using satellites," *IEEE J. Sel. Topics Quantum Electron.*, vol. 9, no. 6, pp. 1541–1551, Nov./Dec. 2003.

[53] C. Bonato *et al.*, "Influence of satellite motion on polarization qubits in a space-earth quantum communication link," *Opt. Exp.*, vol. 14, no. 21, pp. 10050–10059, 2006.

[54] C. Bonato, A. Tomaello, V. D. Deppo, G. Naletto, and P. Villoresi, "Feasibility of satellite quantum key distribution," *New J. Phys.*, vol. 11, Apr. 2009, Art. no. 045017.

[55] A. Tomaello, C. Bonato, V. Da Deppo, G. Naletto, and P. Villoresi, "Link budget and background noise for satellite quantum key distribution," *Adv. Space Res.*, vol. 47, no. 5, pp. 802–810, 2011.

[56] E. Meyer-Scott *et al.*, "How to implement decoy-state quantum key distribution for a satellite uplink with 50-db channel loss," *Phys. Rev. A*, vol. 84, Dec. 2011, Art. no. 062326.

[57] J.-P. Bourgoin *et al.*, "A comprehensive design and performance analysis of low earth orbit satellite quantum communication," *New J. Phys.*, vol. 15, no. 2, 2013, Art. no. 023006.

[58] L. Moli-Sanchez, A. Rodriguez-Alonso, and G. Seco-Granados, "Performance analysis of quantum cryptography protocols in optical earth-satellite and intersatellite links," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 9, pp. 1582–1590, Dec. 2009.

[59] Z. Yan *et al.*, "Novel high-speed polarization source for decoy-state BB84 quantum key distribution over free space and satellite links," *J. Lightw. Technol.*, vol. 31, no. 9, pp. 1399–1408, May 1, 2013.

[60] C. Cheng, R. Chandrasekara, Y. C. Tan, and A. Ling, "Space-qualified nanosatellite electronics platform for photon pair experiments," *J. Lightw. Technol.*, vol. 33, no. 23, pp. 4799–4804, Dec. 1, 2015.

[61] B. Qi *et al.*, "A compact readout electronics for the ground station of a quantum communication satellite," *IEEE Trans. Nucl. Sci.*, vol. 62, no. 3, pp. 883–888, Jun. 2015.

[62] L. Bacsardi, "On the way to quantum-based satellite communication," *IEEE Commun. Mag.*, vol. 51, no. 8, pp. 50–55, Aug. 2013.

[63] L. Bacsardi, "Satellite communication over quantum channel," *Acta Astronautica*, vol. 61, nos. 1–6, pp. 151–159, 2007.

[64] Z. Tang *et al.*, "Generation and analysis of correlated pairs of photons aboard a nanosatellite," *Phys. Rev. Appl.*, vol. 5, no. 5, 2016, Art. no. 054022.

[65] H. Takenaka *et al.*, "Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite," *Nat. Photon.*, vol. 11, no. 8, pp. 502–508, 2017.

[66] S.-K. Liao *et al.*, "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, no. 7670, pp. 43–47, 2017.

[67] J. Yin *et al.*, "Satellite-based entanglement distribution over 1200 kilometers," *Science*, vol. 356, no. 6343, pp. 1140–1144, 2017.

[68] J.-G. Ren *et al.*, "Ground-to-satellite quantum teleportation," *Nature*, vol. 549, pp. 70–73, Sep. 2017.

[69] K. Boone *et al.*, "Entanglement over global distances via quantum repeaters with satellite links," *Phys. Rev. A*, vol. 91, no. 5, 2015, Art. no. 052325.

[70] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[71] G. S. Vernam, "Cipher printing telegraph systems: For secret wire and radio telegraphic communications," *J. Amer. Inst. Elect. Eng.*, vol. 45, pp. 109–115, Jan. 1926.

[72] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, pp. 802–803, Oct. 1982.

[73] D. Dieks, "Communication by EPR devices," *Phy. Lett. A*, vol. 92, no. 6, pp. 271–272, 1982.

[74] R. Renner, "Security of quantum key distribution," Ph.D. dissertation, ETH Zurich, Zürich, Switzerland, 2005.

[75] R. Renner, N. Gisin, and B. Kraus, "Information-theoretic security proof for quantum-key-distribution protocols," *Phys. Rev. A*, vol. 72, no. 1, 2005, Art. no. 012332.

[76] V. Scarani *et al.*, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, pp. 1301–1350, Sep. 2009.

[77] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145–195, 2002.

[78] R. Ursin *et al.*, "Entanglement-based quantum communication over 144km," *Nat. Phys.*, vol. 3, no. 7, pp. 481–486, 2007.

[79] T. Schmitt-Manderbach *et al.*, "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km," *Phys. Rev. Lett.*, vol. 98, no. 1, 2007, Art. no. 010504.

[80] L. S. Madsen, V. C. Usenko, M. Lassen, R. Filip, and U. L. Andersen, "Continuous variable quantum key distribution with modulated entangled states," *Nat. Commun.*, vol. 3, Sep. 2012, Art. no. 1083.

[81] S. Pirandola and S. Mancini, "Quantum teleportation with continuous variables: A survey," *Laser Phys.*, vol. 16, no. 10, pp. 1418–1438, 2006.

[82] S. Pirandola, J. Eisert, C. Weedbrook, A. Furusawa, and S. L. Braunstein, "Advances in quantum teleportation," *Nat. Photon.*, vol. 9, pp. 641–652, Sep. 2015.

[83] G. Adesso and F. Illuminati, "Entanglement in continuous-variable systems: Recent advances and current perspectives," *J. Phys. A Math. Theor.*, vol. 40, no. 28, pp. 7821–7880, 2007.

[84] N. Gisin and R. Thew, "Quantum communication," *Nat. Photon.*, vol. 1, pp. 165–171, Mar. 2007.

[85] U. L. Andersen, G. Leuchs, and C. Silberhorn, "Continuous-variable quantum information processing," *Laser Photon. Rev.*, vol. 4, pp. 337–354, Apr. 2010.

[86] X.-B. Wang, T. Hiroshima, A. Tomita, and M. Hayashi, "Quantum information with Gaussian states," *Phys. Rep.*, vol. 448, nos. 1–4, pp. 1–111, 2007.

[87] C. Weedbrook *et al.*, "Gaussian quantum information," *Rev. Mod. Phys.*, vol. 84, pp. 621–669, May 2012.

[88] H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nat. Photon.*, vol. 8, pp. 595–604, Jul. 2014.

[89] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," *npj Quantum Inf.*, vol. 2, Nov. 2016, Art. no. 16025.

[90] M. Peev *et al.*, "The SECOQC quantum key distribution network in Vienna," *New J. Phys.*, vol. 11, Jul. 2009, Art. no. 075001.

[91] M. Sasaki *et al.*, "Field test of quantum key distribution in the Tokyo QKD network," *Opt. Exp.*, vol. 19, no. 11, pp. 10387–10409, 2011.

[92] B. Fröhlich *et al.*, "A quantum access network," *Nature*, vol. 501, pp. 69–72, Sep. 2013.

[93] T. Scheidl *et al.*, "Feasibility of 300 km quantum key distribution with entangled states," *New J. Phys.*, vol. 11, Aug. 2009, Art. no. 085002.

[94] A. Fedrizzi *et al.*, "High-fidelity transmission of entanglement over a high-loss free-space channel," *Nat. Phys.*, vol. 5, no. 6, pp. 389–392, 2009.

[95] J. Yin *et al.*, "Quantum teleportation and entanglement distribution over 100-kilometre free-space channels," *Nature*, vol. 488, pp. 185–188, Aug. 2012.

[96] X.-S. Ma *et al.*, "Quantum teleportation over 143 kilometres using active feedforward," *Nature*, vol. 489, no. 7415, pp. 269–273, 2012.

[97] S.-K. Liao *et al.*, "Long-distance free-space quantum key distribution in daylight towards inter-satellite communication," *Nat. Photon.*, vol. 11, no. 8, pp. 509–513, 2017.

[98] B. Heim *et al.*, "Atmospheric channel characteristics for quantum communication with continuous polarization variables," *Appl. Phys. B*, vol. 98, no. 4, pp. 635–640, 2010.

[99] A. A. Semenov and W. Vogel, "Quantum light in the turbulent atmosphere," *Phys. Rev. A*, vol. 80, no. 2, 2009, Art. no. 021802(R).

[100] D. Y. Vasylyev, A. A. Semenov, and W. Vogel, "Toward global quantum communication: Beam wandering preserves nonclassicality," *Phys. Rev. Lett.*, vol. 108, Jun. 2012, Art. no. 220501.

[101] D. Vasylyev, A. A. Semenov, and W. Vogel, "Atmospheric quantum channels with weak and strong turbulence," *Phys. Rev. Lett.*, vol. 117, Aug. 2016, Art. no. 090501.

[102] V. C. Usenko *et al.*, "Entanglement of Gaussian states and the applicability to quantum key distribution over fading channels," *New J. Phys.*, vol. 14, Sep. 2012, Art. no. 093048.

[103] M. Bohmann, A. A. Semenov, J. Sperling, and W. Vogel, "Gaussian entanglement in the turbulent atmosphere," *Phys. Rev. A*, vol. 94, Jul. 2016, Art. no. 010302(R).

[104] M. Bohmann, J. Sperling, A. A. Semenov, and W. Vogel, "Higher-order nonclassical effects in fluctuating-loss channels," *Phys. Rev. A*, vol. 95, Jan. 2017, Art. no. 012324.

[105] N. Hosseinidehaj and R. Malaney, "Gaussian entanglement distribution via satellite," *Phys. Rev. A*, vol. 91, Feb. 2015, Art. no. 022304.

[106] N. Hosseinidehaj and R. Malaney, "Quantum key distribution over combined atmospheric fading channels," in *Proc. IEEE Int. Conf. Commun. (ICC)*, London, U.K., 2015, pp. 7413–7419.

[107] N. Hosseinidehaj and R. Malaney, "Entanglement generation via non-Gaussian transfer over atmospheric fading channels," *Phys. Rev. A*, vol. 92, Dec. 2015, Art. no. 062336.

[108] N. Hosseinidehaj and R. Malaney, "CV-MDI quantum key distribution via satellite," *Quantum Inf. Comput.*, vol. 17, nos. 5–6, pp. 361–379, 2017.

[109] N. Hosseinidehaj and R. Malaney, "CV-QKD with Gaussian and non-Gaussian entangled states over satellite-based channels," in *Proc. IEEE Glob. Commun. Conf. (GLOBECOM)*, Washington, DC, USA, 2016, pp. 1–7.

[110] B. Heim *et al.*, "Atmospheric continuous-variable quantum communication," *New J. Phys.*, vol. 16, Nov. 2014, Art. no. 113018.

[111] C. Peuntinger *et al.*, "Distribution of squeezed states through an atmospheric channel," *Phys. Rev. Lett.*, vol. 113, Aug. 2014, Art. no. 060502.

[112] K. Günthner *et al.*, "Quantum-limited measurements of optical signals from a geostationary satellite," *Optica*, vol. 4, no. 6, pp. 611–616, 2017.

[113] J. Eisert and M. B. Plenio, "Introduction to the basics of entanglement theory in continuous-variable systems," *Int. J. Quantum Inf.*, vol. 1, pp. 479–506, Nov. 2003.

[114] G. Adesso, "Entanglement of Gaussian states," Ph.D. dissertation, Dept. Phys., Univ. Salerno, Fisciano, Italy, 2007.

[115] C. C. Gerry and P. L. Knight, *Introductory Quantum Optics*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[116] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Phys. Rev. Lett.*, vol. 88, Jan. 2002, Art. no. 057902.

[117] C. Weedbrook *et al.*, "Quantum cryptography without switching," *Phys. Rev. Lett.*, vol. 93, Oct. 2004, Art. no. 170504.

[118] R. García-Patrón and N. J. Cerf, "Continuous-variable quantum key distribution protocols over noisy channels," *Phys. Rev. Lett.*, vol. 102, Mar. 2009, Art. no. 130501.

[119] J. G. Rarity, P. R. Tapster, and E. Jakeman, "Observation of sub-poissonian light in parametric downconversion," *Opt. Commun.*, vol. 62, no. 3, pp. 201–206, 1987.

[120] P. G. Kwiat *et al.*, "New high-intensity source of polarization-entangled photon pairs," *Phys. Rev. Lett.*, vol. 75, pp. 4337–4341, Dec. 1995.

[121] M. E. Anderson, D. F. McAlister, M. G. Raymer, and M. C. Gupta, "Pulsed squeezed-light generation in $\chi^{(2)}$ nonlinear waveguides," *J. Opt. Soc. Amer. B*, vol. 14, no. 11, pp. 3180–3190, 1997.

[122] W. P. Grice and I. A. Walmsley, "Spectral information and distinguishability in type-II down-conversion with a broadband pump," *Phys. Rev. A*, vol. 56, pp. 1627–1634, Aug. 1997.

[123] Y. Shih, "Entangled biphoton source—Property and preparation," *Rep. Progr. Phys.*, vol. 66, no. 6, pp. 1009–1044, 2003.

[124] R. Simon, "Peres–Horodecki separability criterion for continuous variable systems," *Phys. Rev. Lett.*, vol. 84, pp. 2726–2729, Mar. 2000.

[125] G. Giedke, M. M. Wolf, O. Krüger, R. F. Werner, and J. I. Cirac, "Entanglement of formation for symmetric Gaussian states," *Phys. Rev. Lett.*, vol. 91, Sep. 2003, Art. no. 107901.

[126] M. M. Wolf, G. Giedke, O. Krüger, R. F. Werner, and J. I. Cirac, "Gaussian entanglement of formation," *Phys. Rev. A*, vol. 69, May 2004, Art. no. 052320.

[127] G. Vidal and R. F. Werner, "Computable measure of entanglement," *Phys. Rev. A*, vol. 65, Feb. 2002, Art. no. 032314.

[128] M. B. Plenio, "Logarithmic negativity: A full entanglement monotone that is not convex," *Phys. Rev. Lett.*, vol. 95, Sep. 2005, Art. no. 090503.

[129] C. Weedbrook, S. Pirandola, S. Lloyd, and T. C. Ralph, "Quantum cryptography approaching the classical limit," *Phys. Rev. Lett.*, vol. 105, Sep. 2010, Art. no. 110501.

[130] C. Weedbrook, S. Pirandola, and T. C. Ralph, "Continuous-variable quantum key distribution using thermal states," *Phys. Rev. A*, vol. 86, Aug. 2012, Art. no. 022318.

[131] C. Weedbrook, C. Ottaviani, and S. Pirandola, "Two-way quantum cryptography at different wavelengths," *Phys. Rev. A*, vol. 89, Jan. 2014, Art. no. 012309.

[132] N. Hosseinidehaj and R. Malaney, "Quantum entanglement distribution in next-generation wireless communication systems," in *Proc. 85th IEEE Veh. Technol. Conf. (VTC)*, 2017, pp. 1–7.

[133] N. Hosseinidehaj and R. Malaney, "Multimode entangled states in the lossy channel," in *Proc. IEEE VTC Int. Workshop Quantum Commun. Future Netw. (QCFN)*, Sydney, NSW, Australia, 2017, pp. 1–5.

[134] S. Pirandola, "Entanglement reactivation in separable environments," *New J. Phys.*, vol. 15, Nov. 2013, Art. no. 113046.

[135] R. Garcia-Patron, "Quantum information with optical continuous variables: From bell tests to key distribution," Ph.D. dissertation, Center Quant. Inf. Commun., Universite Libre de Bruxelles, Brussels, Belgium, 2007.

[136] C. Weedbrook, "Continuous-variable quantum key distribution with entanglement in the middle," *Phys. Rev. A*, vol. 87, Feb. 2013, Art. no. 022308.

[137] T. Symul *et al.*, "Experimental demonstration of post-selection-based continuous-variable quantum key distribution in the presence of Gaussian noise," *Phys. Rev. A*, vol. 76, Sep. 2007, Art. no. 030303.

[138] S. Fossier *et al.*, "Field test of a continuous-variable quantum key distribution prototype," *New J. Phys.*, vol. 11, no. 13, 2009, Art. no. 045023.

[139] Y. Shen, H. Zou, L. Tian, P. Chen, and J. Yuan, "Experimental study on discretely modulated continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 82, Aug. 2010, Art. no. 022317.

[140] P. Jouguet *et al.*, "Field test of classical symmetric encryption with continuous variables quantum key distribution," *Opt. Exp.*, vol. 20, no. 13, pp. 14030–14041, 2012.

[141] S. Pirandola, R. García-Patrón, S. L. Braunstein, and S. Lloyd, "Direct and reverse secret-key capacities of a quantum channel," *Phys. Rev. Lett.*, vol. 102, Feb. 2009, Art. no. 050503.

[142] R. Renner and J. I. Cirac, "De Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography," *Phys. Rev. Lett.*, vol. 102, no. 11, 2009, Art. no. 110504.

[143] R. García-Patrón and N. J. Cerf, "Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution," *Phys. Rev. Lett.*, vol. 97, no. 6, 2006, Art. no. 190503.

[144] L. C. Andrews, R. L. Phillips, and C. Y. Hopen, *Laser Beam Scintillation With Applications*. Bellingham, WA, USA: SPIE, 2001.

[145] L. C. Andrews and R. L. Phillips, *Laser Beam Propagation Through Random Media*, vol. PM152, 2nd ed. Bellingham, WA, USA: SPIE, 2005.

[146] F. Dios, J. A. Rubio, A. Rodrfguez, and A. Comerón, "Scintillation and beam-wander analysis in an optical ground station-satellite uplink," *Appl. Opt.*, vol. 43, no. 19, pp. 3866–3873, 2004.

[147] H. Kaushal and G. Kaddoum, "Optical communication in space: Challenges and mitigation techniques," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 57–96, 1st Quart., 2017.

[148] K. S. Shaik, "Atmospheric propagation effects relevant to optical communications," TDA Progr., Lijnden, The Netherlands, Rep. 42-94, pp. 180–200, 1988.

[149] I. Capraro *et al.*, "Impact of turbulence in long range quantum and classical communications," *Phys. Rev. Lett.*, vol. 109, Nov. 2012, Art. no. 200502.

[150] G. Vallone *et al.*, "Adaptive real time selection for quantum key distribution in lossy and turbulent free-space channels," *Phys. Rev. A*, vol. 91, Apr. 2015, Art. no. 042320.

[151] X. Yi and M. Yao, "Free-space communications over exponentiated Weibull turbulence channels with nonzero boresight pointing errors," *Opt. Exp.*, vol. 23, no. 3, pp. 2904–2917, 2015.

[152] M. A. Esmail, H. Fathallah, and M.-S. Alouini, "Analysis of fog effects on terrestrial free space optical communication links," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC)*, 2016, pp. 151–156.

[153] H. Kaushal, V. K. Jain, and S. Kar, *Free Space Optical Communication*, 1st ed. New Delhi, India: Springer, 2017.

[154] I. I. Kim, B. McArthur, and E. J. Korevaar, "Comparison of laser beam propagation at 785 nm and 1550 nm in fog and haze for optical wireless communications," in *Proc. Opt. Wireless Commun. III*, vol. 4214, 2001, pp. 26–38.

[155] P. W. Kruse, L. D. McGlauchlin, and R. B. McQuistan, *Elements of Infrared Technology: Generation, Transmission and Detection*. New York, NY, USA: Wiley, 1962.

[156] J. B. Pors, "Entangling light in high dimensions," Ph.D. dissertation, Casimir Res. School, Leiden Univ., Leiden, The Netherlands, 2011.

[157] P. W. Milonni, J. H. Carter, C. G. Peterson, and R. J. Hughes, "Effects of propagation through atmospheric turbulence on photon statistics," *J. Opt. B Quantum Semiclassical Opt.*, vol. 6, no. 6, pp. S742–S745, 2004.

[158] C. Erven *et al.*, "Studying free-space transmission statistics and improving free-space quantum key distribution in the turbulent atmosphere," *New J. Phys.*, vol. 14, Dec. 2012, Art. no. 123018.

[159] H.-R. Li, F.-L. Li, Y. Yang, and Q. Zhang, "Entanglement swapping of two-mode Gaussian states in a thermal environment," *Phys. Rev. A*, vol. 71, Feb. 2005, Art. no. 022314.

[160] S. Pirandola, D. Vitali, P. Tombesi, and S. Lloyd, "Macroscopic entanglement by entanglement swapping," *Phys. Rev. Lett.*, vol. 97, Oct. 2006, Art. no. 150403.

[161] M. Abdi, S. Pirandola, P. Tombesi, and D. Vitali, "Continuous-variable-entanglement swapping and its local certification: Entangling distant mechanical modes," *Phys. Rev. A*, vol. 89, no. 2, 2014, Art. no. 022331.

[162] J. Hoelscher-Obermaier and P. van Loock, "Optimal Gaussian entanglement swapping," *Phys. Rev. A*, vol. 83, Jan. 2011, Art. no. 012319.

[163] S. Pirandola *et al.*, "High-rate measurement-device-independent quantum cryptography," *Nat. Photon.*, vol. 9, pp. 397–402, May 2015.

[164] S. L. Braunstein, and S. Pirandola, "Side-channel-free quantum key distribution," *Phys. Rev. Lett.*, vol. 108, no. 13, 2012, Art. no. 130502.

[165] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 108, Mar. 2012, Art. no. 130503.

[166] T. Eberle, V. Händchen, and R. Schnabel, "Stable control of 10 dB two-mode squeezed vacuum states of light," *Opt. Exp.*, vol. 21, no. 9, pp. 11546–11553, 2013.

[167] H. Vahlbruch, M. Mehmet, K. Danzmann, and R. Schnabel, "Detection of 15 dB squeezed states of light and their application for the absolute calibration of photoelectric quantum efficiency," *Phys. Rev. Lett.*, vol. 117, Sep. 2016, Art. no. 110801.

[168] X.-C. Ma, S.-H. Sun, M.-S. Jiang, M. Gui, and L.-M. Liang, "Gaussian-modulated coherent-state measurement-device-independent quantum key distribution," *Phys. Rev. A*, vol. 89, Apr. 2014, Art. no. 042335.

[169] Z. Li, Y.-C. Zhang, F. Xu, X. Peng, and H. Guo, "Continuous-variable measurement-device-independent quantum key distribution," *Phys. Rev. A*, vol. 89, May 2014, Art. no. 052301.

[170] Y.-C. Zhang *et al.*, "Continuous-variable measurement-device-independent quantum key distribution using squeezed states," *Phys. Rev. A*, vol. 90, Nov. 2014, Art. no. 052325.

[171] C. Ottaviani, G. Spedalieri, S. L. Braunstein, and S. Pirandola, "Continuous-variable quantum cryptography with an untrusted relay: Detailed security analysis of the symmetric configuration," *Phys. Rev. A*, vol. 91, Feb. 2015, Art. no. 022320.

[172] Y. Zhang *et al.*, "Noiseless linear amplifiers in entanglement-based continuous-variable quantum key distribution," *Entropy*, vol. 17, no. 7, pp. 4547–4562, 2015.

[173] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, "Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks," *Phys. Rev. Lett.*, vol. 111, Sep. 2013, Art. no. 130501.

[174] T. F. da Silva *et al.*, "Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits," *Phys. Rev. A*, vol. 88, Nov. 2013, Art. no. 052303.

[175] Y. Liu *et al.*, "Experimental measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 111, Sep. 2013, Art. no. 130502.

[176] Y.-L. Tang *et al.*, "Measurement-device-independent quantum key distribution over 200 km," *Phys. Rev. Lett.*, vol. 113, Nov. 2014, Art. no. 190501.

[177] Y.-L. Tang *et al.*, "Measurement-device-independent quantum key distribution over untrustful metropolitan network," *Phys. Rev. X*, vol. 6, Mar. 2016, Art. no. 011024.

[178] M. Tomamichel and R. Renner, "Uncertainty relation for smooth entropies," *Phys. Rev. Lett.*, vol. 106, Mar. 2011, Art. no. 110506.

[179] C. Branciard, E. G. Cavalcanti, S. P. Walborn, V. Scarani, and H. M. Wiseman, "One-sided device-independent quantum key distribution: Security, feasibility, and the connection with steering," *Phys. Rev. A*, vol. 85, Jan. 2012, Art. no. 010301(R).

[180] M. Tomamichel, S. Fehr, J. Kaniewski, and S. Wehner, "A monogamy-of-entanglement game with applications to device-independent quantum cryptography," *New J. Phys.*, vol. 15, Oct. 2013, Art. no. 103002.

[181] T. Gehring *et al.*, "Implementation of continuous-variable quantum key distribution with composable and one-sided-device-independent security against coherent attacks," *Nat. Commun.*, vol. 6, Oct. 2015, Art. no. 8795.

[182] N. Walk *et al.*, "Experimental demonstration of Gaussian protocols for one-sided device-independent quantum key distribution," *Optica*, vol. 3, no. 6, pp. 634–642, 2016.

[183] K. Marshall and C. Weedbrook, "Device-independent quantum cryptography for continuous variables," *Phys. Rev. A*, vol. 90, no. 4, 2014, Art. no. 042311.

[184] R. Dong *et al.*, "Continuous-variable entanglement distillation of non-Gaussian mixed states," *Phys. Rev. A*, vol. 82, Jul. 2010, Art. no. 012312.

[185] P. Papanastasiou, C. Weedbrook, and S. Pirandola, "Continuous-variable quantum key distribution in uniform fast-fading channels," *Phys. Rev. A*, vol. 97, no. 3, Mar. 2018, Art. no. 032311. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.97.032311, doi: 10.1103/PhysRevA.97.032311.

[186] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, "Fundamental limits of repeaterless quantum communications," *Nat. Commun.*, vol. 8, Apr. 2017, Art. no. 15043.

[187] C. H. Bennett *et al.*, "Purification of noisy entanglement and faithful teleportation via noisy channels," *Phys. Rev. Lett.*, vol. 76, pp. 722–725, Jan. 1996.

[188] D. E. Browne, J. Eisert, S. Scheel, and M. B. Plenio, "Driving non-Gaussian to Gaussian states with linear optics," *Phys. Rev. A*, vol. 67, Jun. 2003, Art. no. 062320.

[189] J. Eisert, D. E. Browne, S. Scheel, and M. B. Plenio, "Distillation of continuous-variable entanglement with optical means," *Ann. Phys.*, vol. 311, no. 2, pp. 431–458, 2004.

[190] J. Fiurášek, P. Marek, R. Filip, and R. Schnabel, "Experimentally feasible purification of continuous-variable entanglement," *Phys. Rev. A*, vol. 75, no. 5, 2007, Art. no. 050302(R).

[191] A. P. Lund and T. C. Ralph, "Continuous-variable entanglement distillation over a general lossy channel," *Phys. Rev. A*, vol. 80, Sep. 2009, Art. no. 032309.

[192] J. Eisert, S. Scheel, and M. B. Plenio, "Distilling Gaussian states with Gaussian operations is impossible," *Phys. Rev. Lett.*, vol. 89, no. 13, 2002, Art. no. 137903.

[193] G. Giedke and J. I. Cirac, "Characterization of Gaussian operations and distillation of Gaussian states," *Phys. Rev. A*, vol. 66, Sep. 2002, Art. no. 032316.

[194] J. Fiurášek, "Gaussian transformations and distillation of entangled Gaussian states," *Phys. Rev. Lett.*, vol. 89, no. 13, 2002, Art. no. 137904.

[195] T. C. Ralph and A. P. Lund, "Nondeterministic noiseless linear amplification of quantum systems," in *Proc. 9th Int. Conf. Quantum Commun. Meas. Comput. (QCMC)*, 2009, pp. 155–160.

[196] G. Y. Xiang, T. C. Ralph, A. P. Lund, N. Walk, and G. J. Pryde, "Heralded noiseless linear amplification and distillation of entanglement," *Nat. Photon.*, vol. 4, no. 5, pp. 316–319, 2010.

[197] T. C. Ralph, "Quantum error correction of continuous-variable states against Gaussian noise," *Phys. Rev. A*, vol. 84, Aug. 2011, Art. no. 022339.

[198] N. Walk, A. P. Lund, and T. C. Ralph, "Nondeterministic noiseless amplification via non-symplectic phase space transformations," *New J. Phys.*, vol. 15, Jul. 2013, Art. no. 073014.

[199] H. M. Chrzanowski *et al.*, "Measurement-based noiseless linear amplification for quantum communication," *Nat. Photon.*, vol. 8, pp. 333–338, Mar. 2014.

[200] A. E. Ulanov *et al.*, "Undoing the effect of loss on quantum entanglement," *Nat. Photon.*, vol. 9, Oct. pp. 764–768, 2015.

[201] J. Fiurášek and N. J. Cerf, "Gaussian postselection and virtual noiseless amplification in continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 86, no. 6, 2012, Art. no. 060302.

[202] R. Blandino *et al.*, "Improving the maximum transmission distance of continuous-variable quantum key distribution using a noiseless amplifier," *Phys. Rev. A*, vol. 86, Jul. 2012, Art. no. 012327.

[203] N. Walk, T. C. Ralph, T. Symul, and P. K. Lam, "Security of continuous-variable quantum cryptography with Gaussian postselection," *Phys. Rev. A*, vol. 87, Feb. 2013, Art. no. 020303.

[204] T. Opatrný, G. Kurizki, and D.-G. Welsch, "Improvement on teleportation of continuous variables by photon subtraction via conditional measurement," *Phys. Rev. A*, vol. 61, Feb. 2000, Art. no. 032302.

[205] A. Kitagawa, M. Takeoka, M. Sasaki, and A. Chefles, "Entanglement evaluation of non-Gaussian states generated by photon subtraction from squeezed states," *Phys. Rev. A*, vol. 73, no. 2, Apr. 2006, Art. no. 042310.

[206] F. Dell'Anno, S. De Siena, L. Albano, and F. Illuminati, "Continuous-variable quantum teleportation with non-Gaussian resources," *Phys. Rev. A*, vol. 76, 2007, Art. no. 022301.

[207] Y. Yang and F.-L. Li, "Entanglement properties of non-Gaussian resources generated via photon subtraction and addition and continuous-variable quantum-teleportation improvement," *Phys. Rev. A*, vol. 80, no. 2, 2009, Art. no. 022315.

[208] S. L. Zhang and P. van Loock, "Distillation of mixed-state continuous-variable entanglement by photon subtraction," *Phys. Rev. A*, vol. 82, Dec. 2010, Art. no. 062316.

[209] C. Navarrete-Benlloch, R. Garcia-Patrón, J. H. Shapiro, and N. J. Cerf, "Enhancing quantum entanglement by photon addition and subtraction," *Phys. Rev. A*, vol. 86, Jul. 2012, Art. no. 012328.

[210] T. J. Bartley *et al.*, "Strategies for enhancing quantum entanglement by local photon subtraction," *Phys. Rev. A*, vol. 87, Feb. 2013, Art. no. 022313.

[211] S. L. Zhang, Y. Dong, X. Zou, B. Shi, and G. C. Guo, "Continuous-variable-entanglement distillation with photon addition," *Phys. Rev. A*, vol. 88, Sep. 2013, Art. no. 032324.

[212] J. Lee and H. Nha, "Entanglement distillation for continuous variables in a thermal environment: Effectiveness of a non-Gaussian operation," *Phys. Rev. A*, vol. 87, Mar. 2013, Art. no. 032307.

[213] K. P. Seshadreesan, J. P. Dowling, and G. S. Agarwal, "Non-Gaussian entangled states and quantum teleportation of Schrodinger-cat states," *Physica Scripta*, vol. 90, no. 7, 2015, Art. no. 074029.

[214] T. J. Bartley and I. A. Walmsley, "Directly comparing entanglement-enhancing non-Gaussian operations," *New J. Phys.*, vol. 17, Feb. 2015, Art. no. 023038.

[215] M. Allegra, P. Giorda, and M. G. A. Paris, "Role of initial entanglement and non-Gaussianity in the decoherence of photon-number entangled states evolving in a noisy channel," *Phys. Rev. Lett.*, vol. 105, Sep. 2010, Art. no. 100503.

[216] G. Adesso, "Simple proof of the robustness of Gaussian entanglement in bosonic noisy channels," *Phys. Rev. A*, vol. 83, Feb. 2011, Art. no. 024301.

[217] K. K. Sabapathy, J. S. Ivan, and R. Simon, "Robustness of non-Gaussian entanglement against noisy amplifier and attenuator environments," *Phys. Rev. Lett.*, vol. 107, no. 13, 2011, Art. no. 130501.

[218] S. N. Filippov and M. Ziman, "Entanglement sensitivity to signal attenuation and amplification," *Phys. Rev. A*, vol. 90, Jul. 2014, Art. no. 010301(R).

[219] P. Huang, G. He, J. Fang, and G. Zeng, "Performance improvement of continuous-variable quantum key distribution via photon subtraction," *Phys. Rev. A*, vol. 87, Jan. 2013, Art. no. 012317.

[220] Z. Li *et al.*, "Non-Gaussian postselection and virtual photon subtraction in continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 93, Jan. 2016, Art. no. 012310.

[221] L. F. M. Borelli, L. S. Aguiar, J. A. Roversi, and A. Vidiella-Barranco, "Quantum key distribution using continuous-variable non-Gaussian states," *Quantum Inf. Process.*, vol. 15, no. 2, pp. 893–904, 2016.

[222] G. S. Agarwal, S. Chaturvedi, and A. Rai, "Amplification of maximally-path-entangled number states," *Phys. Rev. A*, vol. 81, Apr. 2010, Art. no. 043843.

[223] H. Nha, G. J. Milburn, and H. J. Carmichael, "Linear amplification and quantum cloning for non-Gaussian continuous variables," *New J. Phys.*, vol. 12, Oct. 2010, Art. no. 103010.

[224] A. Leverrier and P. Grangier, "Continuous-variable quantum-key-distribution protocols with a non-Gaussian modulation," *Phy. Rev. A*, vol. 83, Apr. 2011, Art. no. 042312.

[225] K. Wakui, H. Takahashi, A. Furusawa, and M. Sasaki, "Photon subtracted squeezed states generated with periodically poled $KTiOPO_4$," *Opt. Exp.*, vol. 15, no. 6, pp. 3568–3574, 2007.

[226] H. Takahashi *et al.*, "Entanglement distillation from Gaussian input states," *Nat. Photon.*, vol. 4, pp. 178–181, Feb. 2010.

[227] Y. Kurochkin, A. S. Prasad, and A. I. Lvovsky, "Distillation of the two-mode squeezed state," *Phys. Rev. Lett.*, vol. 112, no. 7, 2014, Art. no. 070402.

[228] A. Zavatta, S. Viciani, and M. Bellini, "Quantum-to-classical transition with single-photon-added coherent states of light," *Science*, vol. 306, no. 5696, pp. 660–662, 2004.

[229] A. Zavatta, V. Parigi, and M. Bellini, "Experimental nonclassicality of single-photon-added thermal light states," *Phys. Rev. A*, vol. 75, May 2007, Art. no. 052106.

[230] J. S. Ivan, K. K. Sabapathy, and R. Simon, "Operator-sum representation for bosonic Gaussian channels," *Phys. Rev. A*, vol. 84, Oct. 2011, Art. no. 042311.

[231] H. V. Nguyen *et al.*, "Network coding aided cooperative quantum key distribution over free-space optical channels," *IEEE Access*, vol. 5, pp. 12301–12317, 2017.

[232] H. Weier, T. Schmitt-Manderbach, N. Regner, C. Kurtsiefer, and H. Weinfurter, "Free space quantum key distribution: Towards a real life application," *Fortschritte der Physik*, vol. 54, nos. 8–10, pp. 840–845, 2006.

[233] M. Jofre *et al.*, "Fast optical source for quantum key distribution based on semiconductor optical amplifiers," *Opt. Exp.*, vol. 19, no. 5, pp. 3825–3834, 2011.

[234] U. L. Andersen, J. S. Neergaard-Nielsen, P. van Loock, and A. Furusawa, "Hybrid discrete- and continuous-variable quantum information," *Nat. Phys.*, vol. 11, pp. 713–719, Sep. 2015.

[235] M. O. Gumberidze, A. A. Semenov, D. Vasylyev, and W. Vogel, "Bell nonlocality in the turbulent atmosphere," *Phys. Rev. A*, vol. 94, Nov. 2016, Art. no. 053801.

[236] A. A. Semenov and W. Vogel, "Entanglement transfer through the turbulent atmosphere," *Phys. Rev. A*, vol. 81, Feb. 2010, Art. no. 023835.

[237] O. O. Chumak and R. A. Baskov, "Strong enhancing effect of correlations of photon trajectories on laser beam scintillations," *Phys. Rev. A*, vol. 93, Mar. 2016, Art. no. 033821.

[238] M. Bohmann, R. Kruse, J. Sperling, C. Silberhorn, and W. Vogel, "Probing free-space quantum channels with laboratory-based experiments," *Phys. Rev. A*, vol. 95, Jun. 2017, Art. no. 063801.

[239] D. Elkouss, A. Leverrier, R. Alleaume, and J. J. Boutros, "Efficient reconciliation protocol for discrete-variable quantum key distribution," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Seoul, South Korea, 2009, pp. 1879–1883.

[240] M. Milicevic, C. Feng, L. M. Zhang, and P. G. Gulak, "Key reconciliation with low-density parity-check codes for long-distance quantum cryptography," *arXiv:1702.07740*, 2017.

[241] X. Wang, Y. Zhang, S. Yu, and H. Guo, "High speed information reconciliation for long distance continuous-variable quantum key distribution system," in *Front. Opt. OSA Tech. Dig. Opt. Soc. America*, p. JW4A.36.

[242] M. Bloch, A. Thangaraj, and S. W. McLaughlin, "Efficient reconciliation of correlated continuous random variables using LDPC codes," *arXiv:cs/0509041*, 2005.

[243] A. Leverrier, R. Alléaume, J. Boutros, G. Zémor, and P. Grangier, "Multidimensional reconciliation for a continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 77, Apr. 2008, Art. no. 042325.

[244] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, "Tight finite-key analysis for quantum cryptography," *Nat. Commun.*, vol. 3, Jan. 2012, Art. no. 634.

[245] A. Leverrier, F. Grosshans, and P. Grangier, "Finite-size analysis of a continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 81, Jun. 2010, Art. no. 062343.

[246] P. Jouguet, D. Elkouss, and S. Kunz-Jacques, "High-bit-rate continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 90, Oct. 2014, Art. no. 042329.

[247] F. Furrer *et al.*, "Continuous variable quantum key distribution: Finite-key analysis of composable security against coherent attacks," *Phys. Rev. Lett.*, vol. 109, Sep. 2012, Art. no. 100502.

[248] F. Furrer, "Reverse-reconciliation continuous-variable quantum key distribution based on the uncertainty principle," *Phys. Rev. A*, vol. 90, Oct. 2014, Art. no. 042325.

[249] A. Leverrier, "Composable security proof for continuous-variable quantum key distribution with coherent states," *Phys. Rev. Lett.*, vol. 114, Feb. 2015, Art. no. 070501.

[250] P. Papanastasiou, C. Ottaviani, and S. Pirandola, "Finite-size analysis of measurement-device-independent quantum cryptography with continuous variables," *Phys. Rev. A*, vol. 96, Oct. 2017, Art. no. 042332.

[251] X. Zhang *et al.*, "Finite-size analysis of continuous-variable measurement-device-independent quantum key distribution," *Phys. Rev. A*, vol. 96, Oct. 2017, Art. no. 042334.

[252] R. Arnon-Friedman, R. Renner, and T. Vidick, "Simple and tight device-independent security proofs," *arXiv:1607.01797*, 2016.

[253] D. Elkouss, J. Martinez-Mateo, and V. Martin, "Secure rate-adaptive reconciliation," in *Proc. Int. Symp. Inf. Theory Appl. (ISITA)*, Taichung, Taiwan, 2010, pp. 179–184.

[254] X. Wang *et al.*, "Efficient rate-adaptive reconciliation for continuous-variable quantum key distribution," *Quant. Inf. Comput.*, vol. 17, nos. 13–14, pp. 1123–1134, 2017.

[255] X.-Q. Jiang, P. Huang, D. Huang, D. Lin, and G. Zeng, "Secret information reconciliation based on punctured low-density parity-check codes for continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 95, Feb. 2017, Art. no. 022318.

[256] L. Hanzo, T. H. Liew, B. L. Yeap, R. Y. S. Tee, and S. X. Ng, *Turbo Coding, Turbo Equalisation and Space-Time Coding: EXIT-Chart-Aided Near-Capacity Designs for Wireless Channels*, 2nd ed. New York, NY, USA: Wiley, 2011.

[257] C. Nguyen, G. Van Assche, and N. J. Cerf, "Side-information coding with turbo codes and its application to quantum key distribution," in *Proc. Int. Symp. Inf. Theory Appl. (ISITA)*, Parma, Italy, 2004.

[258] N. Benletaief, H. Rezig, and A. Bouallegue, "Toward efficient quantum key distribution reconciliation," *J. Quantum Inf. Sci.*, vol. 4, no. 2, pp. 117–128, 2014.

[259] W. Y. Liu *et al.*, "Experimental free-space quantum key distribution with efficient error correction" *Opt. Express*, vol. 25, no. 10, pp. 10716–10723, 2017.

[260] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3051–3073, Jul. 2009.

[261] P. Jouguet and S. Kunz-Jacques, "High performance error correction for quantum key distribution using polar codes," *Quantum Inf. Comput.*, vol. 14, nos. 3–4, pp. 329–338, 2014.

[262] J. Niset, J. Fiurasek, and N. J. Cerf, "No-go theorem for Gaussian quantum error correction," *Phys. Rev. Lett.*, vol. 102, no. 12, 2009, Art. no. 120501.

[263] S. L. Braunstein, "Quantum error correction for communication with linear optics," *Nature*, vol. 394, pp. 47–49, Jul. 1998.

[264] S. Lloyd and J.-J. E. Slotine, "Analog quantum error correction," *Phys. Rev. Lett.*, vol. 80, pp. 4088–4091, May 1998.

[265] S. L. Braunstein, "Error correction for continuous variables," *Phys. Rev. Lett.*, vol. 80, no. 18, pp. 4084–4087, May 1998.

[266] T. A. Walker and S. L. Braunstein, "Five-wave-packet linear optics quantum-error-correcting code," *Phys. Rev. A*, vol. 81, Jun. 2010, Art. no. 062305.

[267] M. M. Wilde, H. Krovi, and T. A. Brun, "Entanglement-assisted quantum error correction with linear optics," *Phys. Rev. A*, vol. 76, Nov. 2007, Art. no. 052308.

[268] J. Niset, U. L. Andersen, and N. J. Cerf, "Experimentally feasible quantum erasure-correcting code for continuous variables," *Phys. Rev. Lett.*, vol. 101, no. 13, 2008, Art. no. 130503.

[269] T. Aoki *et al.*, "Quantum error correction beyond qubits," *Nat. Phys.*, vol. 5, no. 8, pp. 541–546, 2009.

[270] M. Lassen *et al.*, "Quantum optical coherence can survive photon loss using a continuous-variable quantum erasure-correcting code," *Nat. Photon.*, vol. 4, no. 10, pp. 700–705, 2010.

[271] M. Lassen, A. Berni, L. S. Madsen, R. Filip, and U. L. Andersen, "Gaussian error correction of quantum states in a correlated noisy channel," *Phys. Rev. Lett.*, vol. 111, Oct. 2013, Art. no. 180502.

[272] S. Hao, X. Su, C. Tian, C. Xie, and K. Peng, "Five-wave-packet quantum error correction based on continuous-variable cluster entanglement," *Sci. Rep.*, vol. 5, Oct. 2015, Art. no. 15462.

[273] C. Eichler *et al.*, "Observation of two-mode squeezing in the microwave frequency domain," *Phys. Rev. Lett.*, vol. 107, Sep. 2011, Art. no. 113601.

[274] E. P. Menzel *et al.*, "Path entanglement of continuous-variable quantum microwaves," *Phys. Rev. Lett.*, vol. 109, Dec. 2012, Art. no. 250502.

[275] E. Flurin, N. Roch, F. Mallet, M. H. Devoret, and B. Huard, "Generating entangled microwave radiation over two transmission lines," *Phys. Rev. Lett.*, vol. 109, Oct. 2012, Art. no. 183901.

[276] S. Barzanjeh, M. Abdi, G. J. Milburn, P. Tombesi, and D. Vitali, "Reversible optical-to-microwave quantum interface," *Phys. Rev. Lett.*, vol. 109, no. 13, 2012, Art. no. 130503.

[277] R. Di Candia *et al.*, "Quantum teleportation of propagating quantum microwaves," *EPJ Quantum Technol.*, vol. 2, p. 25, Dec. 2015.

[278] M. Abdi, P. Tombesi, and D. Vitali, "Entangling two distant non-interacting microwave modes," *Annalen der Physik*, vol. 527, nos. 1–2, pp. 139–146, 2015.

[279] S. Barzanjeh *et al.*, "Microwave quantum illumination," *Phys. Rev. Lett.*, vol. 114, Feb. 2015, Art. no. 080503.

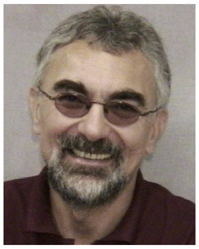
Nedasadat Hosseinidehaj received the B.S. degree in electrical engineering from the Isfahan University of Technology, Isfahan, Iran, in 2008, the M.S. degree in electrical engineering from Tarbiat Modares University, Tehran, Iran, in 2012, and the Ph.D. degree in electrical engineering from the University of New South Wales, Sydney, Australia, in 2017. She is currently a Post-Doctoral Research Fellow with the Centre for Quantum Computation and Communication Technology, School of Mathematics and Physics, University of Queensland, Brisbane, Australia. Her current research interests are in the areas of continuous-variable quantum communications, including quantum key distribution.

Zunaira Babar received the B.Eng. degree in electrical engineering from the National University of Science and Technology, Islamabad, Pakistan, in 2008, and the M.Sc. degree (with Distinction) and the Ph.D. degree in wireless communications from the University of Southampton, U.K., in 2011 and 2015, respectively. She is currently a Research Fellow with the Southampton Wireless Group, University of Southampton.

Her research interests include quantum error correction codes, channel coding, coded modulation, iterative detection, and cooperative communications.

Robert Malaney received the Bachelor of Science degree in physics from the University of Glasgow, and the Ph.D. degree in physics from the University of St. Andrews, U.K. He is currently an Associate Professor with the School of Electrical Engineering and Telecommunications, University of New South Wales, Australia. He has over 150 publications. He has previously held research positions with Caltech, University of California at Berkeley, National Labs, and the University of Toronto. He is a former Principal Research Scientist with CSIRO.

Soon Xin Ng (S'99–M'03–SM'08) received the B.Eng. degree (First Class) in electronic engineering and the Ph.D. degree in telecommunications from the University of Southampton, Southampton, U.K., in 1999 and 2002, respectively. From 2003 to 2006, he was a Post-Doctoral Research Fellow working on collaborative European research projects known as SCOUT, NEWCOM, and PHOENIX. Since 2006, he has been an Academic Staff Member with the School of Electronics and Computer Science, University of Southampton. He was involved in the OPTIMIX and CONCERTO European projects as well as the IU-ATC and UC4G projects. He was the Principal Investigator of an EPSRC project on Cooperative Classical and Quantum Communications Systems. He is currently an Associate Professor in telecommunications with the University of Southampton. His research interests include adaptive coded modulation, coded modulation, channel coding, space-time coding, joint source and channel coding, iterative detection, OFDM, MIMO, cooperative communications, distributed coding, quantum communications, quantum error correction codes, and joint wireless-and-optical-fiber communications. He has published over 240 papers and co-authored two Wiley/IEEE Press books in the above areas. He is a fellow of the Higher Education Academy in the U.K., a Chartered Engineer, and a fellow of IET.



Lajos Hanzo (M'91–SM'92–F'04) received the degree in electronics in 1976, the Doctorate degree in 1983, and the Honorary Doctorate degrees *(Doctor Honoris Causa)* from the Technical University of Budapest in 2009 and the University of Edinburgh in 2015. During his 40-year career in telecommunications he has held various research and academic posts in Hungary, Germany, and the U.K. Since 1986, he has been with the School of Electronics and Computer Science, University of Southampton, U.K., where he holds the chair in telecommunications. He has successfully supervised 112 Ph.D. students, co-authored 18 Wiley/IEEE Press books on mobile radio communications totalling in excess of 10 000 pages, published 1768 research contributions at IEEE Xplore, acted both as a TPC and the General Chair of IEEE conferences, presented keynote lectures, and has been awarded a number of distinctions. He is currently directing a 40-strong academic research team, working on a range of research projects in the field of wireless multimedia communications sponsored by industry, the Engineering and Physical Sciences Research Council, U.K., the European Research Council's Advanced Fellow Grant and the Royal Society's Wolfson Research Merit Award. He is an enthusiastic supporter of industrial and academic liaison and he offers a range of industrial courses.

He was the Editor-in-Chief of the IEEE Press and a Chaired Professor also with Tsinghua University, Beijing, from 2008 to 2012. He is also a Governor of the IEEE ComSoc and of IEEE VTS. He is a fellow of the Royal Academy of Engineering, the Institution of Engineering and Technology, and the European Association for Signal Processing. For further information on research in progress and associated publications please refer to http://www-mobile.ecs.soton.ac.uk.

Low-Complexity Adaptive Optics Aided Orbital Angular Momentum Based Wireless Communications

Huan Chang, Xiaoli Yin, Haipeng Yao, *Senior Member, IEEE,* Jingjing Wang, *Senior Member, IEEE,* Ran Gao, *Member, IEEE,* Jianping An, *Senior Member, IEEE,* and Lajos Hanzo, *Fellow, IEEE*

***Abstract*—Adaptive optics (AO) has the potential to mitigate the effect of atmospheric turbulence and improve the performance of orbital angular momentum (OAM)-based optical wireless communication (OAM-OWC) links. Here, we propose a single-intensity-measurement phase retrieval algorithm (SPRA)-based AO technique of compensating for the distortion of the OAM beam. The only parameter required by the SPRA wavefront sensor is the intensity of the probe beam in the Fourier domain, which substantially simplifies the AO system. We first derive an analytical expression to characterize the expansion of probe beam in OAM-OWC links and then determine the diameter constraints as the apriori information of the SPRA required for guaranteeing a certain compensation performance. The simulation results illustrate that the SPRA-AO approach can indeed correct a distorted OAM beam both in a single-channel scenario and in multiplexed OAM-OWC systems. The bit error rate can be improved by orders of magnitude with the aid of SPRA-AO compensation. Furthermore, we establish noise models of AO-based OAM-OWC systems and analyze the robustness of the SPRA-AO technique. In a nutshell, this paper provides new insights for the applications of AO and forms the theoretical basis of employing probe beams in OAM-OWC systems.**

This work was supported in part by the National Key R&D Program of China from Ministry of Science and Technology under Grant 2019YFA0706300, in part by the China Postdoctoral Science Foundation under Grant 2020M680385, 2020M680384, 2021M690411 and 2020TQ0054, in part by the National Natural Science Foundation of China under 62071062, 62022016, 61835002, 61727817, and in part by the Open Fund of IPOC (BUPT) under IPOC2020A007, IPOC2020A006. The work of H. Yao was supported by the Artificial Intelligence and Smart City Joint Laboratory (BUPT-TGSTII) (B2020001), Future Intelligent Networking and Intelligent Transportation Joint Laboratory (BUPTCTTIC) (B2019007). The work of J. Wang was supported by the Young Elite Scientist Sponsorship Program by CAST under Grant 2020QNRC001. L. Hanzo would like to acknowledge the financial support of the Engineering and Physical Sciences Research Council projects EP/P034284/1 and EP/P003990/1 (COALESCE) as well as of the European Research Council's Advanced Fellow Grant QuantCom (Grant No. 789028). *(Corresponding author: Lajos Hanzo and Ran Gao.)*

H. Chang, R. Gao and J. An are with the School of Information and Electronics, Beijing Institute of Technology, Beijing 100081, China (email: 7520200099@bit.edu.cn; 6120190142@bit.edu.cn; an@bit.edu.cn).

X. Yin is with the School of Electronic Engineering, Beijing University of Posts and Telecommunications and also with the Beijing Key Laboratory of Space-Ground Interconnection and Convergence, Beijing University of Posts and Telecommunications, Beijing 100876, China (email: yinxl@bupt.edu.cn).

H. Yao is with the State Key Lab Networking & Switching Technol, Beijing University of Posts and Telecommunications, Beijing 100876, China (email: yaohaipeng@bupt.edu.cn).

J. Wang is with the Department of Electronic Engineering, Tsinghua University, Beijing, 100084, China (e-mail: chinaeephd@gmail.com).

L. Hanzo is with the School of Electronics and Computer Science, University of Southampton, Southampton, SO17 1BJ, UK (email: lh@ecs.soton.ac.uk).

***Index Terms*—Optical wireless communications, orbital angular momentum, adaptive optics, phase retrieval algorithm.**

I. Introduction

As the demand for data increases, there is keen interest in increasing the transmission capacity in a range of fields [1], [2]. High-capacity optical wireless communication (OWC) is receiving increasing attention in various areas [3]–[5] because of the substantial demands for data transmission. Optical vortex beams carrying orbital angular momentum (OAM) characterized by a particular helical phase structure of $\exp(il\phi)$, have been introduced to meet the growing demand for large-capacity OWC [1], [6], [7] where the OAM state index l represents the number of 2π phase shifts across the beam and ϕ is the azimuthal angle. The OAM beams having a distinct l are orthogonal to each other, and the state index l is an infinite integer [8]. Therefore, the OAM beams are capable of substantially increasing the capacity of communication systems by either encoding information as OAM beam states or using OAM beams as information carriers for multiplexing [9]–[11].

The atmospheric turbulence (AT) effects, which are caused by random variations in temperature and convective motion induced by the random variations of the air's refractive index [12], constitute unavoidable impairments in OAM-aided OWC systems. In practical scenarios the atmospheric turbulence gives rise to phase distortion, which induces intermodal crosstalk among different states and degrades the performance of OAM-aided communication systems [13], [14]. Both experiments and simulations have verified that adaptive optics (AO) efficiently mitigates the distortion of OAM-OWC systems [15]. However, for OAM beams having helical phase fronts, one of the challenges is to directly detect the phase front using typical wave-front sensors due to the associated phase singularity [16]. To circumvent this, the phase retrieval algorithm (PRA)-based AO has gained increasing attention [17]. The Gerchberg-Saxton algorithm (GSA)-based phase correction method has been shown to efficiently mitigate the turbulent aberration of OAM beams both by simulations and experiments [18], [19]. Then, Fu *et al.* [20] used a probing Gaussian beam and the GSA for the pre-compensation of turbulence-infested OAM beams. In 2018, Yin *et al.* [21] proposed the hybrid-input-output-algorithm (HIOA) to compensate for the distortion of OAM beams in OAM-OWC systems.

TABLE I
COMPARISON OF THE PROPOSED SCHEME TO THE LITERATURE

	Our paper	[13]-2020	[4]-2019	[5]-2018	[20]-2017	[19]-2016	[13]-2015	[18]-2012	[33]-2010
Optical Wireless Communication	✓	✓	✓	✓	✓	✓	✓	✓	
Orbital Angular Momentum	✓		✓	✓	✓	✓	✓	✓	
Atmospheric Turbulence Simulation	✓	✓	✓		✓				
Adaptive Optics	✓		✓		✓	✓	✓	✓	
Shack-Hartmann wave-front Sensing technique								✓	
Phase Retrieval Algorithm-based Wave-front sensing technique	✓				✓	✓		✓	
Probe Expansion	✓				✓				
Experimental AO analysis						✓	✓	✓	
Simulation AO analysis	✓		✓		✓			✓	
Noise Model	✓								✓

The phase retrieval algorithm (PRA) has been conceived for reconstructing the phase from intensity information by exploiting any partial constraints, such as those observed in the object and Fourier domains. Explicitly, we have to infer the intensity of the probing beam in both the object and the Fourier domain as the input information of the algorithm to reconstruct the wave-front of the probe beam, which can be collectively termed as double-intensity measurements PRA (DPRA)-based AO (DPRA-AO) approaches [22], for both the HIOA and GSA [23]. These DPRA-AO systems require at least one beam splitter (BS) and two charge-coupled devices (CCDs). The BS halves the intensity of the probe beam, and the two CCDs constitute two detector-noise sources. On the other hand, compared to focused probe detection in the Fourier domain, optical detection in the object domain requires a wide field and imposes more detection noise.

We observe that in most cases of practical interest, the atmospheric phase is uniquely related to the Fourier intensity measurements [24]. Furthermore, AO in the communication links should ideally be miniaturized at a low cost [25], [26]. It is possible to recover the wave-front of the probe beam by solely relying on the intensity in the Fourier domain, provided that sufficient prior information is available about the probe beam [27]. Therefore, in this paper, we propose a low-complexity single-intensity-measurement PRA (SPRA)-based wave-front sensing technique for reconstructing the wave-front information of the probe beam relying on a low-complexity SPRA-based AO (SPRA-AO) system. The primary contributions of this paper are summarized as follows.

- We conceive a low-complexity and yet robust SPRA-AO technique which only has to detect a single Fourier intensity of the probe beam.
- An analytical expression is derived for characterizing the expansion of the OAM probe beam in an AO-based OAM-OWC system. Moreover, since there is a paucity of literature on this subject, the models of both the background noise and of the CCD detector noise of DPRA-AO and SPRA-AO based OAM-OWC systems are established.
- Extensive simulations have been conducted for evaluating the performance of our proposed SPRA-AO, demonstrating that it improves the bit error rate (BER) by orders of magnitude. Furthermore, we demonstrate that SPRA-AO has better robustness than DPRA-AO in the face of both background noise and detector noise.

Our new contributions are boldly and explicitly contrasted to the literature at a glance in Table I.

The rest of this paper is organized as follows. Section II A describes the OAM-OWC system relying on the SPRA-AO technique. Section II B derives the analytical expression of the probe beam expansion in OAM-OWC links. Furthermore, the SPRA principle is introduced and its constraint setting is detailed in Section II C. Then, the models of both the background noise and of the detector noise of the PRA-AO approach are established in Section II D. Finally, Section III evaluates the compensation performance attained by the SPRA-AO technique, while Section IV concludes the paper.

II. CONCEPT AND PRINCIPLE

A. Schematic of an OAM-OWC system relying on the SPRA-AO technique

The schematic of our OAM-OWC system is shown in Fig. 1. At the transmitter, the OAM beam used for the desired signal and the probe beam are polarization-multiplexed by a polarizing beam splitter (PBS) and propagated collinearly through the atmospheric turbulence channel, where the probe beam is used for estimating the turbulence-induced distortions which can then be exploited for decontaminating the OAM beams [12]. The probe beam used for sampling the AT is expanded to a predetermined size as wide as that of the signal OAM beam relying on a beam expander [19]. During the propagation, the

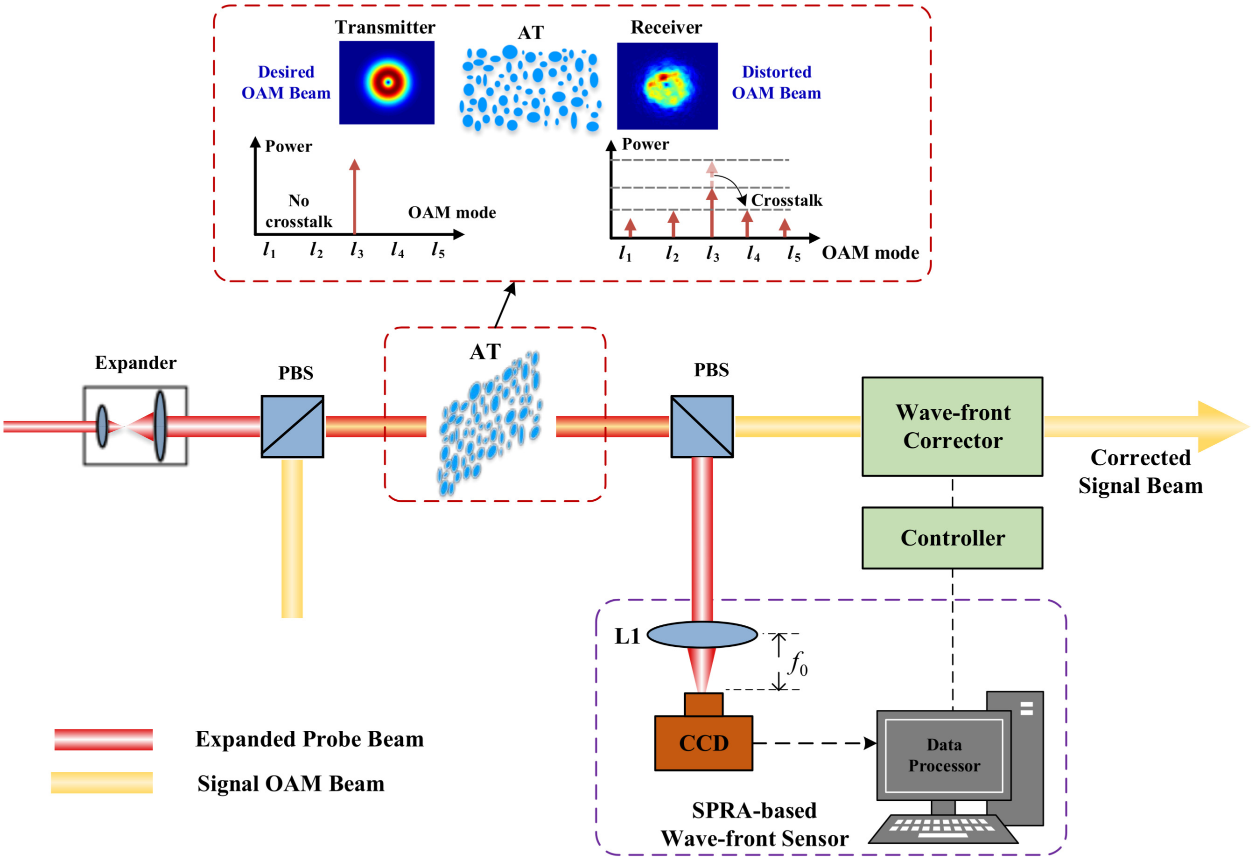


Fig. 1. Schematic of our OAM-OWC system equipped with an SPRA-AO module. (PBS: polarizing beam splitter, AT: atmospheric turbulence, L1: Fourier lens, f_0: back focal length of L1.)

atmospheric turbulence impairs the propagation modes and spreads the emitted modes into adjacent modes. As shown in Fig. 1, the OAM beams having clear doughnut-like intensity distribution would become distorted [28], hence each particular OAM mode may become coupled with its neighbouring modes, and therefore the communication performance may be degraded [15]. The distorted multiplexed beams are then partitioned into the OAM signalling beam and the probe beam by using a PBS at the receiver. The probe beam is then entered into the AO module, which consists of the wave-front sensor, wave-front controller and wave-front corrector. The wave-front sensor surrounded by a dashed line in Fig. 1 is composed of the Fourier lens L1, a CCD camera and a data processor. The Fourier lens L1 of Fig. 1 is used here to focus the beam and to estimate the spatial spectral distribution of the probe beam. The CCD camera of Fig. 1 in the focal plane of L1 is used for capturing the Fourier intensity pattern of the probe beam. Then, the data processor retrieves the phase of the probe beam from the focal plane intensity information with the aid of the SPRA and estimates the phase-change induced by turbulence. Finally, the estimated phase-correction signal is forwarded by the controller to the wave-front corrector of Fig. 1 for decontaminating the signal beam.

The Laguerre-Gaussian (LG) beam is a simple and widely used vortex beam, which can be characterized by a pair of indices, i.e. the azimuthal index l and the radial index p [29]. Hence, we consider it as an example in our analysis. The LG modes having different l values or p values are orthogonal to each other. In the classical domain, mode multiplexing (i.e., each mode carries an independent data stream) and data encoding (i.e., each pulse occupies a given LG mode state) using different l or p values have the potential of substantially increasing the capacity of communication systems [30]. The intensity and phase distributions of LG beams associated with different azimuthal state indices are shown in Fig. 2, where the doughnut-shaped intensity profiles are clearly visible because of the phase singularity at the beam center. The definition of an LG mode [30] that gives the intensity distribution for the lowest-order radial LG mode $p = 0$ can be formulated as:

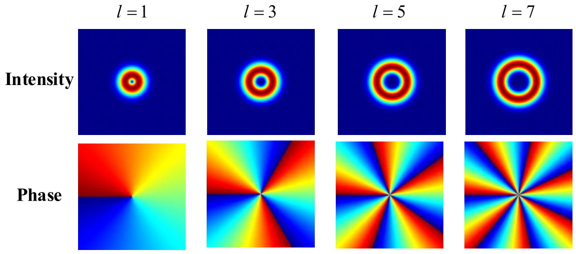


Fig. 2. Intensity and phase distributions of LG beams with different azimuthal state indexes.

$$I(r,\phi,z)=\frac{2}{\omega^2(z)\pi\left|l\right|!}\left[\frac{r\sqrt{2}}{\omega(z)}\right]^{2[l]}\exp\left[\frac{-2r^2}{\omega^2(z)}\right], \quad (1)$$

which is normalized as $\int_0^\infty\int_0^{2\pi} I(r,\phi,z)r\,d\phi\,dr=1$. In (1), r is the radial cylindrical coordinate, ϕ represents the azimuthal angle and l is the azimuthal state index. Moreover, $\omega(z)$ denotes the beam radius at the propagation distance z, which can be expressed as

$$\omega(z)=\sqrt{\omega_0^2+(z/z_R)^2}, \quad (2)$$

where λ is the optical wavelength, while $z_R=\pi\omega_0^2/\lambda$ is the Rayleigh range and ω_0 represents the $1\backslash e$ radius of the Gaussian term of the LG beam, which is also termed as the beam waist [31]. In the AO-based OAM-OWC system of Fig. 1 we utilize the OAM beam as the probe beam, because the OAM beam associated with hollow intensity and used as a probe beam outperforms the Gaussian probe beam in AO-based OAM systems [22].

B. The expansion scheme of the probe beam in OAM-OWC systems

In an AO-based OAM-OWC system, the phase-change imposed by atmospheric turbulence is estimated by the probe beam and then used for the decontamination of the signal beam. For achieving more accurate phase compensation, the expanded probe beam should remain as wide as the signal beam during their collinear propagation in order to satisfy the assumption that the OAM signalling beam and probe beam undergo similar wave-front aberrations because of turbulence [32]. However, if the probe beam is much wider than the signal beam, the probe beam will experience more severe turbulence-induced distortion than the signal beam. It has been demonstrated that the degree of wave-front aberration similarity between the signal and probe beam depends to some extent on the intensity distribution similarity of these two beams. In other words, the AO compensation performance is also affected by the intensity distribution similarity of the signal and the expanded probe beam. Fig. 3 shows the intensity distributions of the OAM signalling beam and expanded probe beam during their propagation. Therefore, in this section, we conceive a beneficial scheme for ensuring that the intensity distributions of the two beams remain similar.

For convenience, the notations used in the following derivation are summarized at a glance in Table II. We define the intensity correlation coefficient [33] between the signal beam and the expanded probe beam as follows:

$$C=\frac{\int_0^\infty\int_0^{2\pi} I_p(r,\phi,z)\cdot I_s(r,\phi,z)r\,d\phi\,dr}{\sqrt{\int_0^\infty\int_0^{2\pi} I_p^2(r,\phi,z)r\,d\phi\,dr\cdot\int_0^\infty\int_0^{2\pi} I_s^2(r,\phi,z)r\,d\phi\,dr}}, \quad (3)$$

where $I_p(r,\phi,z)$ and $I_s(r,\phi,z)$ are the intensities of the probe beam and signal beam, respectively. Combined with (1) and (3), C can be reformulated as

TABLE II
THE EXPLANATION OF NOTATIONS IN THE FOLLOWING DERIVATION.

Notation	Declarations	Notation	Declarations
I_p	The intensity of the probe beam	I_s	The intensity of the signal beam
l_p	The state number of the probe beam	l_s	The state number of the signal beam
$\omega_p(z)$	The beam radius of the probe beam	$\omega_s(z)$	The beam radius of the signal beam
ω_{0_p}	The beam waist of the probe beam	ω_{0_s}	The beam waist of the signal beam

$$\begin{aligned}C=&\left(\frac{1}{\omega_s(z)}\right)^{1+2|l_s|}\left(\frac{1}{\omega_s^2(z)}+\frac{1}{\omega_p^2(z)}\right)^{-1-|l_s|-|l_p|}\\&\cdot\left(\frac{1}{\omega_p(z)}\right)^{1+2|l_p|}\cdot 2^{1+|l_s|+|l_p|}\\&\cdot\frac{\Gamma\left(1+\left|l_s\right|+\left|l_p\right|\right)}{\sqrt{\Gamma\left(1+2\left|l_s\right|\right)\cdot\Gamma\left(1+2\left|l_p\right|\right)}},\end{aligned} \quad (4)$$

where $\Gamma(\cdot)$ represents the classical gamma function.

We can derive the optimal beam waist ω_{0_p} of the probe beam for maximizing C by solving the following equation

$$\frac{\partial C}{\partial\omega_{0\_p}}=\frac{\partial C}{\partial\omega_p}\cdot\frac{\partial\omega_p}{\partial\omega_{0\_p}}=0. \quad (5)$$

Upon combining (2) and (5), and solving (5), we can determine the relationship between $\omega_p(z)$ and $\omega_s(z)$

$$\omega_p(z)=\sqrt{\frac{2\left|l_s\right|+1}{2\left|l_p\right|+1}}\cdot\omega_s(z). \quad (6)$$

The mathematical expression of the probe beam broadening in an OAM-OWC link is shown in (6). When the beam radii of the probe and signal beam satisfy the relationship shown in (6), the correlation coefficient C is maximized, as is the intensity distribution similarity of the two beams.

Note that the optimal beam waist of the probe beam is calculated by (2) and (6) based on the longest propagation distance. The above derivation describes a single OAM channel associated with the transmission state index l_s. By contrast, for multiple links, $|l_s|$ represents the maximum absolute value of the state index in the transmitted OAM beams [22].

C. Single-intensity-measurement based phase retrieval algorithm

In this section, we describe an SPRA that estimates the wave-front of an OAM beam based on its Fourier intensity and on the knowledge of the object constraints. The flow-chart of the SPRA is shown in Fig. 4.

Let us denote the optical field of the received probe beam in the object domain as $f(x,y)$ and in the Fourier domain as $F(u,v)$, where (x,y) are the associated spatial coordinates and (u,v) are the spatial frequency coordinates. The object domain represents here the distorted probe beam $f(x,y)$ of

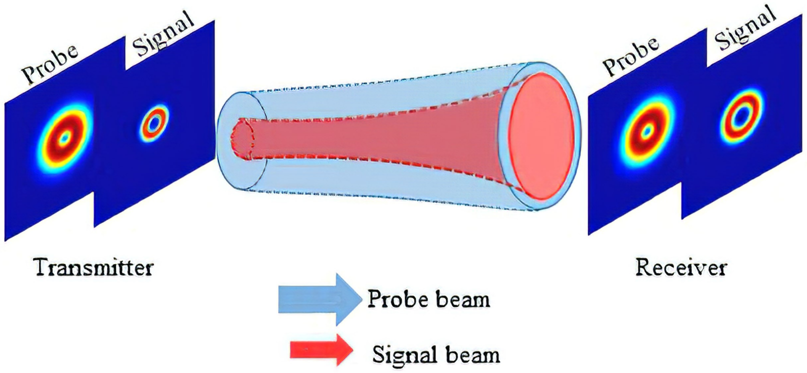


Fig. 3. Stylized propagation of both the OAM signalling beam and expanded probe beam.

the OAM-OWC system, which corresponds to the optical field distribution in the front focal plane of L1 in Fig. 1. Furthermore, $|F(u,v)|$ is the real-valued modulus obtained by taking the square root of the Fourier intensity of the object, which is measured by the CCD of Fig. 1.

Appropriate initialization assists in prompt and accurate convergence. We set the initial estimated object of the SPRA to $g_0(x,y) = \mathscr{F}^{-1}\left\{|F(u,v)| \cdot e^{j\theta_0(u,v)}\right\}$, where θ_0 is set to the phase distribution of the no-turbulence probe beam in the Fourier domain. As shown in Fig. 4, the SPRA consists of the following four steps at the k-th iteration [24]:

(1) From g_k to G_k: Fourier transform g_k;

(2) From G_k to $G_k^{'}$: Replace the modulus of the resultant Fourier transform G_k with the aid of the measured Fourier modulus $|F(u,v)|$ in order to form an estimate of the Fourier transform $G_k^{'}$;

(3) From $G_k^{'}$ to $g_k^{'}$: Inverse Fourier transform the estimate of the Fourier transform $G_k^{'}$ in order to form an estimate of the object $g_k^{'}$;

(4) From $g_k^{'}$ to g_{k+1} : Calculate the input of the next iteration g_{k+1} that satisfies the object constraints [23]. The fourth step is designed by referring to the negative feedback, which can be expressed as

$$g_{k+1}(x,y) = \begin{cases} g_k'(x,y), & (x,y) \in \gamma, \\ g_k(x,y) - \beta g_k'(x,y), & (x,y) \notin \gamma, \end{cases} \tag{7}$$

where γ represents the object constraints and β is a constant feedback parameter having typical values between 0.5 and 1.

The algorithm terminates when the iterations satisfy the termination criterion or reach a given number.

In the proposed SPRA the only known information is the modulus in the Fourier domain $|F(u,v)|$, hence we need sufficient prior information about the object in order to estimate its phase accurately [34]. The OAM beam has the unique characteristic that the beam width is related both to the state index and to the beam waist [31]. In order to achieve accurate compensation, we rely on the diameter constraints as the prior information in the SPRA.

For considering the intensity distribution of the OAM beam, we introduce the diameter constraints as partial constraints of the object quantified by the centrosymmetric circular region γ, which contains more than 99% of the transmitted intensity of the probe beam. The radius of the circular region can be expressed as

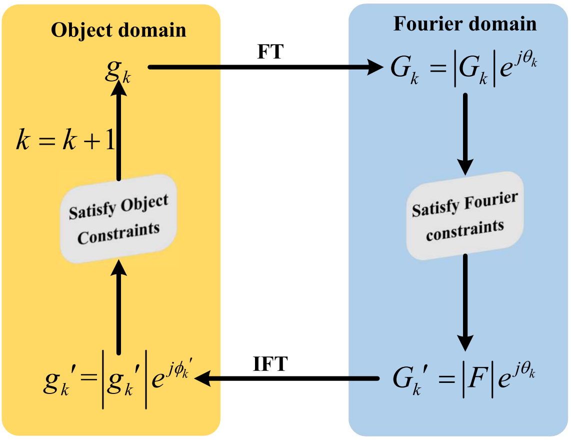

Object domain
Fourier domain
FT
IFT
g_k
$G_k = |G_k| e^{j\theta_k}$
$k = k+1$
Satisfy Object Constraints
Satisfy Fourier constraints
$g_k' = |g_k'| e^{j\phi_k'}$
$G_k' = |F| e^{j\theta_k}$

Fig. 4. The flow-chart of the SPRA. (FT: Fourier transformation; IFT: inverse Fourier transformation.)

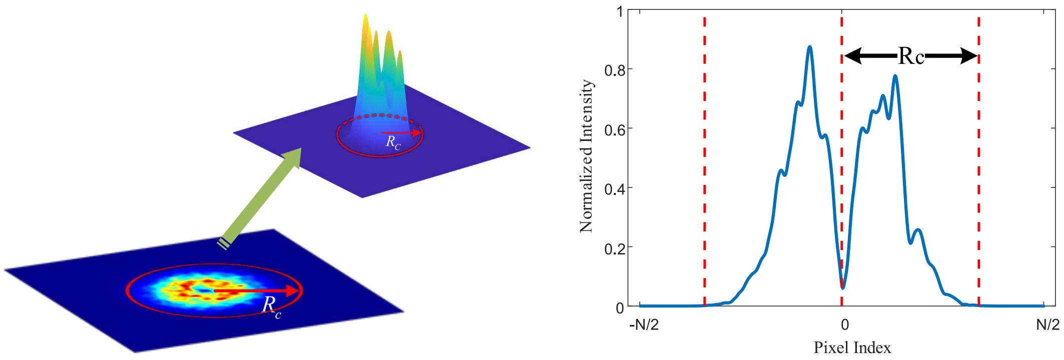
$$R_C = 2\omega_p(z)\sqrt{|l_p|+1}, \tag{8}$$

where $\omega_p(z)$ and l_p represent the beam radius and state index of the probe beam, respectively [24]. An example of the object constraint is given in Fig. 5 from the perspectives of the intensity distribution and the line intensity profile [1]. As shown in Fig. 5, for $(x,y) \in \gamma$ of the distorted probe beam, the next estimated object g_{k+1} is equal to g_k'. We assume that the intensity of the probe beam in the absence of turbulence in $(x,y) \notin \gamma$ is zero. Therefore, for $(x,y) \notin \gamma$, the SPRA provides negative feedback from the most recently estimated object g_k to drive the next estimated object g_{k+1} towards zero, as shown in (7) [22].

D. Robustness analysis of PRA-AO techniques

Sensing light intensity is fundamental to any wave-front sensor technique [27]. As mentioned above, both the DPRA-

[1] Line intensity profile is defined as the teo-deminsional intensity distribution along the horizontal radial vortex centers of the OAM beam.



(a) (b)

Fig. 5. (a) The object constraints and the intensity distribution of the broadened probe beam. (b) Diagram of the constraints and the line intensity profile along the center of the probe beam. (N: the number of grid points.)

TABLE III
THE EXPLANATIONS OF THE NOISE TYPES USED IN THE NOISE MODEL

Noise type	Notation	Noise model
Background noise	N_0	Complex Gaussian white noise
Detector noise	N_i	Shot noise and readout noise
Shot noise	N_{s_i}	Poisson noise
Readout noise	N_{r_i}	Gaussian white noise

AO and SPRA-AO estimate the phase impairment from the measured intensity information, and it is vitally important to analyze the detector-noise resistance of PRAs. At the time of writing there is a paucity of literature on the robustness of the AO approach in OAM-OWC links. We commence our evaluation of the robustness of SPRA-AO techniques by establishing the noise model of the SPRA-AO and DPRA-AO. The principle of GSA-AO has been detailed in [21], while the schematic of the DPRA-AO and SPRA-AO techniques and their noise models are shown in Fig. 6(a) and Fig. 6(b), respectively.

The noise components contaminating the detectors are assumed to be independently and identically distributed and their features are shown at a glance in Table III. The background noise, denoted as N_0, is modeled by a complex Gaussian white noise process of mean 0 and variance σ_0^2 [35], [36]. As for the CCD detector noise, we consider the situation in which the detector noise consists of a combination of shot noise and readout noise. The shot noise is mainly a combination of photon noise and dark noise, both exhibiting a Poisson distribution, since they are based on the random arrival of photos at the CCD of Fig. 6 [37]. The readout noise is imposed on the signal during the process of measuring the signal and it is also assumed to be Gaussian white noise of mean 0 and variance σ_1^2 [38]. The detector noise N_j is given by [39]

$$N_j = N_{s_j} + N_{r_j} \quad i = (1,2,3), \tag{9}$$

where j represents the CCD index of Fig. 6. Note that there is no extra parameter associated with the Poisson noise, but the noise magnitude depends on the intensity of the signal entering the CCD [40].

At the receiver, the contaminated probe beam is denoted as $u_r(r,\phi,z)$, which contains the additive background noise N_0 perturbing the multiplexed beam. For the DPRA-AO technique associated with the noise model of Fig. 6(a), the two inputs of the DPRA can be expressed as [21]

$$|f(x,y)| = \sqrt{I_{CCD1}} = \sqrt{\frac{|u_r(r,\phi,z)|^2}{2} + N_1}, \tag{10}$$

$$|F(u,v)| = \sqrt{I_{CCD2}} = \sqrt{\left|\mathscr{F}\left[\frac{u_r(r,\phi,z)}{\sqrt{2}}\right]\right|^2 + N_2}. \tag{11}$$

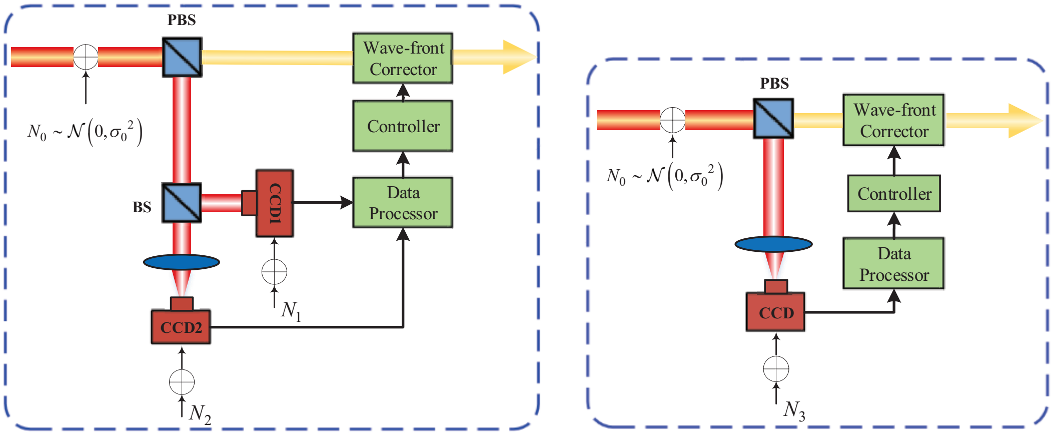
For the SPRA-AO technique having the noise model of Fig. 6(b), one of the SPRA inputs is expressed as

$$|F_s(u,v)| = \sqrt{I_{CCD3}} = \sqrt{|\mathscr{F}\left[u_r(r,\phi,z)\right]|^2 + N_3}, \tag{12}$$

where I_{CCD_3} represents the intensity captured by the CCD$_3$ of Fig. 6(b) and N_3 is the additive detector noise contaminating the magnitude of the probe beam in the Fourier domain for the SPRA.

III. SIMULATIONS AND DISCUSSIONS

In the following, we simulate the propagation of the OAM beam in AT with random phase screens based on Kolmogorov's turbulence theory along the propagation path. The random process of turbulence is typically characterized in statistical theory, because the complexity of the atmosphere does not lend itself to prediction and numerical analysis. Kolmogorov's turbulence theory describes the average effects of total beam wander, beam spreading, and scintillation [41]. In our study, the propagation of the OAM beams through a locally homogeneous and isotropic turbulent medium, which exhibits modified Von-Karman atmospheric phase characteristics [42], is modeled relying on the simulation tool MATLAB. The structure constant of the refractive index C_n^2 is varied in the range of $1 \times 10^{-16} \sim 1 \times 10^{-14}\mathrm{m}^{-2/3}$. As for the simulation parameters, the number of grid points per side is 756. The wavelength λ is set to $532\mathrm{nm}$. The number of random phase screens is 11 along the propagation path. Furthermore,



(a) The GSA-AO system and its noise model

(b) The SPRA-AO system and its noise model

Fig. 6. Schematic of the AO system and its noise model. (BS: beam splitter (50:50).)

the outer and inner scale of turbulence are 50m and 0.01m, respectively. The receiver aperture size is set to 0.3m and the β factor of the SPRA is set to 0.7 [31]. For a given propagation distance, we set the waist of the signal beam to $\omega_{0\_s} = \sqrt{\lambda z/\pi}$ at the transmitter [43]. As for the parameters of the probe beam, the probe beam is an OAM beam associated with $l_p = 1$ and the waist of the expanded probe beam follows (6). As an example, for $z = 400\text{m}$ and $l_s = 3$, the waist of the signal beam ω_{0_s} is 0.0082m and the waist of probe beam ω_{0_p} can be calculated as 0.017m.

A. Compensation performance analysis of the SPRA-AO technique

The OAM spectrum is calculated by relying on the so-called modal decomposition method to characterize the ratio of the power retained by the original transmit state and of the power spread into the adjacent channels. The power associated with the OAM spectrum characterizes the specific proportion of each state [44]. We define the mode purity as the relative power of the desired transmit state in the OAM spectrum, and define the crosstalk as the relative power of the undesired state. The values of mode purity and crosstalk are between 0 and 1, where high mode purity and low crosstalk correspond to a better quality of the OAM beam. Moreover, we define the squared error (SE) function for quantifying the compensation performance, which can be expressed as

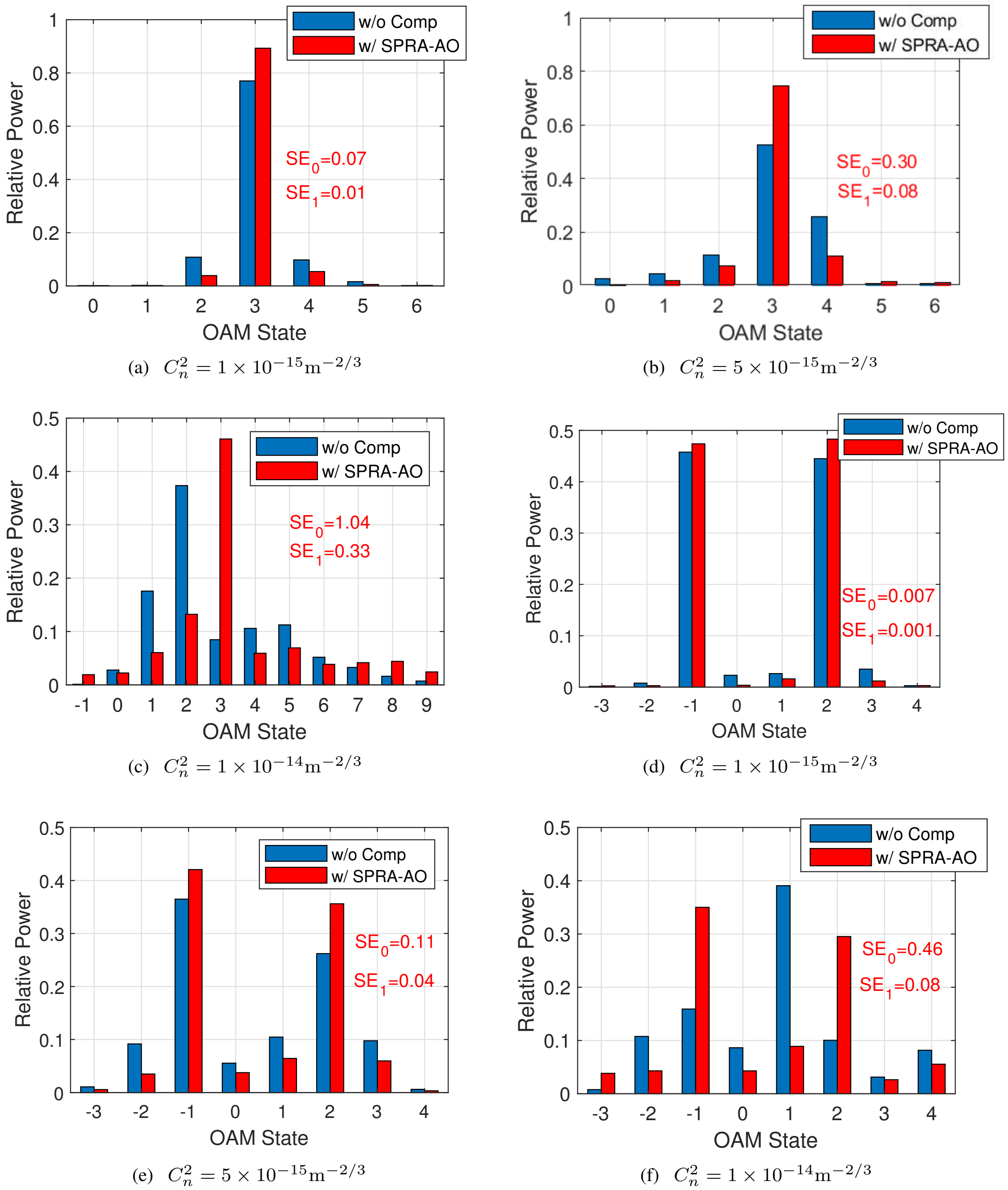
$$\text{SE} = \sum_i |p_w(i) - p_0(i)|^2 , \tag{13}$$

where the variable i represents the state index of the OAM beam; $p_w(i)$ is the relative power of the OAM state index i of the OAM beam with/without SPRA-AO compensation; and $p_0(i)$ is the relative power of the OAM state index i of the desired OAM beam in the absence of turbulence. A smaller SE value corresponds to a better correction performance.

We consider the OAM states $l = 3$ and $l = \{-1, +2\}$ as examples of single-channel and multiplexed-channel communication, respectively, for characterizing the compensation performance of the SPRA-AO technique. Fig. 7 shows the spectrum of the OAM signal beams both with and without SPRA-AO compensation under different turbulence strengths. The SE values are labeled in Fig. 7(a) - 7(f), where SE_0 corresponds to the SE values before compensation, while SE_1 corresponds to the values after SPRA-AO compensation. The SPRA-AO technique has substantial advantages in terms of accuracy by mitigating the impairments of both single-channel and multiplexed OAM-OWC systems. After SPRA-AO compensation, the relative power of the desired state increases, while the crosstalk between adjacent states is mitigated, hence the SE values are significantly reduced. Explicitly, the mode purity is improved from 0.52 to 0.74 after compensation, as shown in Fig. 7(b). In Fig. 7(c), the crosstalk of $l = 3$ imposed on the adjacent mode $l = 2$ is significantly reduced from 0.37 to 0.13 after compensation. Furthermore, the squared error is reduced from 0.11 to 0.04 after compensation, as seen in Fig. 7(e).

To illustrate the improvement of system's power penalty, the bit error rate (BER) both with and without SPRA-AO compensation is calculated based on [28], when an OAM beam associated with $l = 3$ is transmitted under the atmospheric structure constants of $C_n^2 = 1 \times 10^{-15}\text{m}^{-2/3}$ and $C_n^2 = 1 \times 10^{-14}\text{m}^{-2/3}$. The traditional GSA-AO scheme is used for benchmarking the BER improvement of the SPRA-AO and DPRA-AO techniques. During the BER calculations, we assume that on-off keying or binary pulse position modulation is used [30]. Fig. 8 presents the BER curves as a function of the optical signal-to-noise ratio (OSNR), when an OAM beam with $l = 3$ is transmitted [11]. Fig. 8(a) and 8(b) show that after SPRA-AO compensation, the BER performance improves as a benefit of the corrected OAM beam, and the BER falls below the forward error correction (FEC) limit of 3.8×10^{-3}. Furthermore, the BER is considerably reduced from 0.275 to 1.2×10^{-4} and 3.1×10^{-4} relying on SPRA-AO and GSA-AO compensation, when the OSNR is set to 17dB, as shown in Fig. 8(b). It can be concluded from Fig. 8(a) and (b) that our low-complexity SPRA-AO achieves a similar compensation performance to that of GSA-AO.

The convergence performance is a critical performance



(a) $C_n^2 = 1 \times 10^{-15}\mathrm{m}^{-2/3}$

(b) $C_n^2 = 5 \times 10^{-15}\mathrm{m}^{-2/3}$

(c) $C_n^2 = 1 \times 10^{-14}\mathrm{m}^{-2/3}$

(d) $C_n^2 = 1 \times 10^{-15}\mathrm{m}^{-2/3}$

(e) $C_n^2 = 5 \times 10^{-15}\mathrm{m}^{-2/3}$

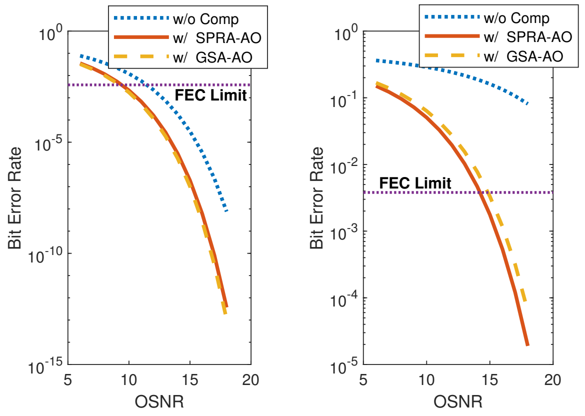
(f) $C_n^2 = 1 \times 10^{-14}\mathrm{m}^{-2/3}$

Fig. 7. OAM spectrum of the OAM beam with or without SPRA-AO compensation. (a)-(c) In the case of a single-OAM link for $l = 3$. (d)-(f) In the case of a multiplexed-channel link for $l = \{-1, +2\}$. The propagation distance is 400 m.

criterion of the algorithm. The traditional GSA-AO scheme is used for benchmarking the convergence performance of the SPRA and GSA. The OAM spectrum of the signal beam using $l = 3$ before and after SPRA-AO and GSA-AO compensation is shown in Fig. 9(a), while the corresponding convergence curve is shown in Fig. 9(b). It can be concluded from Fig. 9(a) and 9(b) that SPRA-AO and GSA-AO can achieve a similar compensation performance and then the SPRA exhibits better convergence speed than the GSA.

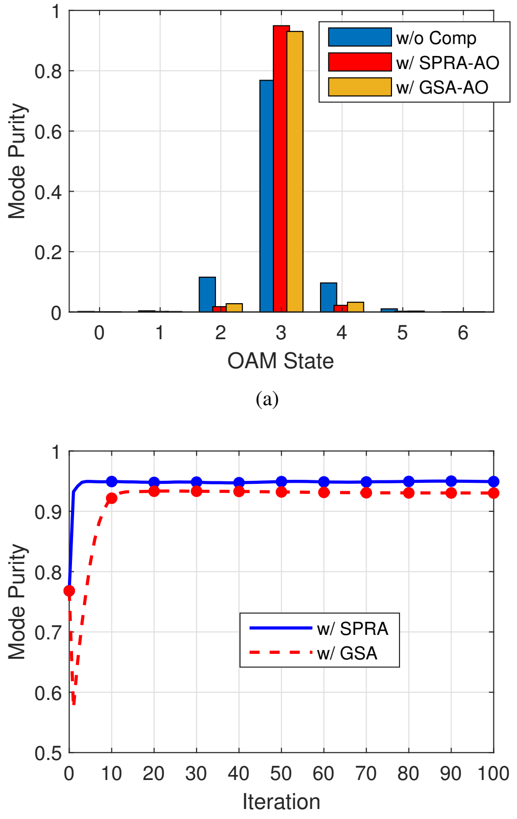
B. Discussion of the probe beam expansion

Recall from Section II B that for accurate phase-compensation the expanded probe beam has to remain wider than the signal beam during their collinear propagation. Hence, to reflect the benefits of the probe beam expansion, we now carry out a detailed comparative analysis of three different expansion schemes. The beam waist of the probe beam associated with the different expansion schemes is listed in Table IV, where ω_{0_s} is the beam waist of the signal beam and ω_{0_p} is that of the expanded probe beam calculated according to (8). As shown in Table IV, the beam waist of the probe is



(a) $C_n^2 = 1 \times 10^{-15}\mathrm{m}^{-2/3}$ (b) $C_n^2 = 1 \times 10^{-14}\mathrm{m}^{-2/3}$

Fig. 8. BER as a function of the OSNR when an OAM beam using $l = 3$ is transmitted both with and without SPRA and GSA-AO compensation for different atmospheric structure constant. The propagation distance is 400 m.



(a)

(b)

Fig. 9. (a) The OAM spectrum of the signal beam associated with $l = 3$ both before and after SPRA-AO and GSA-AO compensation. (b) Mode purity as a function of the number of iterations for the SPRA and GSA. ($C_n^2 = 2 \times 10^{-15}\mathrm{m}^{-2/3}$)

TABLE IV
THE BEAM WAIST OF THE PROBE BEAM WITH DIFFERENT EXPANSION SCHEME

Expansion scheme	Without expansion	Expansion 1	Expansion 2
Beam waist of probe beam	ω_{0_s}	ω_{0_p}	$2\omega_{0\_p}$

TABLE V
THE DETAILED PARAMETERS OF THE DIFFERENT EXPANSION SCHEMES

Parameter Type	Value
State index of signal beam	3
State index of probe beam	1
Beam waist of signal beam	0.0082m
Beam waist of probe beam without expansion	0.0082m
Beam waist of probe beam with Expansion 1	0.0173m
Beam waist of probe beam with Expansion 2	0.0346m

equal to that of the signal if there is no probe expansion. In this context, Expansion 1 represents the scheme we proposed in Section II B, while Expansion 2 represents an oversized probe beam. The detailed parameters with different expansion scheme are shown in Table V.

The curves of the mode purity and the OAM state index recorded both before and after compensation are shown in Fig. 10. The curve marked by stars represents the mode purity after SPRA-AO compensation using Expansion 1, while the curves marked by triangles and squares represent the mode purity after compensation without probe expansion and with Expansion 2, respectively. The results show that the SPRA-AO relying on the proposed expansion scheme substantially improves the mode purity of OAM beams having different state indices and reduces the distortion of the OAM beam. Furthermore, Fig. 10 shows that the mode purity recorded either after compensation without expansion or by using an inappropriate oversized expansion (Expansion 2) is even lower than that without compensation, confirming that beam expansion is necessary in a high-performance AO system.

This phenomenon of Fig. 10 can be explained as follows by relying on a signal beam associated with $l = 7$ as an example. Fig. 11 shows the line intensity profiles [2] along the vortex centers of the signal beam and probe beam both with and without expansion. Compared to the probe beam without expansion or to that with oversized expansion, the probe beam using the proposed expansion has a more similar cross section of the intensity distribution to that of the signal beam and undergoes more similar wave-front aberration, when propagating collinearly with the signal beam through atmospheric turbulence.

The relationship between the propagation distance and mode purity of the signal beam of $l = 7$ before and after compensation is shown in Fig. 12. Each value of mode purity represents an average of 100 realizations. The curve marked with stars in Fig. 12 shows that the SPRA-AO technique compensates the distorted OAM beam quite effectively within 800 m. Fig.

[2] How these were generated was discussed in a footnote in Section II C.

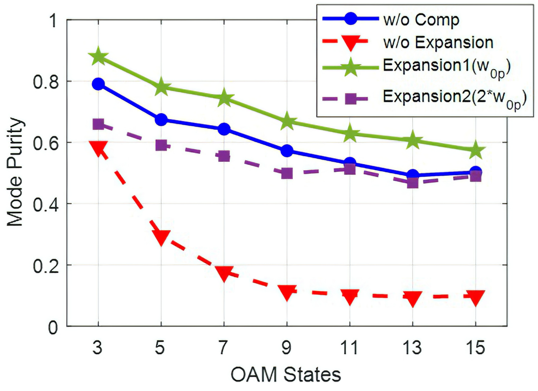


Fig. 10. Mode purity as a function of the transmission state index of signal beams before/after the SPRA-AO operating both with and without probe beam expansion. ($C_n^2 = 2 \times 10^{-15}\mathrm{m}^{-2/3}$, $z = 400$m.)

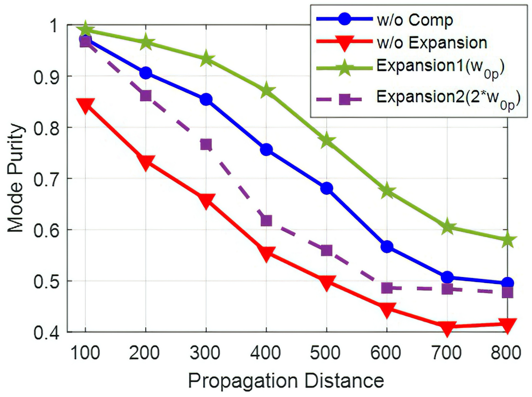
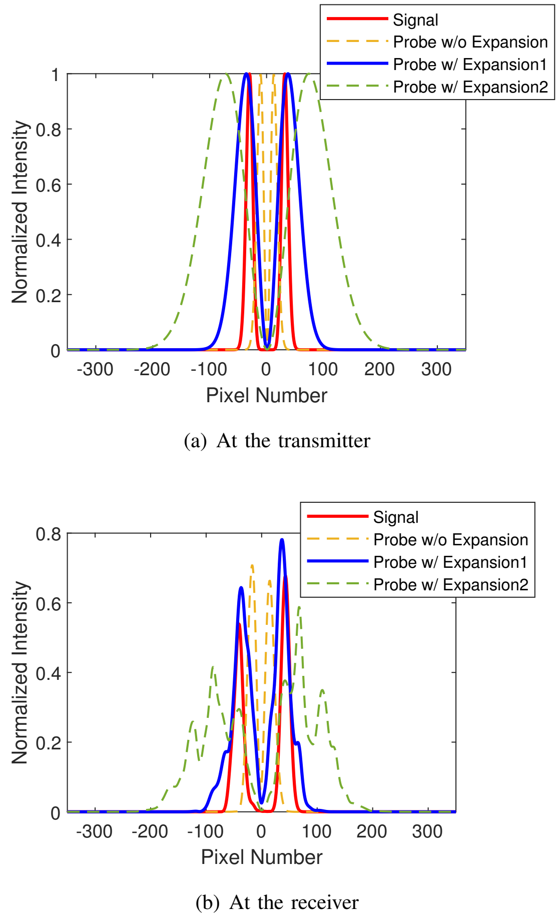


Fig. 12. Mode purity of the signal beam versus the propagation distance with/without SPRA-AO compensation. ($C_n^2 = 2 \times 10^{-15}\mathrm{m}^{-2/3}$.)



(a) At the transmitter

(b) At the receiver

Fig. 11. Line intensity profiles along the vortex centers of the signal beam with l=7 and the probe beam with and without expansion. ($C_n^2 = 2 \times 10^{-15}\mathrm{m}^{-2/3}$, $z = 400$m.)

12 also indicates the importance of using the most appropriate expansion of the probe beam in an AO system.

C. Robustness analysis of the SPRA-AO technique

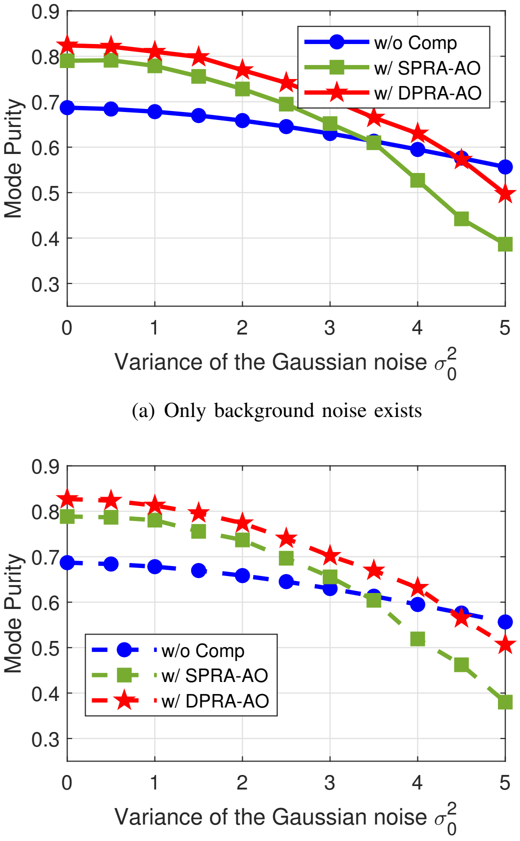
Having verified the efficiency of the SPRA-AO technique and the benefits of probe expansion, we now further analyze the robustness of the SPRA-AO against both the background noise and the CCD detector noise.

We first qualify how the background noise affects the compensation performance of the PRA-AO systems. Fig. 13(a) shows the mode purity as a function of σ_0^2 using the SPRA-AO and DPRA-AO techniques when only the background noise N_0 exists. We run the tests 100 times under different σ_0^2 values and take the average of the mode purity results. Fig. 13(a) shows that despite AO compensation, the mode purity is reduced upon increasing σ_0^2, which means that the background noise degrades the AO compensation performance regardless of whether the SPRA-AO or the DPRA-AO technique is used. In Fig. 13(a), the mode purity equals to 0.65, 0.72 and 0.77 before compensation as well as after SPRA-AO and DPRA-AO compensation, respectively, when $\sigma_0^2 = 2$. This trend is indeed expected because the intensities in both the object and the Fourier domain are exploited as prior information by the DPRA, while the SPRA uses only the intensity in the Fourier domain as its measured input. It can be concluded that the SPRA-based AO technique exhibits eroded compensation performance with less prior information in exchange for its simplicity.

The curves of the mode purity vs σ_0^2 are shown in Fig. 13(b), when both the background noise and the shot noise of the detector exist. Observe that the mode purity seen in Fig. 13(a) and Fig. 13(b) both with and without shot noise are similar. Therefore, the shot noise is not the dominant factor that affects the compensation performance. It can be concluded that both SPRA-AO and DPRA-AO are robust against shot noise.

Let us now introduce both background noise and detector noise - including shot noise and readout noise - into the AO module. The mode purity vs the readout Gaussian noise variance σ_1^2 is shown in Fig. 14, where we observe that upon increasing σ_1^2, the mode purity of SPRA-AO compensation is seen to be more stable than that having DPRA-AO compensation. We conclude that SPRA-AO exhibits unique robustness than DPRA-AO in AO-based OAM-OWC systems.

This phenomenon can be explained as follows. Recall from Fig. 6 that in the DPRA-AO system, the contaminated probe beam is split by a BS into two copies for detecting the intensities in the object and Fourier domain. The split input



(a) Only background noise exists

(b) Both the background noise and the shot noise of the CCD detector exist

Fig. 13. Mode purity versus the background noise variance σ_0^2 for the SPRA and DPRA-AO techniques, when an OAM beam associated with $l = 3$ is transmitted. ($C_n^2 = 3 \times 10^{-15}\mathrm{m}^{-2/3}$, $z = 400\mathrm{m}$.)

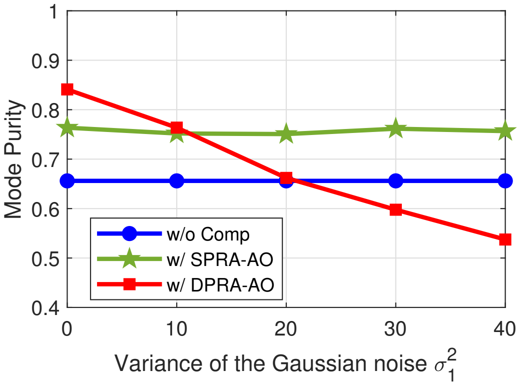


Fig. 14. Mode purity as a function of the Gaussian noise variance when an OAM beam with $l = 3$ is transmitted. ($C_n^2 = 3 \times 10^{-15}\mathrm{m}^{-2/3}$, $z = 400\mathrm{m}$,$\sigma_0^2 = 2$.)

intensity of the DPRA is halved and the use of two CCD detectors - instead of a single one - increases the number of noise sources. As for the SPRA-AO module, the probe beam does not have to be split, and only a single detector-noise component is considered. Additionally, the intensity in the Fourier domain is concentrated on the focal domain by the Fourier lens. Compared to the influence of the readout noise on the intensity in the object domain, the effect of noise having the same variance imposed on the Fourier intensity in the back focal plane is lower. This is also the reason that the mode purity associated with SPRA-AO compensation remains almost unchanged. From this perspective, the SPRA-AO system is more robust than the DPRA-AO system.

IV. Conclusions

In conclusion, we conceived and characterized a low-complexity and high-robustness SPRA-based AO technique capable of compensating for the distortion of the OAM beam in OWC links. Only the intensity of the probe beam in the Fourier domain is required as the measured data of the SPRA wave-front sensor. Moreover, a probe beam expansion scheme was proposed for OAM-OWC links for enhancing the performance of the SPRA. Our simulation results illustrate that the SPRA-AO technique advocated is capable of decontaminating the OAM beam, ameliorating its mode purity and reducing the crosstalk, hence improving the BER performance of OAM-OWC links. Compared to GSA-AO, the SPRA-AO achieves a similar compensation performance at a lower system complexity. Additionally, the results show that the SPRA-AO relying on the proposed expansion scheme accurately improves the mode purity of OAM beams associated with different state indices. Finally, we mathematically analyzed the robustness of the SPRA-AO. Our simulation results show that the background noise degrades the AO compensation performance, regardless whether the SPRA-AO or DPRA-AO approach is used. Under the conditions that both background noise and detector noise are experienced, SPRA-AO exhibits better robustness than DPRA-AO in AO-based OAM-OWC systems.

Our future research may focus on the improvement of the SPRA-AO compensation to make miniaturized low-cost implementations a reality. Moreover, the feasibility of the transmission vector OAM mode will also be explored in our further research. Our work paves the way toward the practical application of PRA-based compensation in the AO field and in OAM-OWC systems.

References

[1] Y. Yang, W. Cheng, W. Zhang, and H. Zhang, "Mode modulation for wireless communications with a twist," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 11, pp. 10 704–10 714, Nov. 2018.

[2] J. Wang, C. Jiang, K. Zhang, X. Hou, Y. Ren, and Y. Qian, "Distributed Q-learning aided heterogeneous network association for energy-efficient IIoT," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 4, pp. 2756–2764, Nov. 2020.

[3] Z. Sun, H. Yu, Y. Zhu, and Z. Tian, "An addition-decomposable relaying protocol and signal design for optical wireless communications," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 7, pp. 5980–5993, Feb. 2018.

[4] H. Yao, T. Mai, J. Wang, Z. Ji, C. Jiang, and Y. Qian, “Resource trading in blockchain-based industrial Internet of Things,” *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3602–3609, Jun. 2019.

[5] J. Wang, C. Jiang, H. Zhang, Y. Ren, K.-C. Chen, and L. Hanzo, “Thirty years of machine learning: The road to Pareto-optimal wireless networks,” *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1472–1514, Jan. 2020.

[6] M. Li, “Orbital angular momentum multiplexing optical wireless communications with adaptive modes adjustment in Internet of Things Network,” *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6134–6139, Aug. 2019.

[7] L. Liang, W. Cheng, W. Zhang, and H. Zhang, “Joint OAM multiplexing and OFDM in sparse multipath environments,” *IEEE Transactions on Vehicular Technology*, vol. 69, no. 4, pp. 3864–3878, Apr. 2020.

[8] A. E. Willner, Y. X. Ren, G. D. Xie, Y. Yan, L. Li, Z. Zhao, J. Wang, M. Tur, A. F. Molisch, and S. Ashrafi, “Recent advances in high-capacity free-space optical and radio-frequency communications using orbital angular momentum multiplexing,” *Philosophical Transactions*, vol. 375, no. 2087, p. 20150439, Feb. 2017.

[9] M. I. Dedo, Z. K. Wang, K. Guo, and Z. Y. Guo, “OAM mode recognition based on joint scheme of combining the Gerchberg-Saxton (GS) algorithm and convolutional neural network (CNN),” *Optics Communications*, vol. 456, p. 124696, Feb. 2019.

[10] W. Zhang, S. Zheng, X. Hui, R. Dong, X. Jin, H. Chi, and X. Zhang, “Mode division multiplexing communication using microwave orbital angular momentum: An experimental study,” *IEEE Transactions on Wireless Communications*, vol. 16, no. 2, pp. 1308–1318, Feb. 2017.

[11] C. H. Kai, Z. K. Feng, M. I. Dedo, P. Huang, K. Guo, F. Shen, J. Gao, and Z. Y. Guo, “The performances of different OAM encoding systems,” *Optics Communications*, vol. 430, pp. 151–157, Jan. 2018.

[12] A. E. Willner, G. D. Xie, L. Li, and Y. X. Ren, “Channel effects and mitigation approaches in free-space and underwater optical communications using orbital angular momentum multiplexing,” in *Asia Communications & Photonics Conference*, Wuhan, China, Nov. 2016.

[13] A. Trichili, K. Park, M. Zghal, B. S. Ooi, and M. Alouini, “Communicating using spatial mode multiplexing: Potentials, Challenges, and Perspectives,” *IEEE Communications Surveys Tutorials*, vol. 21, no. 4, pp. 3175–3203, May 2019.

[14] C. Yang, K. Shan, J. Chen, J. Hou, and S. Chen, “CNN-based phase matching for the OAM mode selection in turbulence heterodyne coherent mitigation links,” *IEEE Photonics Journal*, vol. 12, no. 6, pp. 1–13, Dec. 2020.

[15] G. D. Xie, Y. X. Ren, H. Hao, P. J. Martin, N. Ahmed, Y. Yan, C. J. Bao, L. Li, Z. Zhao, Y. W. Cao, M. Willner, M. Tur, S. J. Dolinar, R. W. Boyd, J. H. Shapiro, and A. E. Willner, “Phase correction for a distorted orbital angular momentum beam using a Zernike polynomials-based stochastic-parallel-gradient-descent algorithm,” *Optics Letters*, vol. 40, no. 7, pp. 1197–1200, Apr. 2015.

[16] A. E. Willner, H.Huang, Y. Yan, Y. X. Ren, and S. Ashraf, “Optical communications using orbital angular momentum beams,” *Advances in Optics & Photonics*, vol. 7, no. 1, pp. 66–106, Mar. 2015.

[17] M. Li, “Phase corrections with adaptive optics and Gerchberg-Saxton iteration: a comparison,” *IEEE Access*, vol. 56, no. 2, pp. 284–297, Oct. 2019.

[18] S. M. Zhao, J. Leach, L. Y. Gong, J. Ding, and B. Y. Zheng, “Aberration corrections for free-space optical communications in atmosphere turbulence using orbital angular momentum states,” *Optics Express*, vol. 20, no. 1, pp. 452–461, Jan. 2012.

[19] Y. X. Ren, H. Huang, J. Y. Yang, Y. Yan, N. Ahmed, Y. Yue, A. E. Willner, K. Birnbaum, J. Choi, B. Erkmen, and S. Dolinar, “Correction of phase distortion of an OAM mode using GS algorithm based phase retrieval,” in *Proc. CLEO 2012*, San Jose, California, USA, 2012, p. CF3I.4.

[20] S. Y. Fu, S. K. Zhang, T. L. Wang, and C. Q. Gao, “Pre-turbulence compensation of orbital angular momentum beams based on a probe and the Gerchberg–Saxton algorithm,” *Optics Letters*, vol. 41, no. 14, pp. 3185–3188, Jul 2016.

[21] H. Chang, X. L. Yin, X. Z. Cui, Z. Z. Zhang, J. X. M. andG. H. Wu, L. J. Zhang, and X. J. Xin, “Adaptive optics compensation of orbital angular momentum beams with a modified Gerchberg-Saxton-based phase retrieval algorithm,” *Optics Communications*, vol. 405, no. 2, pp. 271–275, Dec. 2017.

[22] X. L. Yin, H. Chang, X. Z. Cui, J. X. Ma, Y. J. Wang, G. H. Wu, L. J. Zhang, and X. J. Xin, “Adaptive turbulence compensation with a hybrid input–output algorithm in orbital angular momentum-based free-space optical communication,” *Applied Optics*, vol. 57, no. 26, pp. 7644–7650, Sep. 2018.

[23] J. Fienup, “Comments on ”the reconstruction of a multidimensional sequence from the phase or magnitude of its fourier transform”,” *IEEE Transactions on Acoustics, Speech, and Signal Processing*, vol. 31, no. 3, pp. 738–739, Jun. 1983.

[24] J. N. Cederquist, J. R. Fienup, C. C. Wackerman, S. R. Robinson, and D. Kryskowski, “Wave-front phase estimation from Fourier intensity measurements,” *Optical Society of America*, vol. 6, no. 7, pp. 1020–1026, Jul. 1989.

[25] X. Yuan, H. Yao, J. Wang, T. Mai, and M. Guizani, “Artificial intelligence empowered QoS-oriented network association for next-generation mobile networks,” *IEEE Transactions on Cognitive Communications and Networking*, pp. 1–1, Mar. 2021.

[26] H. Yao, B. Zhang, P. Zhang, S. Wu, C. Jiang, and S. Guo, “RDAM: A reinforcement learning based dynamic attribute matrix representation for virtual network embedding,” *IEEE Transactions on Emerging Topics in Computing*, vol. 9, no. 2, pp. 901–914, Apr. 2021.

[27] J. R. Fienup, “Phase retrieval algorithms: a comparison,” *Applied Optics*, vol. 21, no. 15, pp. 2758–2769, Aug. 1982.

[28] S. H. Li, S. Chen, C. Q. Gao, A. E. Willner, and J. Wang, “Atmospheric turbulence compensation in orbital angular momentum communications: Advances and perspectives,” *Optics Communications*, vol. 408, pp. 68–81, Feb. 2018.

[29] X. Zhong, Y. Zhao, G. Ren, S. He, and Z. Wu, “Influence of finite apertures on orthogonality and completeness of Laguerre-Gaussian beams,” *IEEE Access*, vol. 6, pp. 8742–8754, Feb. 2018.

[30] J. A. Anguita, M. A. Neifeld, and B. V. Vasic, “Turbulence-induced channel crosstalk in an orbital angular momentum-multiplexed free-space optical link,” *Applied Optics*, vol. 47, no. 13, pp. 2414–2429, May 2008.

[31] R. L. Phillips and L. C. Andrews, “Spot size and divergence for Laguerre Gaussian beams of any order,” *Applied Optics*, vol. 22, no. 5, pp. 643–644, Apr. 1983.

[32] Y. X. Ren, G. D. Xie, H. Huang, N. Ahmed, Y. Yan, L. Li, C. J. Bao, P. J. Lavery, M. Tur, and M. A. Neifeld, “Adaptive-optics-based simultaneous pre- and post-turbulence compensation of multiple orbital-angular-momentum beams in a bidirectional free-space optical link,” *Optica*, vol. 1, no. 6, p. 376, Dec. 2014.

[33] S. Nyberg, “Optical determination of the correlation coefficient,” *Optica Acta: International Journal of Optics*, vol. 19, no. 3, pp. 195–201, 1972.

[34] J. R. Fienup and T. R.Crimmins, “Reconstruction of the support of an object from the support of its autocorrelation,” *Journal of the Optical Society of America*, vol. 72, no. 5, pp. 610–624, Jan. 1982.

[35] S. Liu, B. M. Hennelly, and J. T. Sheridan, “Digital image watermarking spread space spread spectrum technique based on double random phase encoding,” *Optics Communications*, vol. 300, no. 2, pp. 162–177, Jul. 2013.

[36] B. T. Jiang, Y. H. Qiu, Y. Wen, and Z. Chen, “Modeling and analyzing the noise of CCD,” *Electro-Optic Technology Application*, vol. 25, no. 2, pp. 64–67, Apr. 2010.

[37] H. Faraji and W. J. Maclean., “CCD noise removal in digital images,” *IEEE Transactions on Image Processing*, vol. 15, no. 9, pp. 2676–2685, Sep. 2006.

[38] C. L. Guo, S. Liu, and J. T. Sheridan, “Optical double image encryption employing a pseudo image technique in the Fourier domain,” *Optics Communications*, vol. 321, no. 2, pp. 61–72, Jun. 2015.

[39] G. Healey and R. Kondepudy, “Radiometric CCD camera calibration and noise estimation,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 16, no. 3, pp. 267–176, Mar. 1994.

[40] T. Le, R. Chartrand, and T. J. Asaki, “A variational approach to reconstructing images corrupted by Poisson noise,” *Journal of Mathematical Imaging and Vision*, vol. 27, no. 3, pp. 257–263, Apr. 2007.

[41] R. L. Fante, “The effect of source temporal coherence on light scintillations in weak turbulence,” *Journal of the Optical Society of America A*, vol. 69, no. 1, pp. 71–73, Jan. 1979.

[42] S. Y. Fu and C. Q. Gao, “Influences of atmospheric turbulence effects on the orbital angular momentum spectra of vortex beams,” *Photonics Research*, vol. 4, no. 5, pp. B1–B4, Oct. 2016.

[43] X. L. Yin, Y. L. Guo, H. Yan, X. Z. Cui, H. Chang, Q. H. Tian, G. H. Wu, Q. Zhang, B. Liu, and X. J. Xin, “Analysis of orbital angular momentum spectra of Hankel-Bessel beams in channels with oceanic turbulence,” *Acta Physica Sinica*, vol. 67, no. 11, p. 114201, Jun. 2018.

[44] X. Z. Cui, X. L. Yin, H. Chang, Z. C. Zhang, Y. J. Wang, and G. H. Wu, “A new method of calculating the orbital angular momentum spectra of Laguerre–Gaussian beams in channels with atmospheric turbulence,” *Chinese Physics B*, vol. 26, no. 11, pp. 232–238, Nov. 2017.

Huan Chang received the Ph.D. degree from the Beijing University of Posts and Telecommunications (BUPT), China, in 2020. She is currently a postdoctor with the School of Information and Electronics, Beijing Institute of Technology. Her main research interests include wireless optical communication and adaptive optics.

Xiaoli Yin received the B.E. degree in applied electronic technology, the M.S. degree in optics, and the Ph.D. degree in physical electronics from the Beijing University of Posts and Telecommunications (BUPT), Beijing, China, in 1993, 1996, and 2008, respectively. She is currently a Professor at BUPT. Her research interests include optical communication and signal processing.

Haipeng Yao (M'16, SM'20) is an associate professor in Beijing University of Posts and Telecommunications. Haipeng Yao received his Ph.D. in the Department of Telecommunication Engineering at University of Beijing University of Posts and Telecommunications in 2011. His research interests include future network architecture, network artificial intelligence, networking, space-terrestrial integrated network, network resource allocation and dedicated networks. He has published more than 100 papers in prestigious peer-reviewed journals and conferences. Dr. Yao has served as an Editor of IEEE Network, IEEE Access, and a Guest Editor of IEEE Open Journal of the Computer Society and Springer Journal of Network and Systems Management. He has also served as a member of the technical program committee as well as the Symposium Chair for a number of international conferences, including IWCMC 2019 Symposium Chair, ACM TUR-C SIGSAC2020 Publication Chair.

Jingjing Wang (S'14-M'19-SM'21) received his B.S. degree in Electronic Information Engineering from Dalian University of Technology, Liaoning, China in 2014 and the Ph.D. degree in Information and Communication Engineering from Tsinghua University, Beijing, China in 2019, both with the highest honors. From 2017 to 2018, he visited the Next Generation Wireless Group chaired by Prof. Lajos Hanzo, University of Southampton, UK. Dr. Wang is currently a postdoc researcher at Department of Electronic Engineering, Tsinghua University. His research interests include AI enhanced next-generation wireless networks and swarm intelligence. Dr. Wang was a recipient of the Best Journal Paper Award of IEEE ComSoc Technical Committee on Green Communications & Computing in 2018, the Best Paper Award from IEEE ICC and IWCMC in 2019.

Ran Gao received the Ph.D. degree in electronic science and technology from the Beijing Institute of Technology, China, in 2015. He is currently a Professor with the School of Information and Electronics, Beijing Institute of Technology. His research interests include fiber optical sensors, optical waveguide, and measurement instruments.

Jianping An received the Ph.D. degree from the Beijing Institute of Technology, China, in 1996. He joined the School of Information and Electronics, Beijing Institute of Technology in 1995, where he is currently a Full Professor. He is also the Dean of the School of Information and Electronics, Beijing Institute of Technology. His research interests are in the fields of digital signal processing, cognitive radios, wireless networks, and high-dynamic broadband wireless transmission technology.

Lajos Hanzo (http://www-mobile.ecs.soton.ac.uk, https://en.wikipedia.org/wiki/Lajos_Hanzo) (FIEEE'04) received his Master degree and Doctorate in 1976 and 1983, respectively from the Technical University (TU) of Budapest. He was also awarded the Doctor of Sciences (DSc) degree by the University of Southampton (2004) and Honorary Doctorates by the TU of Budapest (2009) and by the University of Edinburgh (2015). He is a Foreign Member of the Hungarian Academy of Sciences and a former Editor-in-Chief of the IEEE Press. He has served several terms as Governor of both IEEE ComSoc and of VTS. He has published 2000+ contributions at IEEE Xplore, 19 Wiley-IEEE Press books and has helped the fast-track career of 123 PhD students. Over 40 of them are Professors at various stages of their careers in academia and many of them are leading scientists in the wireless industry. He is also a Fellow of the Royal Academy of Engineering (FREng), of the IET and of EURASIP.

Duality of Quantum and Classical Error Correction Codes: Design Principles & Examples

Zunaira Babar, Hung Viet Nguyen, Panagiotis Botsinis, Dimitrios Alanis, Daryus Chandra, Soon Xin Ng and Lajos Hanzo

***Abstract*—Quantum Error Correction Codes (QECCs) can be constructed from the known classical coding paradigm by exploiting the inherent isomorphism between the classical and quantum regimes, while also addressing the challenges imposed by the strange laws of quantum physics. In this spirit, this paper provides deep insights into the duality of quantum and classical coding theory, hence aiming for bridging the gap between them. Explicitly, we survey the rich history of both classical as well as quantum codes. We then provide a comprehensive slow-paced tutorial for constructing stabilizer-based QECCs from arbitrary binary as well as quaternary codes, as exemplified by the dual-containing and non-dual-containing Calderbank-Shor-Steane (CSS) codes, non-CSS codes and entanglement-assisted codes. Finally, we apply our discussions to two popular code families, namely to the family of Bose-Chaudhuri-Hocquenghem (BCH) as well as of convolutional codes and provide detailed design examples for both their classical as well as their quantum versions.**

***Keywords*—Channel Coding, Quantum Error Correction, BCH Codes, Convolutional Codes.**

ACRONYMS

ARQ	Automatic-Repeat-reQuest
AWGN	Additive White Gaussian Noise
BCH	Bose-Chaudhuri-Hocquenghem
BCJR	Bahl, Cocke, Jelinek and Raviv
BER	Bit Error Ratio
BICM	Bit-Interleaved Coded Modulation
BICM-ID	Bit-Interleaved Coded Modulation with Iterative Decoding
CNOT	Controlled-NOT
CRC	Cyclic Redundancy Check
CRSS	Calderbank-Rains-Shor-Sloane
CSS	Calderbank-Shor-Steane
EA	Entanglement-Assisted
EXIT	EXtrinsic Information Transfer
FPTD	Fully-Parallel Turbo Decoder
FPQTD	Fully-Parallel Quantum Turbo Decoder
GF	Galois Field
IRCC	IRregular Convolutional Code
LDPC	Low Density Parity Check
LUT	Look-Up Table
MAP	Maximum A Posteriori
ML	Maximum Likelihood
MLSE	Maximum Likelihood Sequence Estimation
PCM	Parity Check Matrix
PGZ	Peterso-Gorenstein-Zierler
QBCH	Quantum Bose-Chaudhuri-Hocquenghem
QBER	Quantum Bit Error Ratio
QCC	Quantum Convolutional Code
QECC	Quantum Error Correction Code
QIRCC	Quantum IRregular Convolutional Code
QKD	Quantum Key Distribution
QLDPC	Quantum Low Density Parity Check
QRS	Quantum Reed-Solomon
QSC	Quantum Stabilizer Code
QSDC	Quantum Secure Direct Communication
QTC	Quantum Turbo Code
QURC	Quantum Unity Rate Code
RM	Reed-Muller
RRNS	Redundant Residue Number System
RS	Reed-Solomon
RSC	Recursive Systematic Convolutional
SISO	Soft-In Soft-Out
SNR	Signal-to-Noise Ratio
SOVA	Soft-Output Viterbi Algorithm
TCM	Trellis-Coded Modulation
TTCM	Turbo Trellis Coded Modulation
URC	Unity Rate Code
VA	Viterbi Algorithm

LIST OF SYMBOLS

General Notation

- The notation $|.\rangle$ is used to indicate a quantum state. Therefore, $|\psi\rangle$ represents a qubit having the state ψ.
- The notation $|.|$ is used to indicate a magnitude operation. Therefore, $|\alpha|$ represents the magnitude of a complex number α.
- The notation $\star$ is used to indicate the symplectic product.
- The notation $\otimes$ is used to indicate the tensor product.
- The notation $\circledast$ is used to indicate the discrete convolution operation.
- The notation $\sum$ is used to indicate the sum operation.
- The notation $\langle, \rangle$ is used to represent the inner product.
- The GF(4) variables are represented with a $\hat{}$ on top, e.g. $\hat{x}$.
- The notation (n, k) is used for a classical code, while the notation $[n, k]$ is used for a quantum code.
- The superscript ^{T} is used to indicate the matrix transpose operation. Therefore, $\mathbf{x}^T$ represents the transpose of the matrix $\mathbf{x}$.

Z. Babar, P. Botsinis, D. Alanis, D. Chandra, S. X. Ng, and L. Hanzo are with the School of Electronics and Computer Science, University of Southampton, SO17 1BJ, United Kingdom. Email: {zb2g10,hvn08r,pb8g10,da4g11,dc2n14,sxn,lh}@ecs.soton.ac.uk.

The financial support of the European Research Council under the Advanced Fellow Grant, that of the Royal Society's Wolfson Research Merit Award and that of the Engineering and Physical Sciences Research Council under Grant EP/L018659/1 is gratefully acknowledged.

Special Symbols

η	Spectral efficiency.
B	Classical channel bandwidth.
c	Number of pre-share entangled qubits (ebits).
C	Classical code space.
$\mathcal{C}$	Quantum code space.
$\mathbb{C}$	Set of complex numbers.
$\mathbf{C}$	Classical channel channel.
$C_Q(.)$	Quantum channel capacity.
E	Entanglement consumption rate.
$\mathbb{F}_q$	Galois field GF(q).
$\mathbf{G}$	Generator matrix.
$\mathcal{G}_n$	n-qubit Pauli group.
g_i	ith stabilizer generator.
$\mathbf{H}$	Parity check matrix.
$\mathcal{H}$	Stabilizer group.
$H_2(.)$	Binary entropy function.
H	Hadamard gate.
$\mathbf{I}$	Pauli-$\mathbf{I}$ operator.
k	Length of information word.
n	Length of codeword.
N	Classical noise power.
p	Channel error (or flip) rate, e.g. channel depolarizing probability.
$\mathcal{P}$	Pauli error inflicted on the transmitted codeword.
R_c	Equivalent classical coding rate of a quantum code.
R_Q	Quantum coding rate.
S	Classical signal power.
Tr[.]	Trace operator.
$\mathcal{V}$	Clifford encoder.
$\mathbf{X}$	Pauli-$\mathbf{X}$ operator.
$\mathbf{Y}$	Pauli-$\mathbf{Y}$ operator.
$\mathbf{Z}$	Pauli-$\mathbf{Z}$ operator.

I. Introduction

If computers that you build are quantum,
Then spies everywhere will all want 'em.
Our codes will all fail,
And they'll read our email,
Till we get crypto that's quantum, and daunt 'em.
Jennifer and Peter Shor

In the midst of the fast technological advances seen over the last several decades, 'Quantum Technology' has emerged as a promising candidate, which has the potential of radically revolutionizing the way we compute as well as communicate. Quantum technology derives its strengths from harnessing the peculiar laws of quantum physics, namely the superposition and entanglement. The fundamental postulates of quantum physics are rather different from the widely known and well-understood laws of classical physics, as exemplified by Newton's laws and Maxwell's equations. Explicitly, a quantum bit (qubit[1]), which is the integral constituent unit of a quantum system, exists in 'superposition' of the states $|0\rangle$ and $|1\rangle$ until it is 'measured' or 'observed'. The superimposed state of a qubit is expressed as $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where $|\ \rangle$ is called the Ket or Dirac notation [1], which is used for denoting a quantum state. Furthermore, the complex coefficients α and β may take any arbitrary value as long as $|\alpha|^2 + |\beta|^2 = 1$. Upon 'measurement' or 'observation' invoked for finding out its value, the qubit $|\psi\rangle$ either collapses to the state $|0\rangle$ or to the state $|1\rangle$, which may happen with a probability of $|\alpha|^2$ and $|\beta|^2$, respectively. Hence, a qubit is basically a 2-dimensional vector, while an N-qubit composite system may be represented as a 2^N-dimensional vector, which is formulated as:

$$\alpha_0|00\ldots0\rangle + \alpha_1|00\ldots1\rangle + \cdots + \alpha_{2^N-1}|11\ldots1\rangle, \qquad (1)$$

where $\alpha_i \in \mathbb{C}$ and $\sum_{i=0}^{2^N-1} |\alpha_i|^2 = 1$. By contrast, 'entanglement', which Einstein termed as a 'spooky action at a distance' [2], is the mysterious, correlation-like property of two or more qubits, which implies that the entangled N-qubit state cannot be expressed as tensor product of the individual qubits. For example, consider a 2-qubit state $|\psi\rangle$ given by:

$$|\psi\rangle = \alpha|00\rangle + \beta|11\rangle, \qquad (2)$$

and having non-zero coefficients α and β. It is impossible to express $|\psi\rangle$ as the tensor product of constituent qubits, because we have [3]:

$$\alpha|00\rangle + \beta|11\rangle \neq (\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle), \qquad (3)$$

for any choice of α_i and β_i subject to normalization, where $\otimes$ denotes the tensor product[2]. Consequently, a strange relationship exists between the two entangled qubits, which entails that measuring one of them also reveals the value of the other, even if they are geographically separated. Explicitly, if the first qubit of Eq. (2) collapses to the state $|0\rangle$ upon measurement, which may happen with a probability $|\alpha|^2$, then the second qubit is definitely $|0\rangle$. Similarly, if the first qubit collapses to the state $|1\rangle$, which may occur with a probability $|\beta|^2$, then the second qubit is also $|1\rangle$.

The phenomenon of 'superposition' as well as 'entanglement' have no counterparts in the classical domain, but they give rise to a new range of powerful computing and secure communication paradigms. For example, quantum computing algorithms have the potential to solve problems often deemed intractable at a substantially reduced complexity, as exemplified by Shor's pioneering factorization algorithm [4] and Grover's search algorithm [5]. This astounding processing power is derived from the inherent quantum parallelism resulting from quantum-domain superposition. More specifically, in

[1] A qubit can take different forms, for example two energy levels of an atom, different alignments of a nuclear spin, two different photon polarizations, or the charge/current/energy of a Josephson junction.

[2] The right hand side of Eq. (3) can be expanded as follows:

$$\alpha|00\rangle + \beta|11\rangle \neq \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle.$$

contrast to an N-bit classical register, which can only store *one* of the 2^N possible values, an N-qubit quantum register can hold *all* the 2^N possible values (or states) concurrently, hence facilitating parallel processing, whose complexity is deemed equivalent to a single classical evaluation. This massive parallel processing potential may be beneficially exploited in large-scale communication systems' processes, for example in multi-user detection [6], [7] and in routing optimization [8], [9], as well as in diverse other applications, such as data mining [10] and Gait Recognition [11], [12], just to name a few.

It is anticipated that the enormous processing capability of quantum computing algorithms may threaten the integrity of the state-of-the-art trusted classical public key encryption, which relies on the computational complexity of the underlying mathematical functions. While classical cryptography is at risk of being deciphered due to quantum computing, quantum communications support secure data dissemination, since any 'measurement' or 'observation' by an eavesdropper perturbs the quantum superposition, hence intimating the parties concerned [3], [13]. Some of the main applications of secure quantum communications are Quantum Key Distribution (QKD) techniques [14], [15], Quantum Secure Direct Communication (QSDC) [16]–[18], and unconditional quantum location verification [19] for the future driverless 'Quantum Car' [20] and quantum geo encryption [21]. Deploying quantum communications further is also imperative for making the future 'Quantum Internet' (Qinternet) [22] a reality. Explicitly, the Qinternet is envisaged as a global network of heterogeneous quantum systems, which may be interconnected through quantum channels in pursuit of building larger quantum systems, for example ultra-powerful distributed quantum computers [23], [24], long-haul secure QKD, QKD and quantum based location verification aided secure banking transactions, as well as ultra-precise quantum clocks for global synchronization, as illustrated in Fig. 1. It is pertinent to mention here that the quantum backhaul, which is likely to be a combination of free-space wireless channels and optical fibers, is particularly suitable for the Qinternet owing to the inherent quantum parallelism [22]. More specifically, an N-qubit quantum state would require only N uses of the quantum channel for transmitting the complete state information, while 2^N channel uses would be required if classical transmission is invoked. Similarly, if k N-qubit quantum nodes are entangled, then their overall capacity will be that of a (kN)-qubit system having a 2^{kN}-dimensional state space. By contrast, if the k N-qubit nodes are classically connected, they will have an effective state space of $k2^n$. Hence, quantum connectivity guarantees an exponentially larger state space compared to classical connectivity.

Unfortunately, the quantum channels as well as the quantum systems of Fig. 1 are not perfect, which is a major impediment to the practical realization of a global Qinternet. More specifically, qubits may experience both channel-induced as well as quantum processing impairments [25]. Explicitly, the deleterious quantum channel attenuation measured in dB per km severely limits the reliable transmission rate, or equivalently the transmission range. For example, the secret key transmission rate of a QKD system decays exponentially with the distance [26]. By contrast, the quantum processing impairments are inflicted by the imperfections in the quantum hardware, such as the quantum gates.

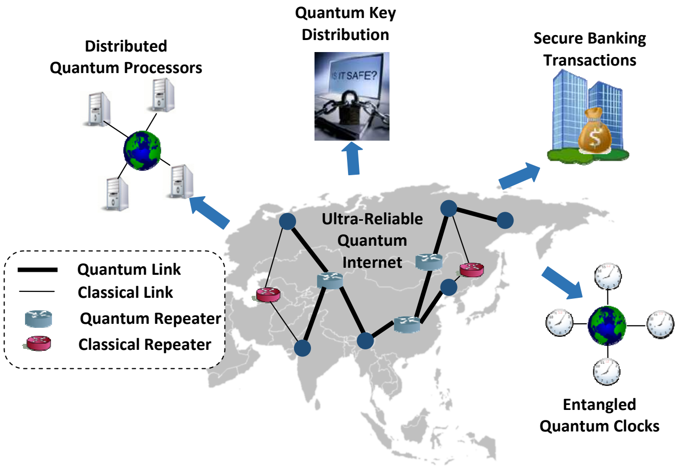


Fig. 1: Stylized illustration of the global 'Qinternet' interconnecting heterogeneous quantum processing and communication nodes over large distances, for example for distributed quantum computing, long-haul QKD, QKD and location verification aided secure banking transactions, as well as for quantum clock aided ultra-precise synchronization and navigation.

Quantum-based communication systems support the transmission of both classical as well as of quantum information. When the information to be transmitted is classical, we may invoke the family of classical error correction techniques for counteracting the impact of quantum impairments [27], [28]. More specifically, the classical information is first encoded using a classical error correction code. The encoded bits are then *mapped* onto the qubits, which are transmitted over a quantum channel. The mapping of classical bits to qubits may be carried out for example by the so-called superdense coding protocol [27], [29]. Likewise, QKD also relies on classical error correction codes [30], [31]. By contrast, for a more general communication system, which supports the transmission of both classical as well as quantum information, and for reliable quantum computation, we have to resort to Quantum Error Correction Codes (QECCs), which exploit redundancy in the quantum domain. More explicitly, similar to the classical error correction codes, QECCs redress the perturbations resulting from quantum impairments, hence enabling qubits to retain their coherent quantum states for longer durations with a high probability. This has been experimentally demonstrated in [32]–[34].

QECCs relying on the quantum-domain redundancy are indispensable for conceiving a quantum communication system supporting the transmission of quantum information and also for quantum computing. Therefore, in this paper, we survey the intricate journey from the realm of classical channel coding theory to that of the QECCs, while also providing a slow-paced tutorial on the duality of these two seemingly different coding regimes. In particular, we provide deeper insights into the subtle similarities and differences between them.

A. Outline

Fig. 2 provides overview of this paper at a glance. We commence our discourse in Section II, where we detail the various quantum channel models and highlight the duality between the widely used quantum depolarizing channel and the classical discrete quaternary channel. We then survey the rich history of classical and quantum codes in Section III. In Section IV, we detail the transition from the classical to the quantum code designs with the help of simple design examples. Specifically, we design the quantum counterpart of the simple classical rate-$1/3$ repetition code. We then generalize our discussions in Section V, where we present the quantum version of classical linear block codes by relying on the so-called stabilizer formalism, which is a theoretical framework conceived for constructing quantum codes from the existing families of classical error correction codes. Continuing further our discussions, we next detail the quantum to classical isomorphism in Section VI, which is a useful analysis technique for mapping quantum codes onto the equivalent classical codes and vice versa. The quantum-to-classical mapping allows us to use the state-of-the-art classical syndrome decoding techniques in the quantum realm, while the inverse mapping, i.e. the classical-to-quantum mapping, helps in importing arbitrary classical codes into the quantum domain. Furthermore, based on this isomorphism, we present the taxonomy of stabilizer codes in Section VII. We also detail the associated design principles with examples. In Section VIII, we delve deeper into a pair of popular code families, explicitly the Bose-Chaudhuri-Hocquenghem (BCH) codes and the convolutional codes, by providing tutorial insights into their classical as well as quantum counterparts. Finally, we conclude our discourse in Section IX.

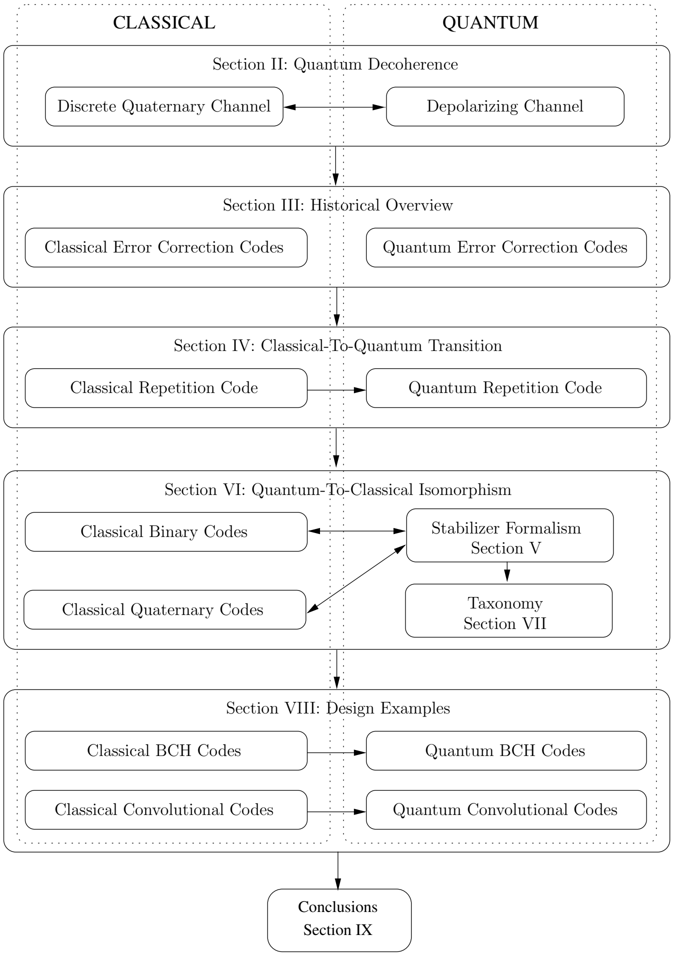

CLASSICAL
QUANTUM
Section II: Quantum Decoherence
Discrete Quaternary Channel
Depolarizing Channel
Section III: Historical Overview
Classical Error Correction Codes
Quantum Error Correction Codes
Section IV: Classical-To-Quantum Transition
Classical Repetition Code
Quantum Repetition Code
Section VI: Quantum-To-Classical Isomorphism
Classical Binary Codes
Stabilizer Formalism Section V
Classical Quaternary Codes
Taxonomy Section VII
Section VIII: Design Examples
Classical BCH Codes
Quantum BCH Codes
Classical Convolutional Codes
Quantum Convolutional Codes
Conclusions Section IX

Fig. 2: Paper Structure.

II. Quantum Decoherence

Environmental decoherence generally constitutes a major source of quantum impairments, which may occur for example during quantum transmission or quantum processing as well as in quantum memories. In this section, we review the quantum channels of Fig. 3, which are widely used for modeling environmental decoherence. Explicitly, our intention is to help the readers understand the duality between quantum and classical channels.

A. Amplitude Damping Channel

In the simple terms, environmental decoherence may be described as the undesired interaction, or more specifically entanglement, of the qubit with the environment, which perturbs its coherent superposition of basis states. In one such instance, the qubit (or quantum system) loses energy due to its interaction with the environment, for example the excited state of the qubit decays due to the spontaneous emission of a photon or the photon is lost (or absorbed) during its transmission through optical fibers [35], [36]. This decoherence process can be conveniently modeled using an amplitude damping channel. Let us consider a qubit realized using a two-level atom having the ground state $|0\rangle$ and the excited state $|1\rangle$. Furthermore, let $|0\rangle_E$ and $|1\rangle_E$ be the basis states of the environment initialized to the vacuum state $|0\rangle_E$. Then, the amplitude damping channel characterizes the evolution of the resultant system as follows [36]:

$$\begin{aligned} &|0\rangle|0\rangle_E \rightarrow |0\rangle|0\rangle_E, \\ &|1\rangle|0\rangle_E \rightarrow \sqrt{1-\gamma}|1\rangle|0\rangle_E + \sqrt{\gamma}|0\rangle|1\rangle_E, \end{aligned} \tag{4}$$

where γ is the damping probability, or more specifically the probability of losing a photon. In physically tangible terms, Eq. (4) implies that the state of the qubit remains the same if it is in the ground state $|0\rangle$, while it looses a photon with a probability of γ, when in the excited state $|1\rangle$. Explicitly, in the event of a photon loss, the state of the qubit changes from $|1\rangle$ to $|0\rangle$, while that of the environment changes from $|0\rangle_E$ to $|1\rangle_E$; hence resulting in the state $|0\rangle|1\rangle_E$ of Eq. (4), which

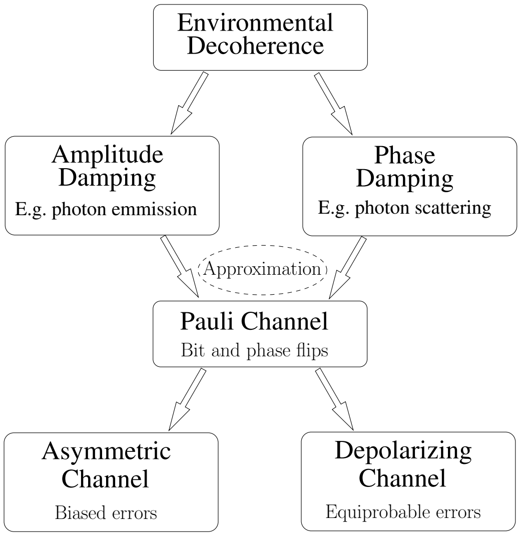


Fig. 3: Quantum channel models.

may occur with a probability of γ. Based on Eq. (4), a qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, which is in coherent superposition of the basis states, entangles with the environment as:

$$|\psi\rangle|0\rangle_E \rightarrow \Big(\alpha|0\rangle + \beta\sqrt{1-\gamma}|1\rangle\Big)\,|0\rangle_E + \sqrt{\gamma}\beta|0\rangle|1\rangle_E. \quad (5)$$

It is pertinent to mention here that $|\psi\rangle$ is generally not an isolated qubit. It may be entangled with other qubits as part of an N-qubit composite quantum system. Hence, slightly 'abusing' the usual notation, the coefficient α and β represent the $(N-1)$-qubit states orthogonal to the states $|0\rangle$ and $|1\rangle$, respectively, of the qubit undergoing decoherence. We furthermore assume that each qubit interacts independently with the environment, hence the associated decoherence process is temporally and spatially uncorrelated. We can readily infer from Eq. (5) that if the environment is found to be in state $|0\rangle_E$, then $|\psi\rangle$ decoheres to $(\alpha|0\rangle + \beta\sqrt{1-\gamma}|1\rangle)$, which reduces to $\left(\frac{\alpha}{\sqrt{1-\gamma\beta^2}}|0\rangle + \frac{\beta\sqrt{1-\gamma}}{\sqrt{1-\gamma\beta^2}}|1\rangle\right)$ upon normalization, otherwise $|\psi\rangle$ collapses to $|0\rangle$. Hence, the loss of energy may be modeled using an amplitude damping channel $\mathcal{N}_{\text{AD}}$, which maps an input state, having the density operator[3] ρ, as follows:

$$\mathcal{N}_{\text{AD}}(\rho) = \mathbf{E}_0\rho\mathbf{E}_0^\dagger + \mathbf{E}_1\rho\mathbf{E}_1^\dagger, \quad (6)$$

where the error operators (also called Kraus operators[4]) $\mathbf{E}_0$ and $\mathbf{E}_1$ are given by [3]:

$$\mathbf{E}_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{pmatrix}, \quad \mathbf{E}_1 = \begin{pmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{pmatrix}. \quad (7)$$

The decohered state of a qubit may be readily described by using the error operators of Eq. (7). Resuming our previous example of $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, the error operator $\mathbf{E}_0$ corrupts $|\psi\rangle$ as follows:

$$\begin{aligned} \mathbf{E}_0|\psi\rangle &= \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \\ &= \begin{pmatrix} \alpha \\ \sqrt{1-\gamma}\beta \end{pmatrix} \\ &\equiv \alpha|0\rangle + \sqrt{1-\gamma}\beta|1\rangle, \end{aligned} \quad (8)$$

which occurs with a probability of $|\mathbf{E}_0|\psi\rangle|^2 = (1-\gamma\beta^2)$. Upon normalization, the corrupted state of Eq. (8) is reduced to:

$$\mathbf{E}_0|\psi\rangle = \frac{\alpha}{\sqrt{1-\gamma\beta^2}}|0\rangle + \frac{\beta\sqrt{1-\gamma}}{\sqrt{1-\gamma\beta^2}}|1\rangle. \quad (9)$$

Similarly, the error operator $\mathbf{E}_1$ acts on $|\psi\rangle$ as follows:

$$\begin{aligned} \mathbf{E}_1|\psi\rangle &= \begin{pmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \\ &= \begin{pmatrix} \sqrt{\gamma}\beta \\ 0 \end{pmatrix} \\ &\equiv \sqrt{\gamma}\beta|0\rangle, \end{aligned} \quad (10)$$

which happens with a probability of $|\mathbf{E}_1|\psi\rangle|^2 = \gamma\beta^2$ and is equivalent to the classical bit $|0\rangle$. In realistic systems, γ at time instant t is characterized by the qubit relaxation time T_1 as follows [37]:

$$\gamma = 1 - e^{-t/T_1}. \quad (11)$$

B. Phase Damping Channel

Another instantiation of environmental decoherence, known as dephasing or phase damping, characterizes the loss of quantum information without the loss of energy, which may occur for example due to the scattering of photons, or the perturbation of electronic states caused by stray electrical charges. The error operators of the resultant phase damping channel $\mathcal{N}_{\text{PD}}$ are defined as follows [3]:

$$\mathbf{E}_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\lambda} \end{pmatrix}, \quad \mathbf{E}_1 = \begin{pmatrix} 0 & 0 \\ 0 & \sqrt{\lambda} \end{pmatrix}, \quad (12)$$

where λ is the scattering probability of a photon (without loss of energy). We may observe that $\mathbf{E}_0$ of Eq. (12) is similar

[3] If a quantum system is an ensemble of pure states $|\psi_i\rangle$, then it may be represented by the density operator (also called density matrix) ρ, which is defined as:

$$\rho \equiv \sum_i p_i|\psi_i\rangle\langle\psi_i|,$$

where p_i denotes the probability of occurrence of the ith state $|\psi_i\rangle$.

[4] A quantum channel $\mathcal{N}$ is a completely positive, trace-preserving linear mapping, which maps an input state having the density ρ as [3]:

$$\mathcal{N}(\rho) = \sum_k \mathbf{E}_k\rho\mathbf{E}_k^\dagger,$$

where the matrices $\mathbf{E}_k$ are known as the Kraus operators or error operators of the channel. Furthermore, we have $\sum_k \mathbf{E}_k^\dagger\mathbf{E}_k = \mathbf{I}$, where $\mathbf{I}$ is an identity matrix.

to the $\mathbf{E}_0$ of the amplitude damping channel, while the error operator $\mathbf{E}_1$ acts on $|\psi\rangle$ as follows:

$$\begin{aligned}\mathbf{E}_1|\psi\rangle &= \begin{pmatrix}0 & 0\\ 0 & \sqrt{\lambda}\end{pmatrix}\begin{pmatrix}\alpha\\ \beta\end{pmatrix}\\ &= \begin{pmatrix}0\\ \sqrt{\lambda}\beta\end{pmatrix}\\ &\equiv \sqrt{\lambda}\beta|1\rangle,\end{aligned} \tag{13}$$

which occurs with a probability of $|\mathbf{E}_1|\psi\rangle|^2 = \lambda\beta^2$ and it is equivalent to the classical state $|1\rangle$. The probability λ relies on the relaxation time T_1 as well as on the dephasing time T_2, i.e. we have [37]:

$$\lambda = 1 - e^{\frac{t}{T_1} - \frac{2t}{T_2}}. \tag{14}$$

Intuitively, Eq. (11) and Eq. (14) imply that the qubit is likely to decohere if the operation time (transmission or processing or storage) t is comparable to the relaxation time T_1 and the dephasing time T_2. Equivalently, T_1 and T_2 characterize the life-time of a reliable qubit.

C. Pauli Channel

The environmental decoherence can be completely modeled using a combined amplitude and phase damping channel. However, it is not feasible to classically simulate such channels for an N-qubit composite system, since the resultant system has a 2^N-dimensional Hilbert space. For the sake of facilitating efficient classical simulations, the combined amplitude and phase damping channel can be approximated using a so-called Pauli channel $\mathcal{N}_\text{P}$, which maps an input state, having the density operator ρ, as follows [38]:

$$\mathcal{N}_\text{P}(\rho) = (1 - p_z - p_x - p_y)\rho + p_z\mathbf{Z}\rho\mathbf{Z} + p_x\mathbf{X}\rho\mathbf{X} + p_y\mathbf{Y}\rho\mathbf{Y}, \tag{15}$$

where $\mathbf{I}$, $\mathbf{X}$, $\mathbf{Y}$ and $\mathbf{Z}$ are single-qubit Pauli operators (or gates) of Fig. 4 defined as:

$$\begin{aligned}\mathbf{I} &= \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \ \mathbf{X} = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix},\\ \mathbf{Z} &= \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}, \ \mathbf{Y} = \begin{pmatrix}0 & -i\\ i & 0\end{pmatrix},\end{aligned} \tag{16}$$

while p_z, p_x and p_y are the probabilities of encountering $\mathbf{Z}$, $\mathbf{X}$ and $\mathbf{Y}$ Pauli errors, respectively, which rely on the qubit relaxation and dephasing time as given below:

$$\begin{aligned}p_x = p_y &= \frac{1}{4}\left(1 - e^{-t/T_1}\right)\\ p_z &= \frac{1}{4}\left(1 + e^{-t/T_1} - 2e^{-t/T_2}\right).\end{aligned} \tag{17}$$

Explicitly, $\mathbf{I}$ is an identity operator, or merely a repeat gate, which leaves the state $|\psi\rangle$ intact, as shown below:

$$\begin{aligned}\mathbf{I}|\psi\rangle &= \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}\alpha\\ \beta\end{pmatrix}\\ &= \begin{pmatrix}\alpha\\ \beta\end{pmatrix} \equiv \alpha|0\rangle + \beta|1\rangle.\end{aligned} \tag{18}$$

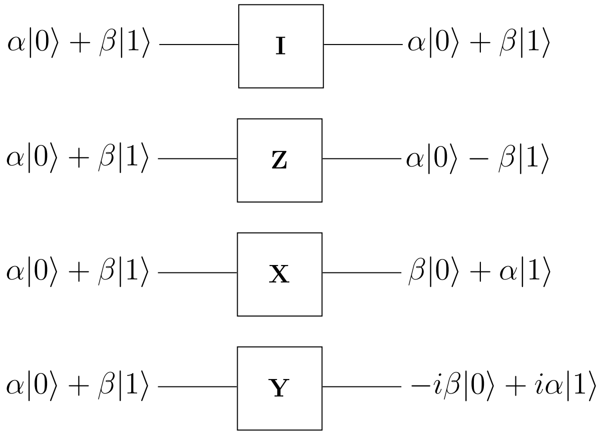


Fig. 4: Schematic of Pauli-$\mathbf{I}$, Pauli-$\mathbf{Z}$, Pauli-$\mathbf{X}$ and Pauli-$\mathbf{Y}$ gates.

The operator $\mathbf{Z}$ is a phase-flip operator, which acts as:

$$\begin{aligned}\mathbf{Z}|\psi\rangle &= \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix}\alpha\\ \beta\end{pmatrix}\\ &= \begin{pmatrix}\alpha\\ -\beta\end{pmatrix} \equiv \alpha|0\rangle - \beta|1\rangle,\end{aligned} \tag{19}$$

while $\mathbf{X}$ is a bit-flip operator analogous to the classical NOT gate, which yields:

$$\begin{aligned}\mathbf{X}|\psi\rangle &= \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}\alpha\\ \beta\end{pmatrix}\\ &= \begin{pmatrix}\beta\\ \alpha\end{pmatrix} \equiv \beta|0\rangle + \alpha|1\rangle.\end{aligned} \tag{20}$$

By contrast, $\mathbf{Y}$ is a combined bit-and-phase-flip operator ($\mathbf{Y} = i\mathbf{XZ}$), which acts on $|\psi\rangle$ as:

$$\begin{aligned}\mathbf{Y}|\psi\rangle &= \begin{pmatrix}0 & -i\\ i & 0\end{pmatrix}\begin{pmatrix}\alpha\\ \beta\end{pmatrix}\\ &= \begin{pmatrix}-i\beta\\ i\alpha\end{pmatrix} \equiv -i(\beta|0\rangle - \alpha|1\rangle).\end{aligned} \tag{21}$$

Hence, the Pauli channel of Eq. (15) maps the input state $|\psi\rangle$ onto a linear combination of the original state (Pauli-$\mathbf{I}$ operation), phase-flipped state (Pauli-$\mathbf{Z}$ operation), bit-flipped state (Pauli-$\mathbf{X}$ operation), as well as bit-and-phase-flipped state (Pauli-$\mathbf{Y}$ operation) during the process of decoherence. In essence, the resultant quantum error is continuous in nature. We may observe in Eq. (17) furthermore that the time T_1 affects bit-flips, phase-flips as well as bit-and-phase-flips. By contrast, the time T_2 is only related to the phase-flip errors. This is because the bit-flip as well as bit-and-phase-flip errors are associated with amplitude damping, while the phase-flip errors result from phase damping. In most practical systems, the value of T_1 is several orders of magnitude higher than that of T_2 [39], [40]. Consequently, most practical quantum systems behave as so-called asymmetric channels and they

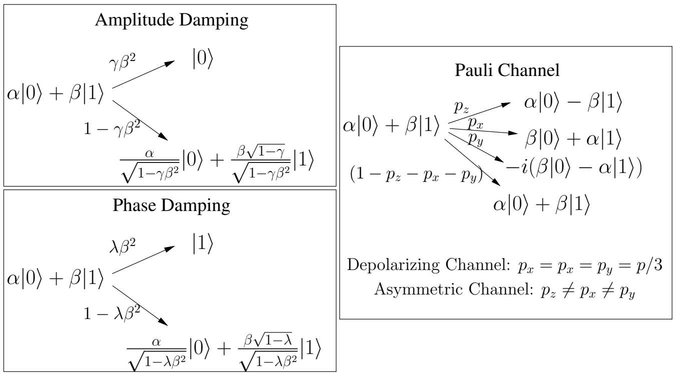

Amplitude Damping
$\alpha|0\rangle + \beta|1\rangle$
$\gamma\beta^2$
$|0\rangle$
$1-\gamma\beta^2$
$\frac{\alpha}{\sqrt{1-\gamma\beta^2}}|0\rangle + \frac{\beta\sqrt{1-\gamma}}{\sqrt{1-\gamma\beta^2}}|1\rangle$
Phase Damping
$\alpha|0\rangle + \beta|1\rangle$
$\lambda\beta^2$
$|1\rangle$
$1-\lambda\beta^2$
$\frac{\alpha}{\sqrt{1-\lambda\beta^2}}|0\rangle + \frac{\beta\sqrt{1-\lambda}}{\sqrt{1-\lambda\beta^2}}|1\rangle$
Pauli Channel
$\alpha|0\rangle + \beta|1\rangle$
p_z
p_x
p_y
$(1-p_z-p_x-p_y)$
$\alpha|0\rangle - \beta|1\rangle$
$\beta|0\rangle + \alpha|1\rangle$
$-i(\beta|0\rangle - \alpha|1\rangle)$
$\alpha|0\rangle + \beta|1\rangle$
Depolarizing Channel: $p_z = p_x = p_y = p/3$
Asymmetric Channel: $p_z \neq p_x \neq p_y$

Fig. 5: Mathematical interpretation of quantum channel models.

experience more phase-flips than bit-flips as well as bit-and-phase-flips. Furthermore, a special class of Pauli channels, known as the 'depolarizing channel', models the worst-case scenario by assuming that all three errors are equally likely, i.e. $(p_z = p_x = p_y)$. Explicitly, a depolarizing channel having the probability p inflicts a phase-flip (Pauli-$\mathbf{Z}$) or a bit-flip (Pauli-$\mathbf{X}$) or bit-and-phase-flip (Pauli-$\mathbf{Y}$) error with a probability of $p/3$ each, which may be mathematically encapsulated as:

$$\mathcal{N}_{\text{DP}}(\rho) = (1-p)\rho + \frac{p}{3}\left(\mathbf{Z}\rho\mathbf{Z} + \mathbf{X}\rho\mathbf{X} + \mathbf{Y}\rho\mathbf{Y}\right). \qquad (22)$$

In this treatise, we will only consider the widely used depolarizing channel model.

The aforementioned quantum channel models are summarized in Fig. 5. We may observe in Fig. 5 that the Pauli channel may be deemed to be the quantum analogue of the classical discrete quaternary channel. However, while the classical quaternary channel may inflict only one of the four possible errors, the error inflicted by the Pauli channel may be in superposition of the four possible errors, i.e. $\mathbf{I}$, $\mathbf{Z}$, $\mathbf{X}$ and $\mathbf{Y}$. The Pauli channel may further be simplified by using two independent bit-flip and phase-flip channels, which are analogous to classical binary symmetric channels having cross-over probabilities of $(p_x + p_y)$ and $(p_z + p_y)$, respectively.

III. Historical Overview of Classical & Quantum Error Correction Codes

In this section, we survey the major milestones both in the realm of classical as well as in quantum coding theory, which are chronologically arranged in Table .

A. *Classical Coding Theory*

1) Design Objectives: Shannon's pioneering work [41] on classical channel capacity marks the beginning of classical coding theory. Explicitly, Shannon predicted that sophisticated channel coding techniques, having coding rate R lower than the Shannon limit (or channel capacity) C, may be invoked for the sake of achieving reliable transmission over a noisy

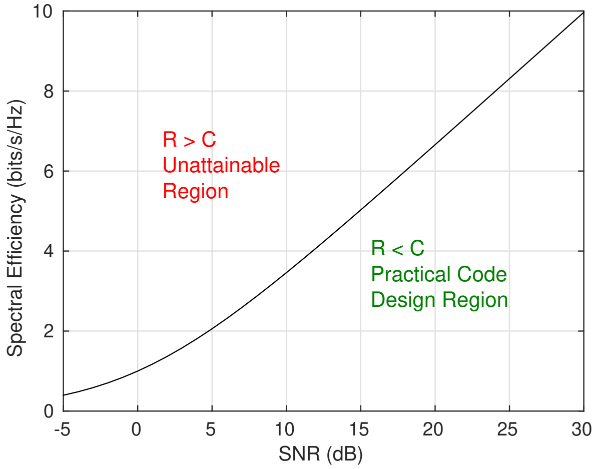


Fig. 6: Shannon capacity limit for AWGN channel characterized by Eq. (24).

bandwidth-limited channel. Intuitively, this implies that it is possible to transmit information virtually free from errors, as long as the coding rate does not exceed the Shannon limit,which is characterized by the channel bandwidth B (Hz), the signal power S (Watts) and the uncorrelated Additive White Gaussian Noise (AWGN) power N (Watts) as follows:

$$\text{C} = B\log_2\left(1 + \frac{S}{N}\right), \qquad (23)$$

or equivalently in terms of the spectral efficiency (bits/s/Hz) as:

$$\eta = \frac{\text{C}}{B} = \log_2\left(1 + \frac{S}{N}\right). \qquad (24)$$

Hence, the Shannon limit of Eq. (23) (and equivalently Eq. (24)) quantifies the highest possible coding rates still capable of ensuring error-free transmission, as illustrated in Fig. 6. Furthermore, we may infer from Eq. (23) that the resultant information transfer rate of a system is limited by the channel bandwidth B as well as the system's Signal-to-Noise Ratio (SNR) S/N. As demonstrated in Fig. 6, the capacity limit increases upon increasing the SNR. Ultimately, when the SNR approaches infinity in the noiseless scenario, it is possible to achieve an infinite transmission rate even for a very low bandwidth. Similarly, the capacity limit also increases upon increasing the bandwidth. Hence, we may strike a trade off between the bandwidth and the SNR, as detailed and exemplified in Section 2.13.1 of [133]. However, an infinite bandwidth does not guarantee an infinite transmission rate, because the noise power also increases upon increasing bandwidth, as shown mathematically in [133].

Shannon did not provide any explicit code constructions in his seminal work [41]. However, his work inspired the research community to design practical codes in line with the achievable code design region of Fig. 6. This in turn

Classical		Quantum
Shannon Limit [41]		
Hamming Codes [42]	1950	
Reed-Muller (RM) Codes [43], [44], Wagner decoding [45]		
Convolutional Codes [46]		
Cyclic codes [47]		
Bose-Chaudhuri-Hocquenghem (BCH) Codes [48], [49]		
Reed-Solomon (RS) codes [50]	1960	
Peterson-Gorenstein-Zierler (PGZ) decoding algorithm [51]		
Low Density Parity Check (LDPC) codes [52]		
Berlekamp-Massey algorithm [53]–[56]		
Redundant Residue Number System (RRNS) codes [57], [58]		
Viterbi algorithm [59]		
	1970	
Chase algorithm [60]		
Maximum A Posteriori (MAP) algorithm [61]		
Trellis decoding of block codes [62]		
	1980	
Trellis Coded Modulation (TCM) [63]–[65]		
Soft-Output Viterbi Algorithm (SOVA) [66]		
Max-Log-MAP algorithm [67]	1990	
Bit-Interleaved Coded Modulation (BICM) [68], [69]		
Turbo Codes [70], [71]		
Soft-In Soft-Out (SISO) Chase algorithm [72], [73]		
Log-MAP algorithm [74], Rediscovery of LDPC codes [75], [76]		Shor's code [77]
Turbo BCH code [78]		Calderbank-Shor-Steane (CSS) codes [79]–[81], 5-qubit code [82], [83], Quantum Stabilizer codes (QSC) [84], [85]
Turbo Hamming code [86], BICM with Iterative Decoding (BICM)-ID [87]		Hashing bound [88], Quantum BCH (QBCH) codes [89]–[94], Toric codes [95], [96]
Turbo Trellis Coded Modulation (TTCM) [97]		
Punctured turbo codes [98]		Quantum Reed-Muller codes [99], Quantum Reed-Solomon codes [100]
Unity Rate Code (URC) [101]	2000	
EXtrinsic Information Transfer (EXIT) chart [102]		Quantum LDPC (QLDPC) codes [103]
IRregular Convolutional Codes (IRCC) [104]		Entanglement-Assisted Quantum Error Correction Codes (EA-QECC) [105]
		Quantum Convolutional Codes (QCC) [106]
Reduced-complexity non-binary EXIT chart [107]		Entanglement-Assisted QSC (EA-QSC) [108]–[110]
Near-capacity TTCM [111]		Quantum Turbo Codes (QTC) [112], [113], Improved QLDPC decoder [114]–[116]
Polar codes [117], Near-capacity BICM-ID [118]		Entanglement-Assisted QLDPC (EA-QLDPC) codes [119]
	2010	Entanglement-Assisted QCC (EA-QCC) [120]
		Entanglement-Assisted QTC (EA-QTC) [121], [122]
		Entanglement-assisted polar codes [123]–[125]
		Degenerate Viterbi decoding [126], Near-capacity codes for entanglement-assisted classical communication [27]
		EXIT chart [127]
Fully-Parallel Turbo Decoder (FPTD) [128]		Quantum IRCC (QIRCC) [129], Unassisted qauntum polar codes [130]
		Quantum URC (QURC) [131], Fully-Parallel Quantum Turbo Decoder (FPQTD) [132]

TABLE : Major achievements in the classical and quantum coding paradigms.

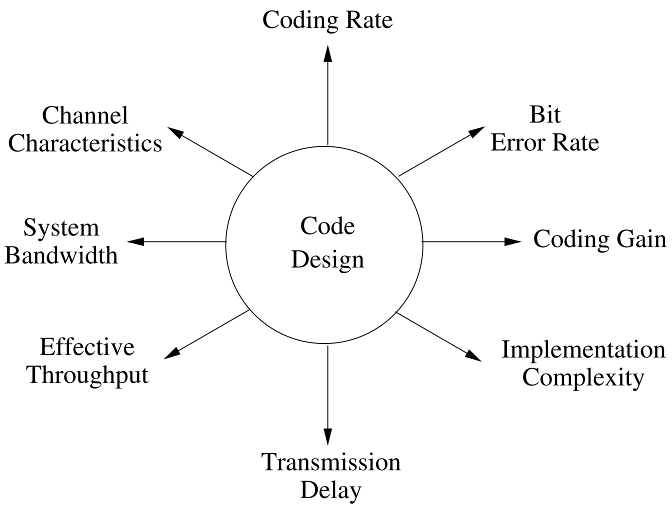


Fig. 7: Stylized representation of conflicting design parameters affecting the design of classical codes.

highlighted various other conflicting design trade-offs, which are captured in Fig. 7. For example, given particular channel conditions, a code may be optimized to achieve a lower Bit Error Ratio (BER) or a higher coding gain[5]. However, this typically imposes an increased decoding complexity and transmission delay, or reduced effective throughput, as detailed in [133], [134].

2) Error Correction Codes: In 1950, Hamming conceived the first practical family of classical error correction codes [42]. More specifically, Hamming proposed an infinite family of binary linear block codes capable of encoding $k = (2^r - 1 - r)$ information bits into $n = (2^r - 1)$ coded bits for $r \geq 2$. The resultant codewords had a minimum Hamming distance of $d_{\text{min}} = 3$, hence correcting $t = (d_{\text{min}} - 1)/2 = 1$ errors. The Hamming codes may be classified as being 'perfect' codes, since the associated coding rate $R = k/n = 1 - r/(2^r - 1)$ is the maximum coding rate achievable for $d_{\text{min}} = 3$ and for a block length of $n = (2^r - 1)$. Following these developments, in 1954, Reed [43] and Muller [44] independently conceived a class of multiple error correcting block codes, known as Reed-Muller (RM) codes. Reed also introduced a simple majority-logic based hard-decision decoder for RM codes in [43]. The same year, a soft-decision based decoding algorithm, known as Wagner decoding [45], was developed for a special class of RM codes.

The afore-mentioned linear block codes primarily relied on maximizing the minimum distance for a given pair of (n, k) codewords encoding k bits into n, or equivalently maximizing the coding rate given the d_{min} and n. The resultant families of Hamming and RM codes only support a limited range of code parameters given by (n, k, d_{min}). For the sake of designing more codes capable of approaching the Shannon limit for a wider range of code parameters at an affordable implementation complexity, Elias discovered convolutional codes in 1955 [46], which marks the commencement of the so-called probabilistic coding era. Convolutional codes are capable of supporting encoding and decoding procedures operating in a sliding window, hence resulting in lower latencies than the above block codes. In this spirit, Viterbi invented a *Maximum Likelihood Sequence Estimation* (MLSE) (or equivalently minimum Euclidean distance) algorithm for convolutional codes [59]. Explicitly, the Viterbi Algorithm (VA) aim for finding the most likely error sequence at an affordable decoding complexity. Although the VA is an MLSE algorithm, the resultant BER of the system is close to the minimum possible BER, but the latter was only achievable by a complex Maximum Likelihood (ML) decoder, which evaluates all valid coded sequences. To circumvent the high complexity of the latter ML decoder, Bahl *et al.* proposed the minimum BER decoding algorithm in 1974 [61], which was named the Maximum A Posteriori (MAP) algorithm. It is also known as BCJR after its inventors Bahl, Cocke, Jelinek and Raviv.

Pursuing further the realm of block codes, Prange investigated cyclic codes in 1957 [47]. Since the cyclic shift of codewords of cyclic codes are also legitimate codewords, the associated encoding and decoding procedures can be efficiently implemented using shift registers. Inspired by these developments, Hocquenghem [48] as well as Bose and Chaudhuri [49], [135] independently discovered the family of Bose-Chaudhuri-Hocquenghem (BCH) codes in 1959 and 1960, respectively. Specifically, BCH codes constitute the family of multiple-error correcting cyclic block codes, which encode $k \geq (n - rt)$ information bits into $n = (2^r - 1)$ coded bits, so that the resultant codewords exhibit the maximum possible minimum Hamming distance. In 1960, Reed and Solomon conceived a non-binary version of BCH codes referred to as Reed-Solomon (RS) codes [50], while the following year Gorenstein and Zierler developed the Peterson-Gorenstein-Zierler (PGZ) decoding scheme for non-binary RS/BCH codes. Later, Berlekamp and Massey developed the Berlekamp-Massey decoding algorithm for cyclic RS/BCH codes in [53]–[56], while a soft-decision aided Chase decoder was proposed in [60]. Both these decoding algorithms are widely adopted for decoding BCH as well as RS codes. Unfortunately BCH codes did not find much practical applications, except as Cyclic Redundancy Check (CRC) codes in Automatic-Repeat-reQuest (ARQ) systems. By contrast, RS codes have found several practical applications owing to their inherent capability of correcting both random as well as burst of errors. Explicitly, RS codes are widely employed in magnetic tape and disk storage, which are susceptible to burst errors. Furthermore, they are also used as outer codes in concatenated coding schemes, which have been integrated in various standardized systems, such as the deep-space coding standard [136]. Another major milestone in algebraic coding was achieved with the development of non-binary Redundant Residue Number System (RRNS) codes [57], [58], which are are also maximum minimum-distance codes and hence exhibit similar distance properties to RS codes.

By 1980, error correction codes were successfully deployed

[5] Coding gain quantifies the reduction in bit-energy achieved at a certain BER, when error correction is invoked.

in various deep-space, satellite and mobile communications systems in conjunction with modulation schemes. However, the error correction and modulation modules were treated independently and the redundancy of the codes extended the bandwidth requirement, when the signal constellation size was fixed. For the sake of circumventing this disadvantage of coding, Ungerboeck invented a bandwidth-efficient trellis-based joint coding and modulation scheme called Trellis-Coded Modulation (TCM) [63]–[65]. Explicitly, TCM is a joint channel coding and modulation scheme, which absorbs the redundant coding bits by expanding the constellation size to accommodate more bits/symbols and hence maintains a fixed bandwidth. TCM provides attractive performance gains over convolutional codes, while incurring a similar decoding complexity. In 1992, another coded modulation scheme termed as Bit-Interleaved Coded Modulation (BICM) [68], [69] was conceived for transmission over fading channels, which invoked bit-based interleavers in conjunction with Gray-coded bit-to-symbol mapping. More specifically, parallel bit interleavers are used at the output of a convolutional code in this joint coding and modulation scheme for the sake of increasing the resultant diversity gain by exploiting the fading of the bits in a multi-bit symbol; hence enhancing the system's performance over fading channels. However, BICM does not outperform TCM over AWGN channels, since it exhibits a reduced minimum Euclidean distance.

Despite being into the fifth decade of coding theory, the notion of operating near the Shannon limit was far from realization until Berrou *et al.* conceived turbo codes in 1993 [70], [71]. More specifically, turbo code rely on a parallel concatenation of Recursive Systematic Convolutional (RSC) codes with an interleaver between them. At the decoder, soft iterative decoding is invoked, which relies on the Soft-In Soft-Out (SISO) MAP algorithm of [61]. It is pertinent to mention here that the MAP algorithm only slightly outperforms the VA in terms of the achievable BER for non-iteratively decoded convolutional codes, while imposing a substantially higher complexity. Consequently, MAP decoding was rarely used for decoding convolutional codes, until turbo codes were invented. But given that turbo decoders require bit-by-bit soft-metrics, they required complex MAP decoding. Fortubately, the complexity of turbo decoders may be reduced by invoking less complex SISO decoders, for example the Soft-Output Viterbi Algorithm (SOVA) [66], the Max-Log-MAP algorithm [67] and the Log-MAP algorithm [74].

Berrou's turbo revolution triggered intensive research efforts directed towards designing iterative 'turbo-like' codes. In particular, it led to the renaissance of Low Density Parity Check (LDPC) codes in 1995 [75], [76]. LDPC codes were proposed by Gallager as early as 1962 [52]. However, the associated complexity was deemed enormous in that era. Consequently, LDPC codes were abandoned for decades to come. However, the invention of turbo codes revived the research interest in LDPC codes. Turbo revolution also led to other iterative coding schemes, which include for example Turbo BCH codes [78], Turbo Hamming codes [86], BICM with Iterative Decoding (BICM)-ID [87], Turbo Trellis Coded Modulation (TTCM) [97], punctured turbo codes [98] and Unity Rate Code (URC) assisted concatenated coding schemes [101]. The invention of EXtrinsic Information Transfer (EXIT) charts [102], [107] by Ten Brink in 2001 marks another important milestone in the realm of the afore-mentioned concatenated schemes relying on iterative decoding. More specifically, EXIT charts constitute a semi-analytical tool, which aids the design of near-capacity iterative schemes [134], [137]. Quantitatively, the resultant systems may operate within 1 dB of the Shannon limit, see for example the IRregular Convolutional Code (IRCC) assisted concatenated schemes of [104], the TTCM of [111] and the BICM-ID of [118].

With the help of intensive research efforts, turbo coding was successfully commercialized within just a few years and was incorporated into various standardized systems, such as mobile communication systems and video broadcast systems [134]. In particular, turbo coding was incorporated in the 3G UMTS [138] and 4G LTE [139] mobile standards. However, the high latency associated with turbo codes is anticipated to be a major impediment in next-generation systems supporting 'tactile services'. Consequently, a Fully-Parallel Turbo Decoder (FPTD) was recently conceived by Maunder in [128], which significantly reduces the associated latency; hence making turbo codes a promising candidate for next-generation systems. Over the years, the LDPC coding scheme has proved to be a fierce competitor of turbo codes, which has also been adopted by various standards, for example WiMax, IEEE 802.11n, IEEE 802.3an, and DVB-S2.

Arikan's polar code [117] conceived in 2009 sparked another wave of excitement within the coding community, since it is the first class of channel codes, which provably achieves the capacity of symmetric memoryless channels, while imposing only a modest encoding and decoding complexity. Polar codes invoke a short and simple kernel code, so that the physical channels are polarized into virtual channels, which are either perfectly noiseless or completely random, provided that the block length is sufficiently long. At practical block lengths, the channels are polarized into a set of high-reliability and low-reliability virtual channels. Finally, the information bits are sent across the high-reliability channels, while dummy bits, called 'frozen bits', are transmitted via the low-reliability channels. If the block lengths are sufficiently long, then the fraction of high reliability virtual channels is equivalent to the achievable channel capacity. At the receiver, the polar decoder invokes a low-complexity successive cancellation decoding algorithm, which processes the received bits serially. Despite having a low encoding and decoding complexity, Polar codes, relying on cyclic redundancy check-aided successive cancellation list decoding, are capable of outperforming the standardized LTE turbo and WiMax LDPC codes at moderate block lengths, as demonstrated in [140]. Furthermore, the coding rate of polar codes can be varied almost continuously by changing the number of frozen bits, hence making them ideal for rate-compatible scenarios. However, a major limitation of polar codes is the high latency associated with the polar decoder, since it sequentially processes the received information. Nonetheless, polar codes have already found their way into the

5G system for enhanced mobile broadband communications, where polar codes and LDPC codes have been chosen for the control and data channels, respectively.

B. Quantum Coding Theory

1) Design Objectives: With around seven decades of rich history, classical coding theory is already quite mature. By contrast, quantum coding theory is still in its infancy, since the implementation of quantum technology has not been commercialized. Researchers have been actively working on discovering the quantum versions of the existing classical codes. In duality to the classical coding theory, QECCs are designed to achieve the quantum channel capacity [88], [141], [142], or more precisely the hashing bound. Explicitly, the hashing bound is only a lower bound, because the actual capacity of a quantum channel may be higher due to the 'degenerate' nature of quantum codes [143], [144]. To elaborate further, the notion of degeneracy implies that different error patterns may yield the same corrupted quantum state. For instance, let us consider the state $|\psi\rangle = |00\rangle + |11\rangle$, which may experience the channel-induced error $\mathbf{IZ}$ or $\mathbf{ZI}$. We may observe that both these error patterns result in the same channel output, i.e. $(|00\rangle - |11\rangle)$. Consequently, the error patterns $\mathbf{IZ}$ and $\mathbf{ZI}$ are classified as degenerate errors, as further discussed in Section V. Similarly, the error pattern $\mathbf{ZZ}$ leaves the state $|\psi\rangle$ intact analogous to the error-free scenario; hence $\mathbf{ZZ}$ and $\mathbf{II}$ are also degenerate errors.

In duality to the Shannon limit of Eq. (23), the hashing bound is completely specified by the channel's depolarizing probability p as follows [82], [122]:

$$C_Q(p) = 1 - H_2(p) - p\log_2(3), \tag{25}$$

where $H_2(p)$ denotes the binary entropy function. Explicitly, a random quantum code $\mathcal{C}$ may exhibit an arbitrarily low Quantum Bit Error Ratio (QBER) at a depolarizing probability of p, if its coding rate does not exceed the hashing limit $C_Q(p)$ of Eq. (25) and the codeword has a sufficiently long length.

The Hashing bound of Eq. (25) is only valid for unassisted quantum codes. Explicitly, there exists a a family of Entanglement-Assisted (EA) quantum codes [105], [108]–[110], which does not exist in the classical domain. In contrast to the unassisted quantum codes, the EA quantum codes rely on pre-shared noiseless entangled qubits, which naturally increases the achievable capacity. Given that c entangled qubits are pre-shared with the receiver over a noiseless channel, the associated EA hashing bound is given by [122], [145]:

$$C_Q(p) = 1 - H_2(p) - p\log_2(3) + \mathrm{E}, \tag{26}$$

where E denotes the 'entanglement consumption' rate, which is equivalent to $\mathrm{E} = \frac{c}{n}$ for a code having k information qubits, n coded qubits and $0 \leq c \leq (n-k)$ pre-shared qubits. Explicitly, when $c = 0$, Eq. (26) reduces to the unassisted hashing bound of Eq. (25). By contrast, when c has the maximum value of $(n-k)$, we get the maximally-entangled quantum codes and the associated maximally-entangled hashing bound is [122], [145]:

$$C_Q(p) = 1 - \frac{H_2(p) - p\log_2(3)}{2}. \tag{27}$$

Hence, as shown in Fig. 8, an EA quantum code can operate anywhere in the hashing region, which is bounded by Eq. (25) and Eq. (27). Furthermore, in duality to Fig. 7, the parameters involved in the design of QECCs are illustrated in Fig. 9.

2) Error Correction Codes: The rate-1/3 repetition code is the simplest single-error correcting code in the classical coding paradigm, which relies on the cloning of information

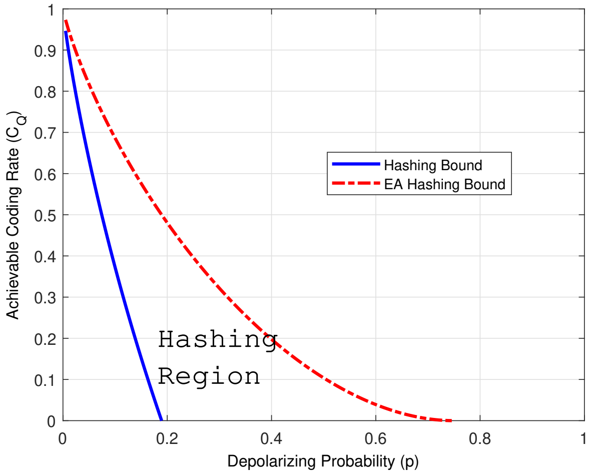


Fig. 8: Hashing bounds for the unassisted ($c = 0$) and maximally-entangled ($c = n - k$) quantum codes, characterized by Eq. (25) and Eq. (27), respectively. The enclosed region, labeled the 'hashing region', quantifies the capacity for $0 < c < (n - k)$.

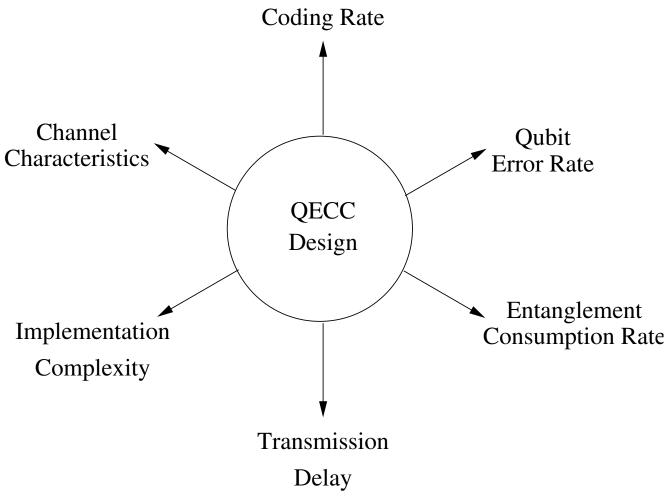


Fig. 9: Stylized representation of conflicting design parameters affecting the design of quantum codes.

bits. Unfortunately, qubits cannot be cloned owing to the existence of the no-cloning theorem. Hence, it was generally believed that QECCs are infeasible, until Shor pioneered the first quantum code in 1995 [77]. Shor's code of [77] is a rate-$1/9$ code capable of correcting a single bit-flip, phase-flip as well as bit-and-phase-flip error. Motivated by this breakthrough, Calderbank and Shor [80] as well as Steane [79], [81] independently conceived a generalized framework for constructing quantum codes from classical binary linear codes, which constitutes the popular family of Calderbank-Shor-Steane (CSS) codes. Explicitly, the CSS construction relies on a pair of classical binary linear block codes C_1 and C_2, which satisfy the criterion $C_2 \subset C_1$. Furthermore, a special class of CSS codes, called dual-containing CSS codes, was also introduced, which was derived from dual-containing binary codes. Explicitly, dual-containing CSS codes constitute a special type of CSS codes having $C_2 = C_1^{\perp}$, where $C_1^{\perp}$ is the dual code[6] of C_1. Following these principles, Steane [81] constructed a rate-$1/7$ single-error correcting code from the classical $[7, 4, 3]$ Hamming code. In the spirit of further improving the coding rate, Laflamme *et al.* [83] and Bennett *et al.* [82] independently designed the rate-$1/5$ quantum code, which is the optimal single-error correcting quantum code.

The CSS construction of [79]–[81] does not exploit the redundant qubits efficiently, since the bit-flip and the phase-flip errors are corrected independently by concatenating a pair of classical binary codes. For the sake of designing an optimal code, similar to the rate-$1/5$ code of [82], [83], it is important to jointly correct bit-flip and phase-flip errors. In pursuit of designing such optimized codes, Gottesman established the theory of Quantum Stabilizer Codes (QSCs) [84] during his Ph.D [85]. Explicitly, Gottesman presented a more general formalism, called stabilizer formalism, capable of facilitating the design of quantum codes from the classical binary and quaternary codes. As compared to the CSS codes, the stabilizer formalism imposes a more relaxed constraint, generally called the 'symplectic product' criterion, on the underlying classical codes; hence, the resultant QECCs can have either a CSS or a non-CSS (also called unrestricted) structure. In simple terms, the symplectic product criterion is the constraint imposed on the constituent classical code (or codes), which ensures that the resultant quantum code is a valid stabilizer code[7]. Furthermore, while the CSS-type codes independently correct bit-flip and phase-flip errors, the non-CSS codes jointly correct bit-flip and phase-flip errors. The advent of stabilizer formalism sparked a major revolution in the history of quantum coding, leading to the development of various code families, which includes Quantum Bose-Chaudhuri-Hocquenghem (QBCH) codes [89]–[94], toric codes [95], [96], Quantum Reed-Muller codes [99], Quantum Reed-Solomon codes (QRS) [100], Quantum Low Density Parity Check (QLDPC) codes [103], [146]–[148], Quantum Convolutional Codes (QCC) [106], [149]–[151], Quantum Turbo Codes (QTC) [112], [113], Quantum IRregular Convolutional Codes (QIRCC) [129] as well Quantum Unity Rate Codes (QURC) [131].

The Quantum research fraternity has invested the last three decades in designing the quantum counterparts of the existing families of classical codes. Except for the parallel concatenated codes as well as for the joint coding and modulation schemes of the classical regime, virtually all major families of classical codes have a quantum counterpart. Amongst these, short block codes are particularly important from an implementation perspective, since the quantum technology is still in its infancy and hence decoherence would prevent the implementation of long codes. However, the desire to approach the hashing bound of Fig. 9 motivated researchers to design QLDPC [103], [146]–[148] codes and QTCs [112], [113], which exploit iterative decoding. In particular, the sparse nature of LDPC matrix is particularly important in the quantum domain for achieving fault-tolerant decoding, since the qubits interact with only a limited number of other qubits during the syndrome computation process. Furthermore, since the LDPC matrix is sparse, the resultant QLDPC codes exhibit high degeneracy. However, the strict symplectic product criterion associated with the design of stabilizer codes severely limits the performance of QLDPC codes. More specifically, owing to the symplectic criterion, the QLDPC matrix consists of numerous short cycles, which have a length of 4. This in turn degrades the performance of the LDPC decoder relying on the message passing algorithm, as detailed in [116]. Unfortunately, the LDPC decoder is not capable of capturing the impact of degenerate errors. In fact, the LDPC decoder suffers from the so-called 'symmetric degeneracy error' [116], which results from the degenerate errors. For the sake of improving the performance of the LDPC decoder in the wake of length-4 cycles and the symmetric degeneracy error, Poulin *et al.* conceived heuristic methods in [114]. These methods primarily relied on introducing random perturbations for triggering decoding convergence. Then the QLDPC decoding methods were further improved in [115], [116]. Despite these developments, the performance of QLDPC codes is still not comparable to that of classical LDPC codes.

In 2008, Poulin *et al.* constructed the quantum counterparts of turbo codes in [112], [113]. While classical turbo codes generally rely on the parallel concatenation of convolutional codes, the QTCs of [112], [113] rely on the serial concatenation of QCCs. As compared to QLDPC codes, QTCs offer more flexible code parameters, for example the frame length, coding rate, constraint length as well as the interleaver type. Furthermore, the iterative decoding of QTCs takes into account the impact of degenerate errors. However, the stabilizer-based QCCs cannot be concurrently recursive as well as noncatastrophic[8] [112], [113], [152]. Both these properties are essential for constructing good turbo codes. Explicitly, a recursive inner code

[6] Let C be a classical linear block code having the generator matrix $\mathbf{G}$ and the PCM $\mathbf{H}$, then the dual code $C^{\perp}$ is the code having the generator matrix $\mathbf{H}^T$ and the PCM $\mathbf{G}^T$.

[7] Further details are given in Section VI.

[8] An encoder is catastrophic if it outputs a finite-weight coded sequence for an infinite-weight input sequence. Consequently, a catastrophic code may result in catastrophic error propagation, since a finite number of errors on the coded sequence may yield infinite number of errors on the decoded sequence. This in turn implies that the constituent codes of a concatenated code must be non-catastrophic for the sake of achieving decoding convergence.

is required for achieving an unbounded minimum distance[9], while both component codes of a serially concatenated code must be noncatastrophic for ensuring decoding convergence to an infinitesimally low error rate. Hence, the QTCs of [112], [113] exhibit a bounded minimum distance, since they rely on non-recursive non-catastrophic QCCs. For the sake of designing near-capacity QTCs, Babar *et al.* [127] developed EXIT charts for the quantum domain, while a Quantum IrRegular Convolutional Code (QIRCC) structure and Quantum Unity Rate Code (QURC) were proposed in [129] and [131], respectively. Recently, a Fully-Parallel Quantum Turbo Decoder (FPQTD) was conceived in [132], which substantially reduces the decoding latency, without degrading the performance.

Recall that stabilizer codes must satisfy the stringent symplectic product criterion. Consequently, not every classical code can be 'imported' into the quantum realm. Furthermore, the symplectic product criterion results in undesired code characteristics, for example the unavoidable length-4 cycles of QLDPC codes and the non-recursive nature of non-catastrophic QCCs. For the sake of overcoming the issues associated with the symplectic product criterion, the theory of EA quantum codes was developed in [105], [108]–[110], which relies on the pre-sharing of entanglement between the transmitter and the receiver. The notion of EA codes was adopted for nearly all coding families, including EA-QLDPC codes [119], EA-QCCs [120] and EA-QTCs [121], [122], hence alleviating the issues arising from the symplectic product criterion. Explicitly, EA-QLDPC codes may be designed with no length-4 cycles in the binary formalism. Consequently, the resultant performance is comparable to that of the classical LDPC codes. Similarly, EA-QCCs can be concurrently recursive as well as non-catastrophic [121], [122]. Consequently, EA-QTCs are capable of having an unbounded minimum distance. Hence, the family of EA quantum codes finally brought the performance of quantum codes in line with that of their classical counterparts.

Polar codes have also attracted considerable attention within the quantum research fraternity. Inspired by the provably capacity achieving nature of Arikan's polar codes as well as their efficient encoding and decoding structures, Wilde and Guha demonstrated the existence of the quantum channel polarization phenomenon for classical and quantum information in [123] and [124], respectively. The quantum polar codes of [123], [124] invoked a quantum-domain successive cancellation decoder, which is based on the notion of quantum hypothesis testing. The resultant decoder failed to match the decoding complexity of Arikan's successive cancellation decoder. This issue was addressed by Renes *et al.* in [125], where CSS-type quantum polar codes were constructed from the classical polar codes, resulting in quantum codes having efficient encoders as well as decoders. However, the quantum polar codes of [123]–[125] rely on the sharing of noiseless entanglement between the transmitter and the receiver. In this context, the first unassisted quantum polar codes were recently conceived in [130], which marks another major milestone in the development of quantum codes.

IV. Classical-to-Quantum Transition

The peculiar laws of quantum mechanics make quantum coding intrinsically different from their classical counterparts. Nevertheless, efficient quantum codes can be designed from the existing families of classical codes by cautiously addressing the following challenges, which do not exist in the classical realm.

1) **No-Cloning Theorem:** Most classical error correction codes rely on cloning. Explicitly, multiple copies of the information bits are transmitted for the sake of providing redundancy. Unfortunately, it is not possible to clone an arbitrary unknown qubit due to the no-cloning theorem [153].
2) **Measurement Operation:** Classical codes rely on measuring (or observing) the values of the received bits for hard-decision as well as soft-decision aided decoding. Unfortunately, it is not possible to measure (or observe) a qubit without perturbing it, which would result in the superimposed quantum states collapsing to the classical domain upon measurement.
3) **Nature of Quantum Errors:** Classical channels only impose bit-flip errors. By contrast, quantum channels inflict both bit-flips as well as phase-flip errors. Furthermore, quantum impairments are continuous in nature, since the received qubit may assume any value on the Bloch sphere.

In this Section, we elaborate on these challenges by designing the quantum counterparts of the simple rate-$1/3$ classical repetition code, which can only correct a single classical error. The overall evolution is summarized in Fig. 10 at a glance.

1) No-Cloning Theorem: *Quantum codes exploit quantum-domain redundancy without cloning the information qubits.*

The encoder of a 3-bit classical repetition code copies each information bit thrice. Explicitly, the information bits 0 and 1 are encoded as follows:

$$0 \rightarrow (000) \qquad\qquad 1 \rightarrow (111)\,. \tag{28}$$

The encoding process of Eq. (28) does not have a quantum equivalent, because quantum information processing does not permit cloning. Let $\mathcal{U}$ be a hypothetical cloning (or copying) operation described as:

$$\mathcal{U}|\psi\rangle = |\psi\rangle \otimes |\psi\rangle. \tag{29}$$

Eq. (29) can be expanded as:

$$\begin{aligned}\mathcal{U}|\psi\rangle &= (\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle) \\ &= \alpha^2|00\rangle + \alpha\beta|01\rangle + \alpha\beta|10\rangle + \beta^2|11\rangle.\end{aligned} \tag{30}$$

Alternatively, Eq. (29) can also be evaluated by considering

[9] A code exhibits an 'unbounded minimum distance', if its minimum distance increases almost linearly with increasing the block (or equivalently frame) length.

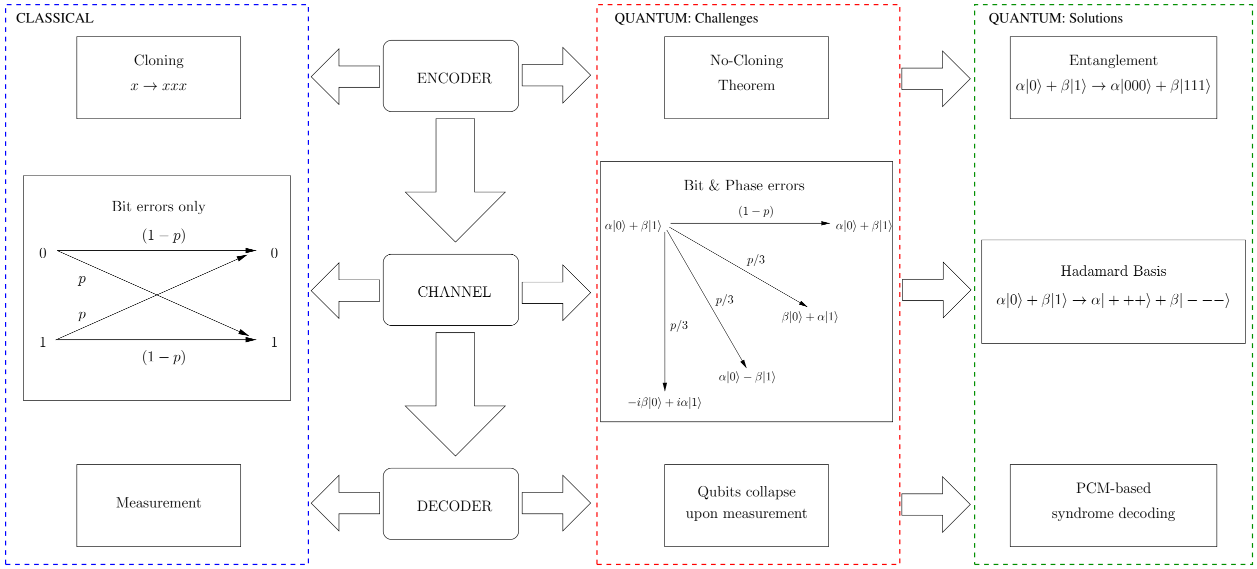

CLASSICAL
Cloning
$x \to xxx$
Bit errors only
$(1-p)$
0
0
p
p
1
1
$(1-p)$
Measurement
ENCODER
CHANNEL
DECODER
QUANTUM: Challenges
No-Cloning Theorem
Bit & Phase errors
$\alpha|0\rangle + \beta|1\rangle$
$(1-p)$
$\alpha|0\rangle + \beta|1\rangle$
$p/3$
$\beta|0\rangle + \alpha|1\rangle$
$p/3$
$\alpha|0\rangle - \beta|1\rangle$
$p/3$
$-i\beta|0\rangle + i\alpha|1\rangle$
Qubits collapse upon measurement
QUANTUM: Solutions
Entanglement
$\alpha|0\rangle + \beta|1\rangle \to \alpha|000\rangle + \beta|111\rangle$
Hadamard Basis
$\alpha|0\rangle + \beta|1\rangle \to \alpha|+++\rangle + \beta|---\rangle$
PCM-based syndrome decoding

Fig. 10: Transition of error correction codes from the classical to the quantum domain [129]. **Encoder**: Classical encoders copy the information bits. Unfortunately, no quantum cloning operator exists. Consequently, quantum codes entangle the information qubits with the auxiliary qubits, so that the information is cloned in the basis states. **Channel**: Classical information may experience only bit-flip errors, while qubits may experience bit-flip as well as phase-flip errors. The additional phase-flip errors of the quantum domain may be corrected by using the Hadamard basis $\{|+\rangle, |-\rangle\}$. **Decoder**: Classical decoders measure the received bits for estimating the transmitted information. Unfortunately, qubits cannot be measured without perturbing their superimposed quantum state. As an alternate, quantum codes rely on the PCM-based syndrome decoding, hence estimating the channel-induced error patterns without measuring the received qubits.

the linearity of the cloning operator. Consequently, we have:

$$\begin{aligned} \mathcal{U}|\psi\rangle &= \mathcal{U}\left(\alpha|0\rangle + \beta|1\rangle\right) \\ &= \alpha\, \mathcal{U}|0\rangle + \beta\, \mathcal{U}|0\rangle \\ &= \alpha|00\rangle + \beta|11\rangle. \end{aligned} \tag{31}$$

It can be readily seen in Eq. (30) and Eq. (31) that:

$$\mathcal{U}\left(\alpha|0\rangle + \beta|1\rangle\right) \neq \alpha\, \mathcal{U}|0\rangle + \beta\, \mathcal{U}|0\rangle, \tag{32}$$

which violates the linearity of cloning operation. Hence, no cloning operator $\mathcal{U}$ exists in the quantum domain. Consequently, $|\psi\rangle$ cannot be encoded to $(|\psi\rangle \otimes |\psi\rangle \otimes |\psi\rangle)$. The 3-qubit bit-flip repetition code overcomes the cloning constraint by cloning the basis states rather than the state $|\psi\rangle$, i.e. the computational basis states $|0\rangle$ and $|1\rangle$ are encoded as follows:

$$\begin{aligned} |0\rangle &\to |\overline{0}\rangle \equiv |000\rangle, \\ |1\rangle &\to |\overline{1}\rangle \equiv |111\rangle. \end{aligned} \tag{33}$$

Explicitly, two auxiliary qubits in state $|0\rangle$ are *entangled* with the information qubit $|\psi\rangle$ with the aid of Controlled-NOT (CNOT) gates, as shown in the circuit of Fig. 11. CNOT represents a two-qubit gate, which takes as its input a control qubit and a target qubit. When the control qubit is in state $|1\rangle$, the target qubit is flipped; otherwise, the target qubit is left unchanged. This can be mathematically expressed as:

$$\text{CNOT}\left(|\psi_0\rangle, |\psi_1\rangle\right) = |\psi_0\rangle \otimes |\psi_0 \oplus \psi_1\rangle, \tag{34}$$

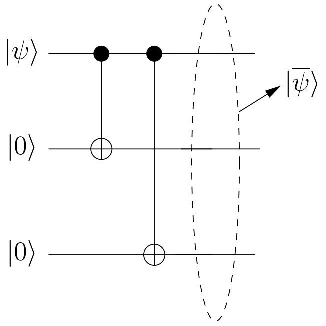


Fig. 11: Encoding circuit of 3-qubit bit-flip repetition code, where the information qubit $|\psi\rangle$ is encoded into $|\overline{\psi}\rangle$ with the help of two auxiliary qubits.

where $|\psi_0\rangle$ is the control qubit, while $|\psi_1\rangle$ is the target qubit. Consequently, the encoder of Fig. 11 replicates the computational basis states $|0\rangle$ and $|1\rangle$ three times in the encoded 3-qubit output $|\overline{\psi}\rangle$, which is given by:

$$\begin{aligned} |\psi\rangle \otimes |0\rangle^{\otimes 2} \to |\overline{\psi}\rangle &= \alpha|\overline{0}\rangle + \beta|\overline{1}\rangle \\ &\equiv \alpha|000\rangle + \beta|111\rangle. \end{aligned} \tag{35}$$

Syndrome $\mathbf{s}$	Error $\mathbf{e}$
(00)	(000)
(11)	(100)
(10)	(010)
(01)	(001)

TABLE I: Look-up table for the rate-$1/3$ classical repetition code.

2) Measurement Operation: *Quantum codes have to estimate the channel errors imposed without measuring (or observing) the received qubits.*

At the receiver, the decoder of a 3-bit classical repetition code reads the received bits and decodes on the basis of majority voting. For example, the received codeword (011) is decoded to 1, while (100) is decoded to 0. This requires measuring (or observing) the received sequence, which is unfortunately not possible in the quantum domain. Explicitly, if the received qubit $(\alpha|0\rangle + \beta|1\rangle)$ is measured in the computational basis, it will collapse to the states $|0\rangle$ and $|1\rangle$ with a probability of $|\alpha|^2$ and $|\beta|^2$, respectively.

Alternatively, an (n, k) classical linear block code can be decoded using an $(n-k) \times n$-element Parity Check Matrix (PCM) $\mathbf{H}$, so that all error-free legitimate codewords $\overline{\mathbf{x}}$ yield:

$$\overline{\mathbf{x}}\mathbf{H}^T = 0, \tag{36}$$

Given a received codeword $\mathbf{y} = \overline{\mathbf{x}} + \mathbf{e}$, where $\mathbf{e}$ is the channel-induced error vector, the associated $(n-k)$-bit syndrome vector, which uniquely and unambiguously identifies the error vector (if the number of channel-induced errors is within the error correction capability of the code), is computed as:

$$\mathbf{s} = \mathbf{y}\mathbf{H}^T = (\overline{\mathbf{x}} + \mathbf{e})\mathbf{H}^T = \overline{\mathbf{x}}\mathbf{H}^T + \mathbf{e}\mathbf{H}^T = \mathbf{e}\mathbf{H}^T. \tag{37}$$

Hence, the syndrome can be used for estimating the error vector $\mathbf{e}$ using a pre-computed Look-Up Table (LUT). More explicitly, since an (n, k) linear block code has $(n-k)$ parity bits, we have $2^{(n-k)}$ unique syndromes. Consequently, we can estimate $2^{(n-k)}$ unique n-bit error patterns, which are pre-computed and stored in an LUT. Similarly, a 3-bit classical repetition code can also be decoded using the PCM-based syndrome decoding[10]. The associated PCM is given by:

$$\mathbf{H} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \tag{38}$$

which yields a zero-valued syndrome vector for both valid codewords (111) and (000), while at least one of the two syndrome elements is 1 when a single bit-flip error is experienced. The resultant LUT is given in Table I, which records all the single bit-flip errors that may be estimated with the help of a 3-bit classical repetition code. Intuitively, the first row of $\mathbf{H}$ compares the first two received bits of $\mathbf{y}$. If both bits are equal, the associated syndrome bit is 0, while if they are different, then the syndrome bit is 1. Similarly, the second row of $\mathbf{H}$ compares the first and third bit of $\mathbf{y}$.

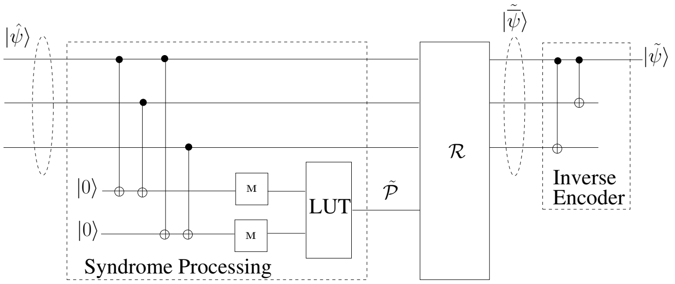


Fig. 12: Decoding circuit of 3-qubit bit-flip repetition code.

Working along similar lines, a 3-qubit bit-flip repetition code can be decoded using a syndrome decoder, which simply compares the qubits without actually knowing their specific values. This is achieved by using two additional auxiliary qubits and the CNOT gates of Eq. (34), as shown in the 'Syndrome Processing' block of Fig. 12. Explicitly, it may be observed in Fig. 12 that the first auxiliary qubit is flipped, if the first two qubits are different, while the second auxiliary qubit is flipped, when the first and third qubits are different. Explicitly, if $|\psi\rangle$ is transmitted, then we may receive one of the following four codewords $|\hat{\psi}\rangle$, assuming that only a single bit-flip is incurred during transmission:

$$\begin{aligned} \alpha|000\rangle + \beta|111\rangle &\xrightarrow{\mathbf{III}} \alpha|000\rangle + \beta|111\rangle, \\ \alpha|000\rangle + \beta|111\rangle &\xrightarrow{\mathbf{XII}} \alpha|100\rangle + \beta|011\rangle, \\ \alpha|000\rangle + \beta|111\rangle &\xrightarrow{\mathbf{IXI}} \alpha|010\rangle + \beta|101\rangle, \\ \alpha|000\rangle + \beta|111\rangle &\xrightarrow{\mathbf{IIX}} \alpha|001\rangle + \beta|110\rangle. \end{aligned} \tag{39}$$

The syndrome computation process operates on each of the possible received codeword $|\hat{\psi}\rangle$ as follows. Firstly, if both the first and second qubits as well as the first and third qubits remain identical, as in the case of error vector $\mathbf{III}$, the auxiliary qubits remain unaltered:

$$\begin{aligned} \alpha|000\rangle + \beta|111\rangle \otimes |0\rangle^{\otimes 2} &\rightarrow \alpha|00000\rangle + \beta|11111\rangle \\ &= (\alpha|000\rangle + \beta|111\rangle)\,|00\rangle. \end{aligned} \tag{40}$$

Secondly, when both the first and second qubits as well as the first and third qubits are different, as in the case of error vector $\mathbf{XII}$, both auxiliary qubits are flipped:

$$\begin{aligned} \alpha|100\rangle + \beta|011\rangle \otimes |0\rangle^{\otimes 2} &\rightarrow \alpha|10011\rangle + \beta|01111\rangle \\ &\equiv (\alpha|100\rangle + \beta|011\rangle)\,|11\rangle. \end{aligned} \tag{41}$$

Thirdly, when the first and second qubits are different, but the first and third qubits are identical, as in the case of error vector $\mathbf{IXI}$, only the first auxiliary qubit is flipped.

$$\begin{aligned} \alpha|010\rangle + \beta|101\rangle \otimes |0\rangle^{\otimes 2} &\rightarrow \alpha|01010\rangle + \beta|10110\rangle \\ &= (\alpha|010\rangle + \beta|101\rangle)\,|10\rangle. \end{aligned} \tag{42}$$

[10] In contrast to the conventional codeword decoding, which finds the most likely codeword, having the minimum Hamming distance, syndrome decoding finds the most likely error, having the minimum Hamming weight.

Finally, when the first and second qubits are identical, but the first and third qubits are different, as in the case of error vector $\mathbf{IIX}$, only the second auxiliary qubit is flipped.

$$\begin{aligned}\alpha|001\rangle + \beta|110\rangle \otimes |0\rangle^{\otimes 2} &\rightarrow \alpha|00101\rangle + \beta|11001\rangle \\ &= (\alpha|001\rangle + \beta|110\rangle)\,|01\rangle. \quad (43)\end{aligned}$$

Then the auxiliary qubits of Eq. (40) Eq. (43) are measured in the block M of Fig. 12 to yield the classical syndrome $\mathbf{s}$, which can take one of the four possible values, i.e. 00, 11, 10 and 01. The syndrome $\mathbf{s}$ can then be used for estimating the error $\tilde{\mathcal{P}}$ using the LUT of Fig. 12 seen in Table I. Thereafter, the transmitted codeword is recovered by applying the recovery operation $\mathcal{R}$ of Fig. 12, which aims for correcting the channel-induced flips based on the estimated error $\tilde{\mathcal{P}}$. Explicitly, in the context of the 3-qubit bit-flip repetition code, Pauli-$\mathbf{X}$ gates are applied during the recovery process for counteracting the impact of the estimated channel error patterns of Table I. Finally, the estimated information word $|\tilde{\psi}\rangle$ is retrieved by feeding the recovered codeword $|\tilde{\overline{\psi}}\rangle$ to the inverse encoder circuit, which is the same as that in Fig. 11, but operates from right to left, hence mapping the recovered encoded qubits onto the information qubits. It is pertinent to mention here that a classical repetition code is systematic in nature. Consequently, the information bit can be extracted from the received codeword without invoking an inverse encoding operation. By contrast, the information qubit of a quantum repetition code is entangled with auxiliary qubits and hence cannot be separated without an inverse encoder. For example, if $|\tilde{\overline{\psi}}\rangle = \alpha|000\rangle + \beta|111\rangle$, then applying the two CNOT gates of the inverse encoder of Fig. 11 yields:

$$\begin{aligned}\alpha|000\rangle + \beta|100\rangle &= (\alpha|0\rangle + \beta|1\rangle)|00\rangle \\ &\equiv |\tilde{\psi}\rangle|00\rangle, \qquad (44)\end{aligned}$$

hence separating the information qubit $|\tilde{\psi}\rangle$ from the auxiliary qubits $|00\rangle$.

3) Nature of Quantum Errors: *Quantum codes correct quantum bit-flip, phase-flip as well as bit-and-phase-flip errors.*

When the classical coded bits (000) or (111) are transmitted, a 0 may be flipped to a 1 and a 1 may be flipped to a 0. Consequently, only discrete bit-flip errors are imposed on the transmitted codewords. By contrast, when a qubit is transmitted over the depolarizing channel of Section II-C, it may experience bit-flip, phase-flip as well as bit-and-phase flip errors, as discussed in Section II. A 3-qubit phase-flip repetition code may be designed analogous to the bit-flip repetition code, since phase-flips and bit-flips only differ in their basis of operation. More specifically, bit-flips flip the computational basis $\{|0\rangle, |1\rangle\}$, while phase-flips flip the Hadamard basis $\{|+\rangle, |-\rangle\}$ defined as:

$$\begin{aligned}|+\rangle &\equiv \mathrm{H}|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \\ |-\rangle &\equiv \mathrm{H}|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}, \qquad (45)\end{aligned}$$

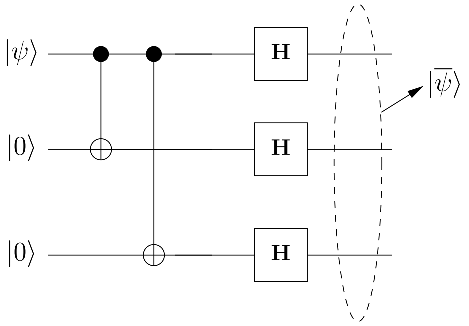


Fig. 13: Encoding circuit of 3-qubit phase-flip repetition code, where the information qubit $|\psi\rangle$ is encoded into $|\overline{\psi}\rangle$ with the help of two auxiliary qubits.

where H represents a Hadamard gate acting on a single qubit and specified by the matrix [3]:

$$\mathrm{H} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1 \\ 1 & -1\end{pmatrix}. \qquad (46)$$

Therefore, a phase-flip (Pauli-$\mathbf{Z}$) switches the Hadamard basis states as follows:

$$\begin{aligned}\mathbf{Z}|+\rangle &= |-\rangle, \\ \mathbf{Z}|-\rangle &= |+\rangle, \qquad (47)\end{aligned}$$

while a bit-flip (Pauli-$\mathbf{X}$) switches the computational basis, i.e. we have:

$$\begin{aligned}\mathbf{X}|0\rangle &= |1\rangle, \\ \mathbf{X}|1\rangle &= |0\rangle. \qquad (48)\end{aligned}$$

Hence, a 3-qubit phase-flip repetition code protects against single phase-flip errors by replicating the Hadamard basis states rather than the information qubit as follows:

$$\begin{aligned}|0\rangle &\rightarrow |\overline{0}\rangle \equiv |+++\rangle, \\ |1\rangle &\rightarrow |\overline{1}\rangle \equiv |---\rangle. \qquad (49)\end{aligned}$$

This can be achieved by using the encoding circuit of Fig. 13, which entangles two auxiliary qubits with the information qubit $|\psi\rangle$ using CNOT and Hadamard gates. The circuit of Fig. 11 is similar to that of the bit-flip repetition code. However, it invokes additional Hadamard gates, which transform the computational basis to the Hadamard basis. Consequently, $|\psi\rangle$ is encoded as:

$$\begin{aligned}|\psi\rangle \otimes |0\rangle^{\otimes 2} \rightarrow |\overline{\psi}\rangle &= \alpha|\overline{0}\rangle + \beta|\overline{1}\rangle \\ &\equiv \alpha|+++\rangle + \beta|---\rangle. \qquad (50)\end{aligned}$$

Analogous to the 3-qubit bit-flip repetition decoder, the decoder of a 3-qubit phase-flip repetition code also uses two auxiliary qubits for computing the associated 2-bit syndromes. The first syndrome compares the phase of the first and second qubits, while the second syndrome compares the phase of the first and third qubits. This may be achieved using the decoding circuit of Fig. 14, which is the same as that of the

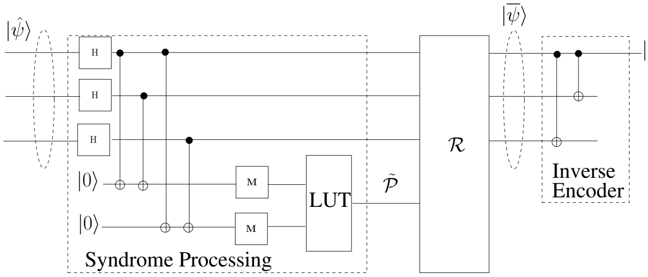


Fig. 14: Decoding circuit of 3-qubit phase-flip repetition code.

3-qubit bit-flip repetition code with the additional Hadamard gates invoked for transforming the Hadamard basis back to the computational basis. In other words, we may say that Hadamard gates are used at the input and output of the channel to transform the phase-flips to bit-flips. Hence, both bit-flip and phase-flip errors can be corrected by concatenating the 3-qubit phase-flip and bit-flip repetition codes, which actually constitutes the rate-$1/9$ Shor code [77] capable of correcting a single bit-flip, or phase-flip or alternatively a bit-and-phase-flip error. More specifically, the information qubit is first encoded in Hadamard basis using the mapping of Eq. (50). The resultant three coded qubits are then independently encoded using the bit-flip repetition code of Eq. (35). Hence, the basis states are mapped onto three 3-qubit blocks as follows:

$$\begin{aligned}|\overline{0}\rangle &\equiv \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right)\\ &\quad \otimes \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right),\\ |\overline{1}\rangle &\equiv \frac{1}{\sqrt{2}}\left(|000\rangle - |111\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|000\rangle - |111\rangle\right)\\ &\quad \otimes \frac{1}{\sqrt{2}}\left(|000\rangle - |111\rangle\right),\end{aligned} \tag{51}$$

where the three qubits within a block are the codewords of a bit-flip repetition code, while the three blocks are the result of phase-flip repetition encoding. Taking the tensor product in Eq. (51) yields:

$$\begin{aligned}|\overline{0}\rangle &\equiv \frac{1}{\sqrt{8}}(|000000000\rangle + |000000111\rangle + |000111000\rangle\\ &\quad + |000111111\rangle + |111000000\rangle + |111000111\rangle\\ &\quad + |111111000\rangle + |111111111\rangle),\\ |\overline{1}\rangle &\equiv \frac{1}{\sqrt{8}}(|000000000\rangle - |000000111\rangle - |000111000\rangle\\ &\quad + |000111111\rangle - |111000000\rangle + |111000111\rangle\\ &\quad + |111111000\rangle - |111111111\rangle).\end{aligned} \tag{52}$$

Consequently, the encoded state $|\overline{\psi}\rangle$ is equivalent to:

$$\begin{aligned}\alpha|\overline{0}\rangle + \beta|\overline{1}\rangle &\equiv \frac{1}{\sqrt{8}}(\alpha+\beta)(|000000000\rangle + |000111111\rangle\\ &\quad + |111000111\rangle + |111111000\rangle) + \frac{1}{\sqrt{8}}(\alpha-\beta)\\ &\quad (|000000111\rangle + |000111000\rangle + |111000000\rangle\\ &\quad + |111111111\rangle),\end{aligned} \tag{53}$$

which may be decoded by concatenating the decoding circuits of Fig. 12 and Fig. 14. Explicitly, the three 3-qubit blocks of Eq. (51) are first independently decoded using the 3-qubit bit-flip repetition decoder of Fig. 12, resulting in three information qubits, which constitute the received codeword for the 3-qubit phase-flip repetition decoder. Consequently, the resultant three qubits are decoded using the 3-qubit phase-flip repetition decoder of Fig. 14.

Furthermore, as encapsulated in Eq. (22), the received qubit may be in the superposition of all the possible errors. In essence, an (n,k) classical code, designed to protect a k-bit message by encoding it into an n-bit codeword, aims for restoring one of the 2^k valid codewords. By contrast, since a k-qubit information word is completely described by 2^k continuous-valued complex coefficients, quantum codes have to restore all the 2^k complex coefficients [146]. Fortunately, this continuous search space is reduced to a discrete one upon the measurement of the auxiliary qubits used for computing the syndrome. More specifically, although the 2^k coefficients are continuous-valued, some what serendipitously, the entire continuum of errors can be rectified, if the code is capable of correcting discrete bit-flip, phase-flip as well as bit-and-phase-flip errors acting on the constituent qubits. For example, let us assume that only a single bit-flip error may be inflicted during transmission. Then the received codeword of a 3-bit repetition code can be expressed as:

$$|\hat{\psi}\rangle = p_0\mathbf{III}|\overline{\psi}\rangle + p_1\mathbf{XII}|\overline{\psi}\rangle + p_2\mathbf{IXI}|\overline{\psi}\rangle + p_3\mathbf{IIX}|\overline{\psi}\rangle, \tag{54}$$

where p_0 is the probability of error-free transmission, while p_i is the probability of encountering a bit-flip error on the ith qubit. The syndrome computation process of Fig. 12 entangles two auxiliary qubits with $|\hat{\psi}\rangle$ of Eq. (54) as:

$$\begin{aligned}|\hat{\psi}\rangle \otimes |0\rangle^{\otimes 2} \rightarrow & p_0\left(\mathbf{III}|\overline{\psi}\rangle\right)|00\rangle + p_1\left(\mathbf{XII}|\overline{\psi}\rangle\right)|11\rangle\\ & + p_2\left(\mathbf{IXI}|\overline{\psi}\rangle\right)|10\rangle + p_3\left(\mathbf{IIX}|\overline{\psi}\rangle\right)|01\rangle,\end{aligned} \tag{55}$$

which collapses to one of the four superimposed states when the auxiliary qubits are measured. The resultant state can then be corrected based on the specific syndrome observed.

V. Stabilizer Formalism

The family of Quantum Stabilizer Codes (QSCs) rely on the same design principles as that of the repetition codes of Section IV. In particular, QSCs rely on the PCM-based syndrome decoding of classical linear block codes, hence, finding the channel-induced error by measuring the auxiliary syndrome qubits, rather than by observing the received qubits.

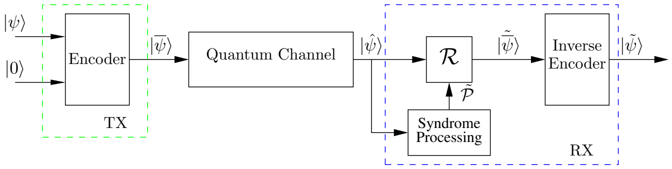


Fig. 15: Schematic of a quantum communication system invoking a quantum stabilizer code for error correction [116].

Intuitively, the stabilizer formalism [84], [85] may be interpreted as the quantum-domain dual of the classical linear block coding paradigm. Furthermore, most classical codes exploit the same basic infrastructure as that of the classical linear block codes. Consequently, the stabilizer formalism provides a general theoretical framework for designing the quantum versions of the known classical codes. In Section V-A, we provide deeper insights into the duality of QSCs and classical linear block codes, while in Section V-B, we discuss the classification of error patterns for both the QSCs as well as the classical linear block codes.

A. Stabilizer-based Code Design

Fig. 15 shows the system model of a quantum communication system relying on a QSC. A classical linear block code $C(n, k)$ encodes k-bit information word x into an n-bit codeword $\overline{x}$ with the aid of $(n-k)$ parity bits $\mathbf{0}^{n-k}$ (initialized to zeros) as follows:

$$C = \{\overline{x} = \left(x : \mathbf{0}^{n-k}\right)\mathbf{V}\}, \tag{56}$$

where $\mathbf{V}$ is an invertible encoding matrix of size $(n \times n)$. Similarly, a QSC $\mathcal{C}[n, k]$[11] encodes a k-qubit information word (logical qubits) $|\psi\rangle$ into an n-qubit codeword (physical qubits) $|\overline{\psi}\rangle$ with the help of $(n-k)$ auxiliary qubits (also known as ancilla), as follows:

$$\mathcal{C} = \{|\overline{\psi}\rangle = \mathcal{V}(|\psi\rangle \otimes |\mathbf{0}_{n-k}\rangle)\}, \tag{57}$$

where $\mathcal{V}$ is an n-qubit unitary encoder. Explicitly, the auxiliary qubits of a QSC are analogous to the classical parity bits. The encoded qubits $|\overline{\psi}\rangle$ are transmitted over the quantum depolarizing channel of Section II-C, which imposes an n-qubit channel error vector $\mathcal{P}$. The erroneous channel output $|\hat{\psi}\rangle$ may then be expressed as:

$$|\hat{\psi}\rangle = \mathcal{P}|\overline{\psi}\rangle. \tag{58}$$

Similar to the decoders of the 3-qubit bit-flip and phase-flip repetition codes of Fig. 12 and Fig. 14, the decoder of a QSC invokes a 3-step process for correcting the transmission errors, which includes syndrome processing, error recovery ($\mathcal{R}$) and the inverse encoder.

Let us now revisit the 'syndrome processing' block of 3-qubit bit-flip repetition code from the perspective of the stabilizer formalism. Recall from Fig. 12 that we compute the first syndrome bit by comparing the first and second qubits in computational basis, while the second syndrome is obtained by comparing the first and third qubits. This is equivalent to measuring the eigenvalues[12] corresponding to the 3-qubit Pauli operators $g_1 = \mathbf{ZZI}$ and $g_2 = \mathbf{ZIZ}$, which are known as the stabilizer generators. Explicitly, Pauli-$\mathbf{Z}$ based stabilizer generators are used for comparing qubits in computational basis, because they are capable of detecting errors in the computational basis, i.e. bit-flip errors. If the qubits, which are being compared, are identical in computational basis, then the Pauli-$\mathbf{Z}$ based stabilizer generators yield an eigenvalue of $+1$, while if they are different, then the eigenvalue is -1. For example, if the received codeword is a valid one, implying that both the first and second qubits as well as the first and third qubits are identical as in Eq. (40), then we have:

$$\begin{aligned} g_1\left[|\overline{\psi}\rangle\right] &= \mathbf{ZZI}\left(\alpha|000\rangle + \beta|111\rangle\right) = |\overline{\psi}\rangle, \\ g_2\left[|\overline{\psi}\rangle\right] &= \mathbf{ZIZ}\left(\alpha|000\rangle + \beta|111\rangle\right) = |\overline{\psi}\rangle. \end{aligned} \tag{59}$$

Hence, the resultant eigenvalue is $+1$ for both g_1 as well as g_2, when a legitimate codeword is received. By contrast, if the corrupted codeword of $|\hat{\psi}\rangle = |100\rangle + \beta|011\rangle$ is received, implying that both the first and second qubits as well as the first and third qubits are different as in Eq. (41), then we have:

$$\begin{aligned} g_1\left[|\hat{\psi}\rangle\right] &= \mathbf{ZZI}\left(\alpha|100\rangle + \beta|011\rangle\right) \\ &= -\alpha|100\rangle - \beta|011\rangle = -|\hat{\psi}\rangle, \\ g_2\left[|\hat{\psi}\rangle\right] &= \mathbf{ZIZ}\left(\alpha|100\rangle + \beta|011\rangle\right) \\ &= -\alpha|100\rangle - \beta|011\rangle = -|\hat{\psi}\rangle, \end{aligned} \tag{60}$$

where both g_1 as well as g_2 yield an eigenvalue of -1. Recall from Eq. (36) that the PCM of a classical linear block code is designed so that it yields an all-zero syndrome vector for legitimate codewords, while yielding a non-zero syndrome vector for erroneous codewords, provided the number of channel-induced errors is within the error correction capability of the code. Similarly, the stabilizer generators of a QSC have to be designed, so that they yield an eigenvalue of $+1$ for legitimate codewords, while resulting in an eigenvalue of -1 for corrupted codewords. Hence, in duality to the PCM $\mathbf{H}$, which completely specifies the codes space of a classical code C, the stabilizer generators define the code space a QSC. Furthermore, the complete stabilizer group $\mathcal{H}$ of a QSC consists of all the stabilizer generators and their products. For example, the stabilizer group $\mathcal{H}$ of the 3-qubit bit-flip repetition code consists of the independent generators g_1 and g_2 as well as the product of g_1 and g_2, i.e. $\mathbf{IZZ}$.

The $+1$ and -1 eigenvalues of Eq. (60) are mapped onto the classical syndromes 0 and 1, respectively, when the constituent $\mathbf{Z}$ operators are realized using the quantum circuit of Fig. 16, where the circuit on the left may be deemed more popular, while the one on the right is the equivalent circuit more suitable

[11] We consistently use round brackets (.) for classical codes, while the square brackets [.] are used for quantum codes.

[12] The eigenvector of a linear transformation $\mathbf{T}$ is a non-zero vector $\mathbf{v}$, which only changes by a scaling factor when $\mathbf{T}$ is applied, i.e. $\mathbf{T}(\mathbf{v}) = \lambda\mathbf{v}$. The associated scaling factor λ is known as the eigenvalue.

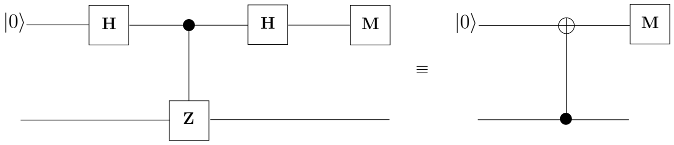


Fig. 16: Quantum circuit of measuring the $\mathbf{Z}$ operator acting on the bottom qubit [3] for bit-flip correction. The top qubit is the auxiliary qubit used for computing the syndrome. The circuit on the left is more popular, while the one on the right is more suitable for implementation.

$\vert\hat{\psi}\rangle = \mathcal{P}\vert\overline{\psi}\rangle$	$g_1\vert\hat{\psi}\rangle$	$g_2\vert\hat{\psi}\rangle$	**Syndrome (s)**	$\hat{\mathcal{P}}$
$\alpha\vert 000\rangle + \beta\vert 111\rangle$	$+1$	$+1$	(00)	**III**
$\alpha\vert 100\rangle + \beta\vert 011\rangle$	-1	-1	(11)	**XII**
$\alpha\vert 010\rangle + \beta\vert 101\rangle$	-1	$+1$	(10)	**IXI**
$\alpha\vert 001\rangle + \beta\vert 110\rangle$	$+1$	-1	(01)	**IIX**

TABLE II: Single-qubit bit-flip errors together with the associated eigenvalues for the 3-qubit bit-flip repetition code having $g_1 = \mathbf{ZZI}$ and $g_2 = \mathbf{ZIZ}$.

for implementation [3]. In both circuits of Fig. 16, the top qubit is the auxiliary qubit used for computing the syndrome, while the bottom qubit is the coded qubit subjected to the $\mathbf{Z}$ operator. The resultant syndromes are listed in Table II together with the associated single-qubit bit-flip errors, eigenvalues and the estimated error pattern $\hat{\mathcal{P}}$, which may be estimated using the syndrome decoding approach.

Analogous to the 3-qubit bit-flip repetition code, the codeword of a 3-qubit phase-flip repetition code is stabilized by the generators $g_1 = \mathbf{XXI}$ and $g_2 = \mathbf{XIX}$. We may notice here that while Pauli-$\mathbf{Z}$ based stabilizer generators are invoked for bit-flip detection, Pauli-$\mathbf{X}$ based stabilizer generators are invoked for comparing qubits in the Hadamard basis, because they are capable of detecting errors in the Hadamard basis, i.e phase-flip errors. The associated $\mathbf{X}$ operators can be implemented using the circuit of Fig. 17.

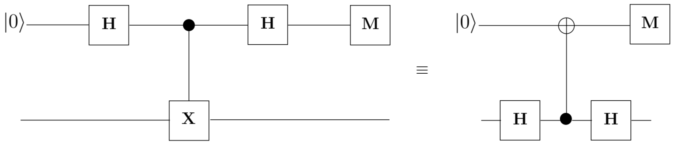


Fig. 17: Quantum circuit of measuring the $\mathbf{X}$ operator acting on the bottom qubit [3] for phase-flip correction. The top qubit is the auxiliary qubit used for computing the syndrome. The circuit on the left is the more usual conceptual construction, while the one on the right is more suitable for implementation.

Recall from Section IV that Shor's codewords consist of three 3-qubit blocks, so that the three qubits within each block constitute the codeword of a 3-qubit bit-flip repetition code. Consequently, bit-flips may be detected by independently applying the stabilizer generators of the 3-qubit bit-flip repetition code to the three 3-qubit blocks, which is equivalent to comparing the three qubits within each block. This results in the following six stabilizer generators:

$$\begin{aligned}
g_1 &= \mathbf{ZZIIIIIII}, \\
g_2 &= \mathbf{ZIZIIIIII}, \\
g_3 &= \mathbf{IIIZZIIII}, \\
g_4 &= \mathbf{IIIZIZIII}, \\
g_5 &= \mathbf{IIIIIIZZI}, \\
g_6 &= \mathbf{IIIIIIZIZ},
\end{aligned} \tag{61}$$

which helps in detecting single bit-flip errors occurring in each 3-qubit block. By contrast, phase-flip errors may be detected by comparing the blocks using Pauli-$\mathbf{X}$ operators. Explicitly, the phase information of a 3-qubit block is extracted by applying the $\mathbf{XXX}$ operator to the three qubits. For the 9-qubit Shor's code, which consists of three 3-qubit blocks, this may be implemented using the following two stabilizer generators:

$$\begin{aligned}
g_7 &= \mathbf{XXXXXXIII}, \\
g_8 &= \mathbf{XXXIIIXXX},
\end{aligned} \tag{62}$$

where g_7 compares the phase of the first two blocks, while g_8 compares the phase of the first and third blocks.

Based on the above discussions, the 3-step decoding process of Fig. 15 may be generalized as follows:

1) **Syndrome Processing:** While the code space C of a classical linear block code is defined by a PCM $\mathbf{H}$ having $(n-k)$ independent rows, the associated code space $\mathcal{C}$ of a QSC is described by $(n-k)$ independent n-qubit Pauli operators g_i, for $1 \leq i \leq (n-k)$, which are generally termed as the stabilizer generators (or stabilizers in short). Explicitly, stabilizers are unique operators, which do not perturb the state of legitimate codewords, hence yielding an eigenvalue of $+1$. Furthermore, stabilizers yield an eigenvalue of -1 for corrupted codewords, provided the number of channel-induced errors is within the error correction capability of the stabilizer code. This is equivalent to the classical syndrome values of 0 and 1, respectively, which are the elements of the syndrome vector of Eq. (37). Alternatively, we may say that resulting eigenvalue is $+1$, when the channel-induced error $\mathcal{P}$ commutes with the stabilizer g_i, while it is -1, when the error anti-commutes with g_i. This can be mathematically encapsulated as:

$$g_i|\hat{\psi}\rangle = \begin{cases} |\overline{\psi}\rangle, & g_i\mathcal{P} = \mathcal{P}g_i \\ -|\overline{\psi}\rangle, & g_i\mathcal{P} = -\mathcal{P}g_i, \end{cases} \tag{63}$$

where $|\hat{\psi}\rangle = \mathcal{P}|\overline{\psi}\rangle$. The resultant eigenvalues can be mapped onto the classical error syndrome s by invoking the quantum circuits of Fig. 16 and Fig. 17. Hence, the set of stabilizers constitute the quantum counterpart of the classical PCM. However, the stabilizers must exhibit the additional commutativity property, which states that the stabilizers must be each other's commutative pairs. Explicitly, for a pair of stabilizers g_1 and g_2, we have:

$$g_1 g_2|\overline{\psi}\rangle = g_1|\overline{\psi}\rangle = |\overline{\psi}\rangle, \tag{64}$$

and similarly:

$$g_2 g_1|\overline{\psi}\rangle = g_2|\overline{\psi}\rangle = |\overline{\psi}\rangle. \tag{65}$$

Hence, the commutativity criterion naturally arises, which does not exist in the classical realm. Furthermore, the associated stabilizer group $\mathcal{H}$, which contains the $(n-k)$ stabilizers g_i as well as all the products of g_i, forms an Abelian subgroup of $\mathcal{G}_n$.

The decoder of Fig. 15 processes the syndrome of the received sequence $|\hat{\overline{\psi}}\rangle$ with the aid of the associated stabilizers, which are implemented using auxiliary qubits. Analogous to the decoders of the 3-qubit bit-flip and phase-flip repetition codes seen in Fig. 12 and Fig. 14, respectively, the auxiliary qubits collapse to classical syndromes upon measurement, hence mapping the eigenvalues of $+1$ and -1 onto the classical bits 0 and 1, respectively. The resultant classical syndrome bits are then fed to an LUT or to a classical PCM-based syndrome decoder for estimating the channel error vector $\tilde{\mathcal{P}}$ (discussed further in Section VI).

2) **Error Recovery ($\mathcal{R}$):** The error recovery block $\mathcal{R}$ of Fig. 15 recovers the potentially error-free codeword $|\tilde{\overline{\psi}}\rangle$ using the estimated error pattern $\tilde{\mathcal{P}}$. Naturally, if the number of errors exceeds the codes' error-correction capability, the recovery process becomes flawed. Hence, its flawed corrective action actually precipitates more errors than we originally had.
3) **Inverse Encoder:** Finally, the inverse encoder of Fig. 15 maps the recovered codeword $|\tilde{\overline{\psi}}\rangle$ onto the estimated transmitted information word $|\tilde{\psi}\rangle$. More specifically, while an encoder maps the information words onto the codewords, an inverse encoder works in the reverse direction, hence mapping the codewords onto the information words.

Recall from Eq. (64) and Eq. (65) that the $(n-k)$ stabilizer generators g_i of a QSC always commute with each other. This implies that the constituent $\mathbf{X}$, $\mathbf{Y}$ and $\mathbf{Z}$ operations must be selected so that all the resultant stabilizers commute. Explicitly, the non-Identity $\mathbf{X}$, $\mathbf{Y}$ and $\mathbf{Z}$ operators intrinsically anti-commute with each other. For example, we have:

$$\mathbf{XY} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = i\mathbf{Z}, \tag{66}$$

while:

$$\mathbf{YX} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} = -i\mathbf{Z}. \tag{67}$$

This implies that the operators $\mathbf{XY}$ and $\mathbf{YX}$ anti-commute, i.e. we have:

$$\mathbf{XY} = -\mathbf{YX}. \tag{68}$$

Similarly, we can readily show that:

$$\begin{aligned} \mathbf{YZ} = i\mathbf{X},\ \mathbf{ZY} = -i\mathbf{X} \rightarrow \mathbf{YZ} = -\mathbf{ZY} \\ \mathbf{ZX} = i\mathbf{Y},\ \mathbf{XZ} = -i\mathbf{Y} \rightarrow \mathbf{ZX} = -\mathbf{XZ}. \end{aligned} \tag{69}$$

Owing to this anti-commutative nature of non-Identity Pauli operators, the stabilizers have to be designed so that there are only an even number of indices having different non-Identity operators. For example, the 3-qubit Pauli operators $\mathbf{ZZI}$ and $\mathbf{XYZ}$ commute, because they consist of two indices having different non-Identity operators. By contrast, the operators $\mathbf{ZZI}$ and $\mathbf{YZI}$ anti-commute, since there is a single index, which has different non-identity operators.

B. Classification of Error Patterns

Based on the aforementioned discussions, we may conclude that the stabilizer generators play the same role in quantum error correction as the classical PCM $\mathbf{H}$ in classical error correction. Explicitly, analogous to the classical PCM, stabilizers yield syndrome bits, which in turn help in estimating the quantum channel errors. More specifically, the error set of a classical linear block code C having a PCM $\mathbf{H}$ can be classified as:

1) **Detected Error Patterns:** These error patterns yield a non-trivial syndrome, i.e. $e\mathbf{H}^T \neq 0$, which may be corrected by the code.
2) **Undetected Error Patterns:** This class of error patterns results in a trivial syndrome, i.e. $e\mathbf{H}^T = 0$, which cannot be detected by the code. More specifically, an undetected error maps the transmitted codeword onto another valid codeword. Since the resultant codeword still lies in the code space C, it does not trigger a non-zero syndrome. These undetected error patterns result from the limited minimum distance of the code.

Analogous to the classical detected error patterns, quantum-domain detected error patterns anti-commute with at least one of the stabilizer generators, which results in a non-trivial syndrome. Similarly, the quantum undetected error patterns commute with all the stabilizer generators, yielding an all-zero syndrome. This commuting set of error patterns is also known as the centralizer (or normalizer) of the stabilizer code having the stabilizer group $\mathcal{H}$, which is denoted as $C(\mathcal{H})$ (or $N(\mathcal{H})$). In particular, the centralizer of an $[n, k]$ QSC is a dual subspace consisting of n-tuple Pauli errors $\mathcal{P} \in \mathcal{G}_n$, which are orthogonal to all the stabilizers of the stabilizer group $\mathcal{H}$. Furthermore, since the $\mathcal{H}$ is itself an Abelian group consisting of mutually orthogonal generators, it is contained in the centralizer, i.e. we have $\mathcal{H} \subset N(\mathcal{H})$. Recall that the stabilizer generators do not modify the state of valid codewords. This in turn implies that errors which belong to the stabilizer group, i.e. we have $\mathcal{P} \in \mathcal{H}$, do not corrupt the transmitted codewords and therefore may be classified as harmless undetected error patterns. This class of errors does not have any classical counterpart. By contrast, those error patterns, which lie in the subspace $N(\mathcal{H}) \setminus \mathcal{H}$, are the harmful undetected errors, which map one valid codeword onto another.

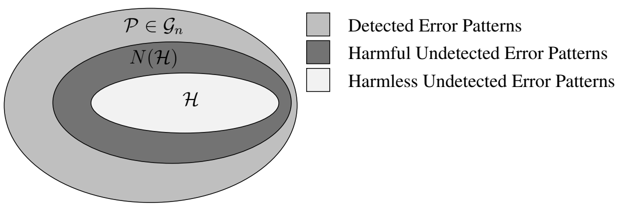

$\mathcal{P} \in \mathcal{G}_n$
$N(\mathcal{H})$
$\mathcal{H}$
Detected Error Patterns
Harmful Undetected Error Patterns
Harmless Undetected Error Patterns

Fig. 18: Error pattern classification for stabilizer codes.

Pauli	$(\mathbb{F}_2)^2$	GF(4)
I	00	0
X	01	1
Y	11	$\overline{\omega}$
Z	10	ω
Multiplication	Bit-wise Addition	Addition
Commutativity	Symplectic Product	Trace Inner Product

TABLE III: Quantum-to-classical isomorphism.

Hence, as depicted in Fig. 18, quantum error patterns can be classified as follows:

1) **Detected Errors Patterns:** These error patterns fall outside the normalizer subspace, i.e. they satisfy $\mathcal{P} \in \mathcal{G}_n \setminus N(\mathcal{H})$.
2) **Harmful Undetected Error Patterns:** This class of error patterns is defined as $N(\mathcal{S}) \setminus \mathcal{H}$.
3) **Harmless Undetected Errors Patterns:** These error patterns fall in the stabilizer group $\mathcal{H}$.

The class of harmless undetected error patterns makes quantum codes 'degenerate' [126]. More specifically, error patterns $\mathcal{P}$ and $\mathcal{P}' = g_i\mathcal{P}$ are said to be degenerate, because they differ only by the elements of the stabilizer group, which are harmless. Consequently, both $\mathcal{P}$ as well as $\mathcal{P}'$ yield the same output, as shown below:

$$\mathcal{P}'[|\overline{\psi}\rangle] = g_i\mathcal{P}[|\overline{\psi}\rangle] = \mathcal{P}g_i[|\overline{\psi}\rangle]. \tag{70}$$

Since $g_i[|\overline{\psi}\rangle] = |\overline{\psi}\rangle$, we get:

$$\mathcal{P}'[|\overline{\psi}\rangle] = \mathcal{P}[|\overline{\psi}\rangle]. \tag{71}$$

This in turn implies that degenerate error patterns can be rectified by the same recovery operation.

Let us consider the error patterns $\mathcal{P} = \mathbf{IIX}$ and $\mathcal{P}' = g_1\mathcal{P} = \mathbf{ZZX}$, where g_1 is the stabilizer of the 3-qubit bit-flip repetition code defined in Eq. (59). When these error patterns are applied to the legitimate codeword of Eq. (35), we get:

$$\begin{aligned} \mathbf{IIX}[\alpha|000\rangle + \beta|111\rangle] &= \alpha|001\rangle + \beta|110\rangle, \\ \mathbf{ZZX}[\alpha|000\rangle + \beta|111\rangle] &= \alpha|001\rangle + \beta|110\rangle. \end{aligned} \tag{72}$$

Hence, $\mathcal{P}$ and $\mathcal{P}'$ are degenerate errors, since both error patterns yield the same corrupted codeword. Furthermore, degeneracy enhances the achievable capacity, because the codewords are not corrupted by the harmless undetected error patterns; hence, the impact of quantum impairments is reduced. Equivalently, we may say that degeneracy enables a quantum code to pack more information as compared to the underlying classical design, because it can operate at a higher coding rate.

VI. Quantum-to-Classical Isomorphism

Based on the duality of QSCs and classical linear block codes established in Section V, in this section we present the isomorphism between these two regimes, which in turn helps in constructing the quantum-domain versions of the known classical codes. Explicitly, QSCs may be designed from binary and quaternary classical codes using the quantum-to-classical mappings of Table III, as detailed in Sections VI-A and VI-B, respectively. Furthermore, this quantum-to-classical isomorphism also allows us to use the classical PCM-based syndrome decoding procedures for decoding QSCs.

A. *Pauli-to-Binary Isomorphism*

Recall from Section V that stabilizers constitute the counterparts of the classical PCM. Based on this duality, QSCs can be described using an equivalent binary PCM, which in turn aids in designing quantum codes from the existing families of classical codes. More specifically, QSCs can be completely characterized in the binary formalism by an equivalent binary PCM $\mathbf{H}$ derived from the associated stabilizer generators. The rows of $\mathbf{H}$ correspond to the stabilizers, while the constituent $\mathbf{I}$, $\mathbf{X}$, $\mathbf{Y}$ and $\mathbf{Z}$ Pauli operators of the stabilizers are mapped onto a pair of binary digits as follows:

$$\mathbf{I} \rightarrow (00), \quad \mathbf{X} \rightarrow (01), \quad \mathbf{Z} \rightarrow (10), \quad \mathbf{Y} \rightarrow (11), \tag{73}$$

where a binary 1 at the first index represents a $\mathbf{Z}$ operator, while a binary 1 at the second index represents an $\mathbf{X}$ operator. The PCM $\mathbf{H}$ resulting from the Pauli-to-binary mapping of Eq. (73) can also be expressed as:

$$\mathbf{H} = \left(\mathbf{H}_z|\mathbf{H}_x\right), \tag{74}$$

where $\mathbf{H}_z$ and $\mathbf{H}_x$ are $(n-k) \times n$ binary matrices corresponding to the $\mathbf{Z}$ and $\mathbf{X}$ operators, respectively. Let us recall that the 3-qubit bit-flip repetition code relied on the stabilizers $g_1 = \mathbf{ZZI}$ and $g_2 = \mathbf{ZIZ}$. Consequently, the associated PCM $\mathbf{H}$ is given by:

$$\mathbf{H} = \left(\begin{array}{ccc|ccc} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \end{array}\right), \tag{75}$$

where $\mathbf{H}_x$ is an all-zero matrix, since g_1 and g_2 do not contain any Pauli-$\mathbf{X}$ operators. Furthermore, the $\mathbf{H}_z$ of Eq. (75) is identical to the PCM $\mathbf{H}$ of the classical repetition code given in Eq. (38), hence both yield identical syndrome patterns in Table I and Table II. Similarly, the PCM of the 3-qubit phase-flip repetition code is:

$$\mathbf{H} = \left(\begin{array}{ccc|ccc} 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{array}\right), \tag{76}$$

+	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

TABLE IV: $(\mathbb{F}_2)^2$ Addition.

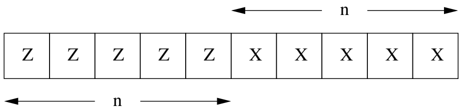


Fig. 19: Effective error P corresponding to the n-qubit Pauli error $\mathcal{P}$.

where we have $g_1 = \mathbf{XXI}$ and $g_2 = \mathbf{XIX}$, while that of Shor's code is given in Eq. (77).

$$\mathbf{H} = \left(\begin{array}{ccccccccc|ccccccccc} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \end{array}\right). \tag{77}$$

Hence, an $[n,k]$ QSC, having $(n-k)$ stabilizers, can be characterized by a binary PCM of size $(n-k) \times 2n$. Furthermore, the equivalent classical coding rate R_c can be determined as follows:

$$\begin{aligned} R_c &= \frac{2n-(n-k)}{2n} \\ &= \frac{n+k}{2n} \\ &= \frac{1}{2}\left(1+\frac{k}{n}\right) \\ &= \frac{1}{2}\left(1+R_Q\right), \end{aligned} \tag{78}$$

where R_Q is its quantum coding rate. Based on Eq. (78), the equivalent classical coding rate of the rate-$1/3$ quantum repetition code is $2/3$, while that of Shor's rate-$1/9$ code is $5/9$.

The binary formalism of Eq. (73) transforms the multiplication of Pauli operators into the bit-wise addition of the corresponding binary representation. For example, multiplying the set of Pauli operators $\{\mathbf{I}, \mathbf{X}, \mathbf{Z}, \mathbf{Y}\}$ with Pauli-$\mathbf{X}$ is equivalent to the second column of Table IV, if the Pauli operators are mapped onto $(\mathbb{F}_2)^2$ according to Eq. (73). Similarly, the commutative property of stabilizers in the Pauli formalism implies that the rows of the PCM $\mathbf{H}$ must be orthogonal to each other with respect to symplectic product (also referred to as a twisted product) in the binary formalism. Explicitly, if the ith row of $\mathbf{H}$ is denoted as $\mathbf{H}_i = (\mathbf{H}_{z_i}|\mathbf{H}_{x_i})$ following the notation of Eq. (74), then the commutativity of the stabilizers g_i and $g_{i'}$ is transformed into the symplectic product of rows $\mathbf{H}_i$ and $\mathbf{H}_{i'}$, which is computed as follows:

$$\mathbf{H}_i \star \mathbf{H}_{i'} = (\mathbf{H}_{z_i} \cdot \mathbf{H}_{x_{i'}} + \mathbf{H}_{z_{i'}} \cdot \mathbf{H}_{x_i}) \bmod 2. \tag{79}$$

The resultant symplectic product yields a value of zero, if the number of different non-Identity operators ($\mathbf{X}$, $\mathbf{Y}$ or $\mathbf{Z}$) in the stabilizers g_i and $g_{i'}$ is even; hence, satisfying the commutativity criterion. Furthermore, since all stabilizers must be commutative, the symplectic product must be zero for all rows of $\mathbf{H}$, i.e. the PCM $\mathbf{H}$ should satisfy:

$$\mathbf{H}_z\mathbf{H}_x^T + \mathbf{H}_x\mathbf{H}_z^T = 0 \bmod 2. \tag{80}$$

This in turn implies that any pair of classical binary codes having the PCMs $\mathbf{H}_z$ and $\mathbf{H}_x$ and satisfying the symplectic product of Eq. (80) may be used for constructing a valid QSC.

The symplectic product of Eq. (80) may also be exploited for computing the syndrome of a QSC in the binary domain, for example during the PCM-based syndrome decoding. More specifically, the Pauli-to-binary isomorphism of Eq. (73) transforms an n-qubit Pauli error $\mathcal{P} \in \mathcal{G}_n$ into an effective error vector P of length $2n$. Explicitly, analogous to the $\mathbf{H}$ of Eq. (74), the effective error vector P may be expressed as $P = (P_z|P_x)$, where P_z and P_x denote the Pauli-$\mathbf{Z}$ and Pauli-$\mathbf{X}$ errors, respectively. More precisely, a 1 at the tth index of P_z denotes a Pauli-$\mathbf{Z}$ (phase-flip) error on the tth qubit, while a 1 at the tth index of P_x represents the occurrence of the Pauli-$\mathbf{X}$ (bit-flip) error on the tth qubit. Similarly, the Pauli-$\mathbf{Y}$ (bit-and-phase-flip) error on the tth qubit yields a 1 at the tth index of P_z as well as P_x. Finally, the syndrome of a QSC can be computed in the binary formalism using the symplectic product and the effective error vector P as follows:

$$s = \mathbf{H} \star P^T = \left(\mathbf{H}_z P_x^T + \mathbf{H}_x P_z^T\right) \bmod 2, \tag{81}$$

where the $\mathbf{H}_z$ and $\mathbf{H}_x$ are used for correcting bit-flip and phase-flip errors, respectively, as previously discussed in the context of 3-qubit bit-flip and phase-flip repetition codes. The resultant syndrome has either a value of 0 or 1. Thus, the quantum-domain syndrome processing may be carried out in the binary domain using the PCM $\mathbf{H}$ and the effective error P. This in turn implies that the quantum decoding process is equivalent to the syndrome decoding of the equivalent classical code relying on the PCM $\mathbf{H}$ [146]. However, since quantum codes are degenerate, as discussed in Section V, quantum decoding aims for estimating the most probable error coset, while the classical syndrome decoding estimates the most probable error.

B. *Pauli-to-Quaternary Isomorphism*

Analogous to the Pauli-to-binary isomorphism, the Pauli-to-quaternary isomorphism facilitates the design of quantum codes from the existing classical quaternary codes. Explicitly, the $\mathbf{I}$, $\mathbf{X}$, $\mathbf{Y}$ and $\mathbf{Z}$ Pauli operators may be transformed into the elements of Galois Field GF(4) using the mapping given below:

$$\mathbf{I} \to 0, \quad \mathbf{X} \to 1, \quad \mathbf{Z} \to \omega, \quad \mathbf{Y} \to \overline{\omega}, \tag{82}$$

$+$	0	1	ω	$\overline{\omega}$
0	0	1	ω	$\overline{\omega}$
1	1	0	$\overline{\omega}$	ω
ω	ω	$\overline{\omega}$	0	1
$\overline{\omega}$	$\overline{\omega}$	ω	1	0

TABLE V: GF(4) Addition.

$\times$	0	1	ω	$\overline{\omega}$
0	0	0	0	0
1	0	1	ω	$\overline{\omega}$
ω	0	ω	$\overline{\omega}$	1
$\overline{\omega}$	0	$\overline{\omega}$	1	ω

TABLE VI: GF(4) Multiplication.

where 0, 1, ω and $\overline{\omega}$ are the elements of GF(4). Furthermore, the multiplication operation in the Pauli domain is equivalent to the addition operation in GF(4), while the commutativity (symplectic product) criterion in the Pauli domain is equivalent to the trace[13] inner product [85] in GF(4). The associated additive and multiplicative rules of GF(4) are listed in Table V and Table VI[14], respectively. To elaborate further, multiplying the Pauli operators $\{\mathbf{I}, \mathbf{X}, \mathbf{Z}, \mathbf{Y}\}$ with Pauli-$\mathbf{X}$ is equivalent to adding the GF(4) element 1 (corresponding to Pauli-$\mathbf{X}$) to each element of GF(4), as done in the second column of Table V. On the other hand, the commutative relationship between two GF(4) elements $\hat{A}$ and $\hat{B}$ may be established with the help of the trace inner product as follows[15]:

$$\mathrm{Tr}\langle \hat{A}, \hat{B}\rangle = \mathrm{Tr}(\hat{A} \times \overline{\hat{B}}) = 0, \tag{83}$$

where $\langle , \rangle$ denotes the Hermitian inner product, while $\overline{\hat{B}}$ is the conjugate[16] of $\hat{B}$. Moreover, $\mathrm{Tr}(0) = \mathrm{Tr}(1) = 0$, while $\mathrm{Tr}(\omega) = \mathrm{Tr}(\overline{\omega}) = 1$. Explicitly, both the Hermitian inner product and the trace inner product between the elements of GF(4) are tabulated in Table VII and Table VIII, respectively.

$\langle , \rangle$	0	1	ω	$\overline{\omega}$
0	0	0	0	0
1	0	1	ω	$\overline{\omega}$
ω	0	$\overline{\omega}$	1	ω
$\overline{\omega}$	0	ω	$\overline{\omega}$	1

TABLE VII: GF(4) Hermitian inner product.

$\mathrm{tr}\langle , \rangle$	0	1	ω	$\overline{\omega}$
0	0	0	0	0
1	0	0	1	1
ω	0	1	0	1
$\overline{\omega}$	0	1	1	0

TABLE VIII: GF(4) trace inner product.

If a QSC is characterized by the classical PCM $\hat{\mathbf{H}}$ in the quaternary domain, then the commutativity constraint of the stabilizers g_i and g'_i is transformed into the trace inner product of the ith and i'th row of $\hat{\mathbf{H}}$. Explicitly, this may be formulated as:

$$\hat{\mathbf{H}}_i \star \hat{\mathbf{H}}_{i'} = \mathrm{Tr}\langle \hat{\mathbf{H}}_i, \hat{\mathbf{H}}_{i'}\rangle = \mathrm{Tr}\left(\sum_{t=1}^{n} \hat{\mathbf{H}}_{it} \times \overline{\hat{\mathbf{H}}}_{i't}\right) = 0, \tag{84}$$

where $\hat{\mathbf{H}}_{it}$ is the element in the ith row and tth column of $\hat{\mathbf{H}}$.

Let us now prove the equivalence of Eq. (79) and Eq. (84), since both these equations correspond to the commutativity requirement. Given $\mathbf{H}_i = (\mathbf{H}_{z_i}, \mathbf{H}_{x_i})$ and the mapping of Eq. (82), $\hat{\mathbf{H}}_i$ may be expressed as:

$$\hat{\mathbf{H}}_i = \omega \mathbf{H}_{z_i} + \mathbf{H}_{x_i}. \tag{85}$$

Substituting Eq. (85) into Eq. (84) yields:

$$\begin{aligned}\hat{\mathbf{H}}_i \star \hat{\mathbf{H}}_{i'} &= \mathrm{Tr}\langle(\omega\mathbf{H}_{z_i} + \mathbf{H}_{x_i}), (\omega\mathbf{H}_{z_{i'}} + \mathbf{H}_{x_{i'}})\rangle \\ &= \mathrm{Tr}\left((\omega\mathbf{H}_{z_i} + \mathbf{H}_{x_i})\,(\overline{\omega}\mathbf{H}_{z_{i'}} + \mathbf{H}_{x_{i'}})\right) \\ &= \mathrm{Tr}\left(\mathbf{H}_{z_i}\mathbf{H}_{z_{i'}} + \omega\mathbf{H}_{z_i}\mathbf{H}_{x_{i'}} + \overline{\omega}\mathbf{H}_{x_i}\mathbf{H}_{z_{i'}} + \mathbf{H}_{x_i}\mathbf{H}_{x_{i'}}\right).\end{aligned} \tag{86}$$

Recall that $\mathrm{Tr}(1) = 0$ and $\mathrm{Tr}(\omega) = \mathrm{Tr}(\overline{\omega}) = 1$. Therefore, Eq. (86) reduces to:

$$\hat{\mathbf{H}}_i \star \hat{\mathbf{H}}_{i'} = \mathbf{H}_{z_i}\mathbf{H}_{x_{i'}} + \mathbf{H}_{x_i}\mathbf{H}_{z_{i'}}, \tag{87}$$

which is the same as Eq. (79). Consequently, analogous to Eq. (81), the syndrome in the quaternary domain is computed as:

$$s_i = \mathrm{Tr}(\hat{s}_i) = \mathrm{Tr}\left(\sum_{t=1}^{n} \hat{\mathbf{H}}_{it} \times \overline{\hat{P}}_t\right), \tag{88}$$

where s_i is the syndrome corresponding to the ith row of $\hat{\mathbf{H}}$ and $\hat{P}_t$ is the tth element of $\hat{P}$, which represents the error inflicted on the tth qubit.

Any arbitrary classical quaternary linear code, which is self-orthogonal with respect to the trace inner product of Eq. (84), can be used for constructing a QSC. Since a quaternary linear code is closed under multiplication by the elements of GF(4), this condition reduces to satisfying the Hermitian inner product, rather than the trace inner product [91]. This can be proved as follows.

Let C be a classical linear code in GF(4) having codewords u and v. Furthermore, let us assume that:

$$\langle u, v\rangle = \alpha + \beta\omega. \tag{89}$$

[13] The trace operator of GF(4) maps x onto $(x + \overline{x})$, where $\overline{x}$ denotes the conjugate of x [91].

[14] The addition and multiplication rules for GF(p), having a prime p, are the same as the modulo p addition and multiplication, while the rules for GF(p^m), having $m > 1$, do not follow the conventional rules for modulo p^m addition and multiplication. For example, the addition of the elements of GF(4) is equivalent to the bitwise modulo 2 addition of the equivalent 2-bit patterns. Hence, Table V may be obtained by mapping the 2-bit patterns of Table IV onto the corresponding GF(4) elements.

[15] GF(4) variables are denoted with a ˆ on top, e.g. $\hat{x}$.

[16] The conjugate operation of GF(4) is defined as $\overline{x} = x^2$ [91]. Consequently, conjugation has no impact on the GF(4) elements 0 and 1, while the elements ω and $\overline{\omega}$ are swapped upon taking the conjugate.

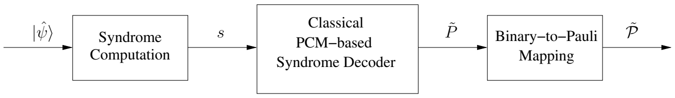


Fig. 20: Syndrome processing block of Fig. 15.

For the sake of satisfying the symplectic product, we must have:

$$\mathrm{Tr}\langle u, v\rangle = 0. \tag{90}$$

Since $\mathrm{Tr}(\omega) = 1$, Eq. (90) is only valid, when β is zero in Eq. (89). Furthermore, since the code C is GF(4)-linear, Eq. (90) leads to:

$$\mathrm{Tr}\langle u, \overline{\omega} v\rangle = 0, \tag{91}$$

which in turn implies that α should also be zero in Eq. (89). Hence, for a classical GF(4)-linear code, the Hermitian inner product of Eq. (89) must be zero, when the trace inner product of Eq. (90) is zero.

To conclude, the stabilizers may be mapped onto the equivalent binary or quaternary representations, as summarized in Table III. These mappings in turn help in designing quantum codes from the existing classical codes, as discussed further in the next section. Furthermore, since a QSC can be mapped onto an equivalent classical binary or quaternary PCM, classical PCM-based syndrome decoding may be invoked during the quantum decoding process. More explicitly, the 'syndrome processing' block of Fig. 15 may be expanded, as shown in Fig. 20. The process begins with the computation of the syndrome of the received sequence $|\hat{\psi}\rangle$ using the stabilizer generators, which collapse to a binary 0 or 1 upon measurement. The binary syndrome sequence s is then fed to a classical PCM-based syndrome decoder, which operates over the equivalent classical PCM associated with the QSC for estimating the equivalent channel error $\tilde{P}$ (or $\tilde{\hat{P}}$ in quaternary domain). The classical PCM-based syndrome decoder of Fig. 20 is exactly the same decoder, which we would use for any conventional classical code, with the exception of the following two differences:

1) In contrast to the syndrome of a classical code, which is the product of the PCM and the transpose of the channel error ($\mathbf{H}P^T$), the syndrome of a quantum code is computed using the symplectic product of Eq. (81) (or the trace inner product of Eq. (88)).
2) The conventional classical decoding aims for estimating the most probable error, given the observed syndrome, while quantum decoding aims for estimating the most probable error coset, which takes into account the degeneracy of quantum codes, as discussed in Section V.

Finally, the binary-to-Pauli mapping of Eq. (73) (or quaternary-to-Pauli mapping of Eq. (82)) is invoked for mapping the estimated binary (or quaternary) error onto the equivalent Pauli error $\tilde{\mathcal{P}}$.

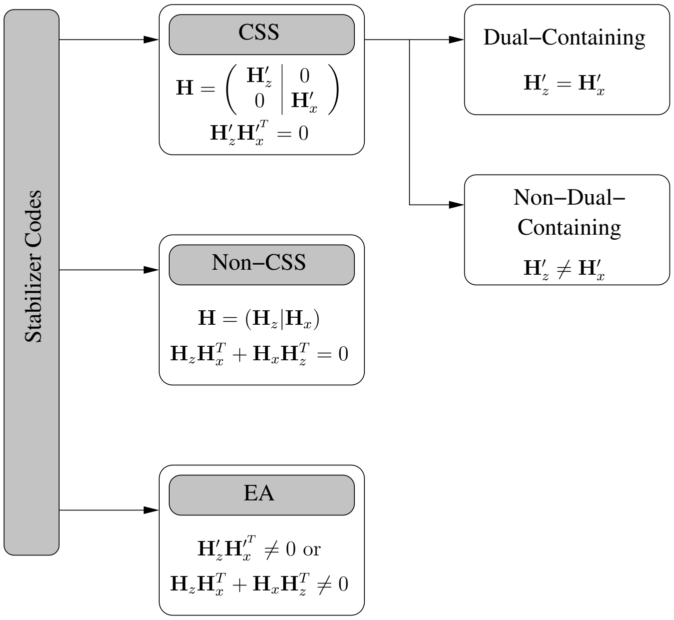

Stabilizer Codes
CSS
$\mathbf{H} = \left(\begin{array}{c|c} \mathbf{H}'_z & 0 \\ 0 & \mathbf{H}'_x \end{array}\right)$
$\mathbf{H}'_z \mathbf{H}'^T_x = 0$
Dual–Containing
$\mathbf{H}'_z = \mathbf{H}'_x$
Non–Dual–Containing
$\mathbf{H}'_z \neq \mathbf{H}'_x$
Non–CSS
$\mathbf{H} = (\mathbf{H}_z|\mathbf{H}_x)$
$\mathbf{H}_z\mathbf{H}_x^T + \mathbf{H}_x\mathbf{H}_z^T = 0$
EA
$\mathbf{H}'_z \mathbf{H}'^T_x \neq 0$ or
$\mathbf{H}_z\mathbf{H}_x^T + \mathbf{H}_x\mathbf{H}_z^T \neq 0$

Fig. 21: Taxonomy of Stabilizer Codes *(CSS: Calderbank-Shor-Steane, EA: Entanglement-Assisted).*

VII. Taxonomy of Stabilizer Codes

The quantum-to-classical isomorphism of Section VI provides a solid theoretical framework for building quantum codes from the known classical codes, which have already found their way into commercial applications. Particularly, quantum codes can be designed from a pair of arbitrary classical binary codes, if they meet the symplectic criterion, or from arbitrary classical quaternary codes, if they satisfy the Hermitian inner product. Continuing further our discussions, in this section we present the taxonomy of stabilizer codes with the aid of Fig. 21, which is based on the structure of the underlying equivalent classical PCM $\mathbf{H}$.

A. Calderbank-Shor-Steane Codes

Calderbank-Shor-Steane (CSS) codes [79]–[81] is a class of stabilizer codes constructed from a pair of binary classical codes. Specifically, the family of CSS codes may be defined as:

An $[n, k_1 - k_2]$ CSS code can be designed from the binary linear block codes $C_1(n, k_1)$ and $C_2(n, k_2)$, if the code space of C_1 subsumes that of C_2 ($C_2 \subset C_1$). Furthermore, if both C_1 as well as the dual of C_2, i.e. $C_2^{\perp}$, exhibit a minimum Hamming distance of d_{min}, then the resultant CSS code also exhibits a minimum distance of d_{min}; hence, it is capable of concurrently correcting $(d_{min} - 1)/2$ bit-flips as well as $(d_{min} - 1)/2$ phase-flips.

Explicitly, analogous to Shor's code, a CSS code independently corrects bit-flip and phase-flip errors. More specifically, the binary code C_1 is invoked for correcting bit-flips, while the code $C_2^{\perp}$ is used for phase-flip correction. Hence, if $\mathbf{H}'_z$

and $\mathbf{H}_x'$ are the PCMs of C_1 and $C_2^{\perp}$, respectively, then the resultant CSS code has the following PCM:

$$\mathbf{H} = [\mathbf{H}_z|\mathbf{H}_x] = \left(\begin{array}{c|c} \mathbf{H}_z' & \mathbf{0} \\ \mathbf{0} & \mathbf{H}_x' \end{array} \right), \tag{92}$$

where we have $\mathbf{H}_z = \begin{pmatrix} \mathbf{H}_z' \\ \mathbf{0} \end{pmatrix}$, $\mathbf{H}_x = \begin{pmatrix} \mathbf{0} \\ \mathbf{H}_x' \end{pmatrix}$, while $\mathbf{H}_z'$ and $\mathbf{H}_x'$ are $(n-k_1) \times n$ and $k_2 \times n$ binary matrices, respectively. Furthermore, since $C_2 \subset C_1$, the symplectic condition of Eq. (80) is reduced to:

$$\mathbf{H}_z'\mathbf{H}_x'^{T} = 0. \tag{93}$$

Hence, the process of designing a QSC is reduced to finding a pair of binary codes whose PCMs conform to the symplectic criterion of Eq. (93). Since the resultant PCM of Eq. (92) has $(n-k_1+k_2)$ rows, the quantum code encodes (k_1-k_2) information qubits into n qubits. Moreover, if we have $\mathbf{H}_z' = \mathbf{H}_x'$, then the resultant code is called a dual-containing (or self-orthogonal) code having $\mathbf{H}_z{}'\mathbf{H}_z'^{T} = 0$, which is equivalent to $C_1^{\perp} \subset C_1$. Explicitly, in case of dual-containing CSS codes, $C_2(n,k_2)$ is the dual code of $C_1(n,k_1)$. Therefore, we have $k_2 = (n-k_1)$ and the resultant dual-containing CSS codes encodes $(k_1-k_2) = (2k_1-n)$ qubits into n coded qubits. We classify the remaining CSS constructions, having $\mathbf{H}_z' \neq \mathbf{H}_x'$, as non-dual-containing CSS codes.

An $[n, k_1-k_2]$ CSS code, relying on the binary codes C_1 and $C_2^{\perp}$, is implemented by finding the unique cosets[17] of C_2 in C_1, so that each of the $2^{k_1-k_2}$ superimposed state can be mapped onto a unique coset of C_2 in C_1. These unique cosets are in turn derived by adding (bit-wise modulo-2) each codeword of C_1 to the code space of C_2. More specifically, if $x_1 \in C_1$ and $x_2 \in C_2$, then the normalized addition operation can be formulated as:

$$|x_1 + C_2\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{x_2 \in C_2} |x_1 + x_2\rangle. \tag{94}$$

Since the cardinality of C_1 is $|C_1| = 2^{k_1}$, while that of C_2 is $|C_2| = 2^{k_2}$, we get $|C_1|/|C_2| = 2^{k_1-k_2}$ unique cosets of C_2 in C_1. Consequently, each of the $2^{k_1-k_2}$ (k_1-k_2)-qubit orthogonal quantum state can be mapped onto a superposition of the codewords of the unique coset.

Coset 1	Coset 2
0000000	1111111
0111001	1000110
1011010	0100101
1100011	0011100
1101100	0010011
1010101	0101010
0110110	1001001
0001111	1110000

TABLE IX: Unique cosets of $C_1^{\perp}$ in C_1.

Let us now consider the construction of Steane's $[7,1]$ code, which is derived from the dual-containing classical $(7,4)$ Hamming code having the PCM:

$$\mathbf{H} = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}. \tag{95}$$

The PCM $\mathbf{H}$ of Eq. (95) yields $\mathbf{H}\mathbf{H}^T = 0$, hence lending itself to constructing a dual-containing CSS code. More specifically, C_1 is the $(7,4)$ Hamming code, while C_2 is its dual code, i.e. $C_2 = C_1^{\perp}$, having the parameters $(7,3)$. Since $\mathbf{H}\mathbf{H}^T = 0$, the code space of C_2 is contained in that of C_1, i.e. we have $C_2 \subset C_1$. Furthermore, both C_1 and $C_2^{\perp} = C_1$ can correct a single error. Consequently, a single-error correcting CSS code can be constructed by finding the unique cosets of $C_1^{\perp}$ in C_1 using Eq. (94). This results in two unique cosets, which are listed in Table IX. These two cosets together yield the code space of the $(7,4)$ Hamming code. The two orthogonal states $|0\rangle$ and $|1\rangle$ of the single qubit information word are hence encoded as follows:

$$\begin{aligned} |\bar{0}\rangle \equiv \frac{1}{\sqrt{8}}(&|0000000\rangle + |0111001\rangle + |1011010\rangle + |1100011\rangle \\ &+ |1101100\rangle + |1010101\rangle + |0110110\rangle + |0001111\rangle), \\ |\bar{1}\rangle \equiv \frac{1}{\sqrt{8}}(&|1111111\rangle + |1000110\rangle + |0100101\rangle + |0011100\rangle \\ &+ |0010011\rangle + |0101010\rangle + |1001001\rangle + |1110000\rangle). \end{aligned} \tag{96}$$

In other words, $|\bar{0}\rangle$ and $|\bar{1}\rangle$ are the equally weighted superpositions of all the codewords of the two cosets of Table IX. Furthermore, $\mathbf{H}_z'$ and $\mathbf{H}_x'$ of the resultant quantum code space are equivalent to the binary PCM of the Hamming code (Eq. (95)). Hence, the associated bit-flip and phase-flip detecting stabilizers of the $[7,1]$ Steane's code are as follows:

$$\begin{aligned} g_1 &= \mathbf{ZZIZZII} \\ g_2 &= \mathbf{ZIZZIZI} \\ g_3 &= \mathbf{IZZZIIZ} \\ g_4 &= \mathbf{XXIXXII} \\ g_5 &= \mathbf{XIXXIXI} \\ g_6 &= \mathbf{IXXXIIX}. \end{aligned} \tag{97}$$

We may observe in Eq. (97) as well as in Eq. (92) that the bit-flip and phase-flip detecting stabilizers (or equivalently syndromes) of a CSS-type quantum code are independent. Therefore, bit-flip and phase-flip estimation may be carried out independently by two separate classical syndrome decoders

[17] Assume $C_1 = (0,1,2,3)$ with $k_1 = 2$ and $C_2 = (0,2)$ with $k_2 = 1$, *modulo* 4 addition yields following cosets:

$$\begin{aligned} 0 + C_2 &\equiv (0,2) = C_2, \\ 1 + C_2 &\equiv (1,3) = 1 + C_2, \\ 2 + C_2 &\equiv (2,0) = C_2, \\ 3 + C_2 &\equiv (3,1) = 1 + C_2. \end{aligned}$$

Hence, resulting in two different cosets of C_2 in C_1 i.e. $(0,2)$ and $(1,3)$. Equivalently, we may say that the two unique cosets $(0,2)$ and $(1,3)$ of C_2 together constitute the code space of C_1.

using $\mathbf{H}'_z$ and $\mathbf{H}'_x$, respectively, as illustrated in Fig. 22. Furthermore, when the simplified decoder of Fig. 22 is invoked, the performance of CSS codes observed in the face of the depolarizing channel of Eq. (22) is isomorphic to their performance over two independent phase-flip and bit-flip channels, where each has a marginalized depolarizing probability of $2p/3$. Hence, the QBER performance of CSS codes may be approximated by adding together the BERs of the constituent binary codes. More explicitly, given that p_e^x and p_e^z are the classical BERs for $\mathbf{H}'_z$ and $\mathbf{H}'_x$, respectively, the resultant CSS code exhibits a QBER of:

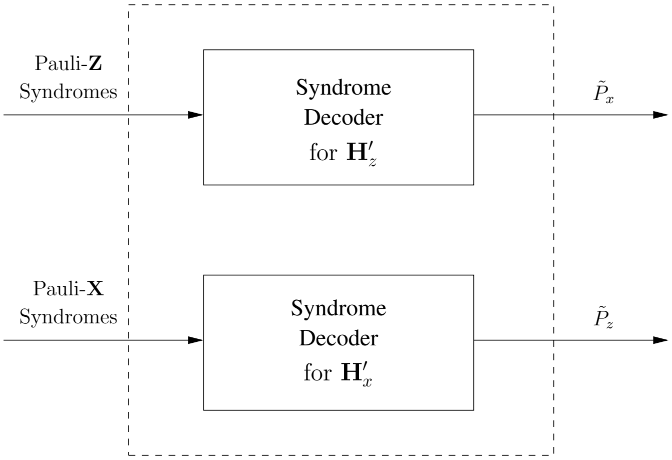

Pauli-**Z**
Syndromes
Syndrome Decoder for $\mathbf{H}'_z$
$\tilde{P}_x$
Pauli-**X**
Syndromes
Syndrome Decoder for $\mathbf{H}'_x$
$\tilde{P}_z$

Fig. 22: Syndrome decoder for CSS-type Quantum Codes.

$$\text{QBER} = p_e^x + p_e^z - p_e^x p_e^z \approx p_e^x + p_e^z, \tag{98}$$

which is equivalent to $2p_e^z$ for a dual-containing CSS code having $\mathbf{H}'_x = \mathbf{H}'_z$.

B. Non-CSS Codes

We observed in the previous section that CSS codes independently correct bit-flip and phase-flip errors. This in turn results in a low coding rate. By contrast, non-CSS stabilizer codes are capable of exploiting the redundancy more efficiently, since they jointly correct bit-flip and phase-flip errors. The PCM of a non-CSS code assumes the general structure of Eq. (74). Consequently, a pair of binary PCMs conforming to the symplectic product criterion of Eq. (80) or a classical quaternary PCM satisfying the trace inner product of Eq. (84) may be used for designing a non-CSS stabilizer code.

Calderbank, Rains, Shor and Sloane conceived a special class of non-CSS codes, called Calderbank-Rains-Shor-Sloane (CRSS) codes, which are constructed from the known classical quaternary codes as follows [91]:

An [n,k] QSC can be designed in the quaternary domain from a classical self-orthogonal (under the Hermitian inner product) GF(4)-linear block code $C(n,(n-k)/2)$. Furthermore, if the dual (also called orthogonal) code $C^{\perp}(n,(n+k)/2)$ exhibits a minimum Hamming distance of d_{min}, then the resultant non-CSS code also exhibits a minimum distance of d_{min}; hence, it is capable of concurrently correcting $(d_{min}-1)/2$ bit-flips as well as $(d_{min}-1)/2$ phase-flips.

Based on this formalism, the PCM of the resultant CRSS code is characterized as:

$$\hat{\mathbf{H}} = \begin{pmatrix} \hat{\mathbf{H}}_c \\ \omega\hat{\mathbf{H}}_c \end{pmatrix}, \tag{99}$$

where $\hat{\mathbf{H}}_c$ is the PCM of the dual code $C^{\perp}(n,(n+k)/2)$. For example, there exists a classical self-orthogonal GF(4)-linear code $C(5,2)$, whose dual code $C^{\perp}(5,3)$ is a Hamming code having the PCM $\hat{\mathbf{H}}_c$ given by [151]:

$$\hat{\mathbf{H}}_c = \begin{pmatrix} 0 & \overline{\omega} & \omega & \omega & \overline{\omega} \\ \overline{\omega} & 0 & \overline{\omega} & \omega & \omega \end{pmatrix}. \tag{100}$$

Consequently, the $(5,1)$ quantum Hamming code can be constructed as:

$$\hat{\mathbf{H}} = \begin{pmatrix} 0 & \overline{\omega} & \omega & \omega & \overline{\omega} \\ \overline{\omega} & 0 & \overline{\omega} & \omega & \omega \\ 0 & 1 & \overline{\omega} & \overline{\omega} & 1 \\ 1 & 0 & 1 & \overline{\omega} & \overline{\omega} \end{pmatrix}. \tag{101}$$

Using the Pauli-to-GF(4) mapping of Eq. (82), the PCM $\hat{\mathbf{H}}$ of Eq. (101) is mapped onto the stabilizer generators listed below:

$$\begin{aligned} g_1 &= \mathbf{IYZZY} \\ g_2 &= \mathbf{YIYZZ} \\ g_3 &= \mathbf{IXYYX} \\ g_4 &= \mathbf{XIXYY}. \end{aligned} \tag{102}$$

Hence, while a single-error correcting CSS-type code has a coding rate of $1/7$, a single-error correcting non-CSS code exhibits an improved coding rate of $1/5$. The resultant codes may be decoded by invoking a classical non-binary syndrome decoder or a binary syndrome decoder operating over the binary PCM of Eq. (74), which exploit the correlation between the bit-flip and phase-flip errors, hence facilitating the joint decoding of bit-flip and phase-flip errors. This in turn provides enhanced decoding performance, albeit at the cost of an increased decoding complexity.

C. Entanglement-Assisted Codes

Let us recall that QSCs may be constructed from the classical binary and quaternary codes only if the constituent classical codes conform to the symplectic criterion of Eq. (80). Consequently, while every QSC may have a classical counterpart, we cannot claim that every classical code has a stabilizer-based quantum version. Furthermore, the stringent symplectic criterion may result in various design issues, such as the unavoidable short cycles in QLDPC codes and the non-recursive nature of non-catastrophic QCCs. For the sake of overcoming these limitations, the entanglement-assisted stabilizer formalism of [105], [108] was conceived, which relies on entangled qubits pre-shared with the receiver over a noiseless channel. Explicitly, the EA formalism helps in transforming a set of non-commuting Pauli generators into a set of commuting generators, which in turn constitute valid stabilizer codes. Consequently, when the underlying classical codes do not satisfy the symplectic criterion, the EA formalism is invoked for making the resultant stabilizers commutative.

Fig. 23 shows the system model of a quantum communication system relying on an Entanglement-Assisted Quantum Stabilizer Code (EA-QSC). Explicitly, an $[n, k, c]$ EA-QSC encodes a k-qubit information word $|\psi\rangle$ into an n-qubit codeword $|\overline{\psi}\rangle$ with the help of $(n-k-c)$ auxiliary qubits in state $|0\rangle$ and c pre-shared entangled qubits (ebits). Explicitly, ebits may be created in the Bell state $|\phi^+\rangle$, expressed as:

$$|\phi^+\rangle = \frac{|00\rangle^{T_X R_X} + |11\rangle^{T_X R_X}}{\sqrt{2}}, \tag{103}$$

so that the first qubit is retained at the transmitter, while the associated entangled qubit is sent to the receiver before actual transmission commences, for example during off-peak hours, when the channels are under-utilized. The notations T_X and R_X in Eq. (103) are used to identify the transmitter's and receiver's half of the ebit, respectively. It is generally assumed that the pre-sharing of ebits takes place over a noiseless channel. Furthermore, as illustrated in Fig. 23, the transmitter only utilizes the transmitter's half of the ebits for encoding the information word $|\psi\rangle$ into the codeword $|\overline{\psi}\rangle$. Finally, the encoded information is sent over a noisy quantum channel. At the receiver, the received noisy codeword $|\hat{\overline{\psi}}\rangle$ is combined with the receiver's half of the c ebits during the decoding process. Specifically, the stabilizers of an EA-QSC jointly act on $|\hat{\overline{\psi}}\rangle$ and the receiver's ebits for computing the syndrome vector, which is then fed to a classical syndrome decoder for estimating the error pattern $\tilde{\mathcal{P}}$, as previously shown in Fig. 20. The rest of the processing at the receiver is identical to that of the unassisted QSC of Fig. 15.

The Bell state of Eq. (103) has unique properties, which facilitate the mapping of a set of non-commuting generators into a set of commuting generators. More explicitly, the 2-qubit commuting generators $\mathbf{X}^{T_X}\mathbf{X}^{R_X}$ and $\mathbf{Z}^{T_X}\mathbf{Z}^{R_X}$ stabilize the state $|\phi^+\rangle$, i.e. we have:

$$[\mathbf{X}^{T_X}\mathbf{X}^{R_X}, \mathbf{Z}^{T_X}\mathbf{Z}^{R_X}] = 0. \tag{104}$$

However, the Pauli operators acting on the individual qubits anti-commute with each other, i.e. we have:

$$\begin{aligned}[\mathbf{X}^{T_X}, \mathbf{Z}^{T_X}] &\neq 0,\\ [\mathbf{X}^{R_X}, \mathbf{Z}^{R_X}] &\neq 0.\end{aligned} \tag{105}$$

Therefore, if we have a pair of non-commutative generators $\mathbf{X}^{T_X}$ and $\mathbf{Z}^{T_X}$, which only act on the transmitter's ebit, then these generators can be transformed into a pair of commuting generators by appropriately augmenting them with an additional operator acting on the receiver's ebit. Explicitly, the operator acting on the receiver's ebits is specifically chosen for ensuring that the resultant 2-qubit generators have an even number of indices, which have different non-identity operators; hence, resolving the anti-commutativity of the initial single qubit operators.

Let us now construct an EA-QSC from two binary codes having the PCMs[18]:

$$\mathbf{H}_z = \begin{pmatrix} 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 0\\ 1 & 1 & 1 & 0\\ 0 & 1 & 1 & 1 \end{pmatrix}, \tag{106}$$

and:

$$\mathbf{H}_x = \begin{pmatrix} 1 & 0 & 1 & 0\\ 1 & 1 & 0 & 1\\ 1 & 0 & 0 & 1\\ 1 & 1 & 1 & 0 \end{pmatrix}. \tag{107}$$

The PCMs $\mathbf{H}_z$ and $\mathbf{H}_x$ may be concatenated for constructing a non-CSS code having:

$$\mathbf{H} = \left(\begin{array}{cccc|cccc} 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0\\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1\\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1\\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \end{array}\right). \tag{108}$$

Unfortunately, the PCM of Eq. (108) does not meet the symplectic product criterion of Eq. (80). Furthermore, the PCM $\mathbf{H}$ may be transformed into the following non-commutative Pauli generators using the Pauli-to-binary mapping of Eq. (73):

$$\mathbf{H}_Q = \begin{pmatrix} \mathbf{X} & \mathbf{Z} & \mathbf{X} & \mathbf{I}\\ \mathbf{X} & \mathbf{X} & \mathbf{I} & \mathbf{X}\\ \mathbf{Y} & \mathbf{Z} & \mathbf{Z} & \mathbf{X}\\ \mathbf{X} & \mathbf{Y} & \mathbf{Y} & \mathbf{Z} \end{pmatrix}. \tag{109}$$

Explicitly, the first two generators (or rows) of $\mathbf{H}_Q$ anti-commute, while all other generators (or rows) commute with each other. This is because the first two generators have a single index having different non-Identity operators. In other words, only the operators acting on the second qubit anti-commute, while the operators individually acting on all other qubits commute. For the sake of making the generators of Eq. (109) commutative, the first two rows of $\mathbf{H}_Q$ may be augmented with a pair of anti-commuting operators, as shown below:

$$\mathbf{H}_Q = \left(\begin{array}{cccc|c} \mathbf{X} & \mathbf{Z} & \mathbf{X} & \mathbf{I} & \mathbf{Z}\\ \mathbf{X} & \mathbf{X} & \mathbf{I} & \mathbf{X} & \mathbf{X}\\ \mathbf{Y} & \mathbf{Z} & \mathbf{Z} & \mathbf{X} & \mathbf{I}\\ \mathbf{X} & \mathbf{Y} & \mathbf{Y} & \mathbf{Z} & \mathbf{I} \end{array}\right), \tag{110}$$

where the operators to the left of the vertical bar $(|)$ act on the n-qubit transmitted codewords, while those on the right of the vertical bar act on the receiver's half of the ebits. Hence, only a single ebit is required in this design example.

VIII. Design Examples

We may conclude from the above discussions that the stabilizer formalism is a useful framework for exploiting the known classical coding families. In this section, we extend our discussions to the two widely used channel coding families, i.e. the BCH codes (Section VIII-A) and the convolutional codes (Section VIII-B), emphasizing the duality between their classical and quantum versions.

[18] This is an arbitrary, random example only conceived for illustrating the construction of EA codes from the known classical codes. The associated classical/quantum code may not have good error correction capabilities.

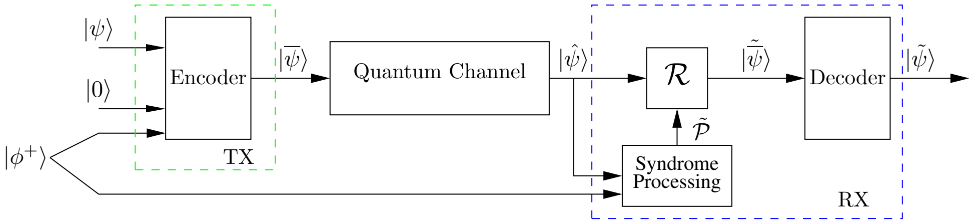


Fig. 23: System Model: Quantum communication system relying on an entanglement-assisted quantum stabilizer code

.

A. *Bose-Chaudhuri-Hocquenghem Codes*

1) Classical Bose-Chaudhuri-Hocquenghem Codes [134]: Bose-Chaudhuri-Hocquenghem (BCH) codes are classified as maximum minimum-distance multiple-error correcting cyclic block codes. A classical BCH code denoted as BCH(n, k, d_{min}) encodes $k \geq (n - mt)$ information bits into n-bit codewords, where $n = 2^m - 1$, so that the resultant code space has an odd minimum Hamming distance of d_{min}, hence it is capable of correcting $t = (d_{\text{min}} - 1)/2$ errors. Furthermore, BCH codes can be both systematic as well as non-systematic. However, systematic BCH codes are known to outperform their non-systematic counterparts [134]. This is because they can exploit their error-detection capability for disabling the decoding operations, when this would result in correcting the wrong symbols owing to having more than t errors. In such instances, the systematic BCH decoder simply retains the systematic part of the codeword. Unfortunately, the non-systematic decoder does not have separate information and parity segments, hence it would correct the wrong symbols, when it is overloaded by more than t errors. This causes even more errors after decoding than we had at the channel's output.

A systematic binary BCH code encodes k information bits into n coded bits by appending $(n - k)$ parity bits to the block of k information bits. The parity bits are computed from the information bits based on the generator polynomial $g(x)$, which is given by:

$$g(x) = g_0 + g_1 x + g_2 x^2 + \cdots + g_{n-k} x^{n-k}. \tag{111}$$

As detailed in [134], [154], the systematic encoder operates by first shifting the information polynomial $d(x)$ to the highest order position of the codeword $c(x)$ by multiplying $d(x)$ with $x^{(n-k)}$ and then attaching the parity segment to it. Explicitly, the parity symbols denoted by the polynomial $p(x)$ are defined according to the generator polynomial $g(x)$, so that the resulting codeword $c(x)$ is a valid codeword. The overall systematic encoding process may be summarized as:

$$c(x) = x^{(n-k)}.d(x) + p(x), \tag{112}$$

where $p(x)$ is defined as:

$$p(x) = -\text{Rem}\left[\frac{x^{(n-k)}.d(x)}{g(x)}\right], \tag{113}$$

for the sake of ensuring that $c(x)$ constitutes a valid codeword, hence yielding a zero-valued remainder upon division by the generator polynomial $g(x)$, i.e. we have:

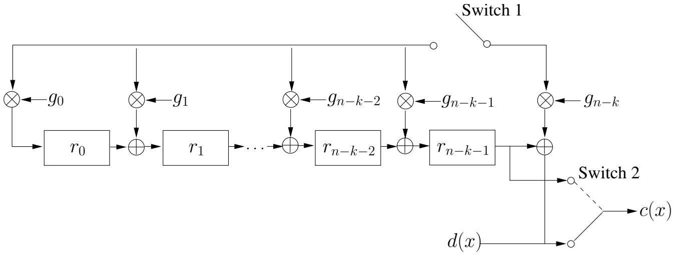


Fig. 24: Schematic of the systematic BCH(n, k, d_{min}) encoder.

$$\begin{aligned}\text{Rem}\left[\frac{c(x)}{g(x)}\right] &= \text{Rem}\left[\frac{x^{(n-k)}.d(x) + p(x)}{g(x)}\right] \\ &= \text{Rem}\left[\frac{x^{(n-k)}.d(x)}{g(x)}\right] + \text{Rem}\left[\frac{p(x)}{g(x)}\right] = 0,\end{aligned} \tag{114}$$

since,

$$\text{Rem}\left[\frac{p(x)}{g(x)}\right] = p(x), \tag{115}$$

according to Eq. (113). The corresponding polynomial multiplications and divisions of Eq. (112) and Eq. (113), respectively, may be carried out by low-complexity shift register based operations, as exemplified below.

The encoder of a systematic BCH code may be implemented using shift registers, as depicted in Fig. 24, where ⊗ denotes the multiplication operation, while ⊕ is the modulo-2 addition. Specifically, the information bits $d(x)$ are encoded into the coded bits $c(x)$ as follows:

1) Switch 1 is closed during the first k time instants (or clock cycles), hence allowing the information bits $d(x)$ to flow into the $(n - k)$ shift registers according to the rules defined by the generator polynomial $g(x)$. Explicitly, the contents of the shift registers after the kth time instant constitute the parity bits.
2) Concurrently, Switch 2 is in the down position, so that the k information bits $d(x)$ constitute the first k bits of $c(x)$.
3) After k time instants, Switch 1 is opened, while Switch 2 is moved to the upper position. This clears the shift

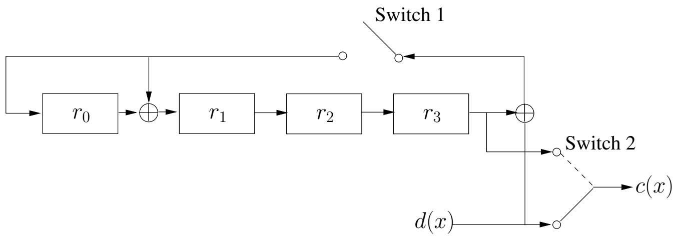


Fig. 25: Encoder of systematic BCH$(15, 11, 3)$.

Index	Input	State $(r_0r_1r_2r_3)$		Output
	Bit	Binary	Decimal	Bit
0	-	0000	0	-
1	1	1100	12	1
2	0	0110	6	0
3	0	0011	3	0
4	0	0001	1	0
5	1	1100	12	1
6	1	1010	10	1
7	1	1001	9	1
8	0	0100	4	0
9	0	0010	2	0
10	1	1101	13	1
11	1	1010	10	1
12	-	0101	5	0
13	-	0010	2	1
14	-	0001	1	0
15	-	0000	0	1

TABLE X: BCH$(15, 11, 3)$ encoding process for d = 11001110001 ($d(x) = 1 + x + x^4 + x^5 + x^6 + x^{10}$), which yields the codeword $c = 101011001110001$ ($c(x) = x^2 + x^4 + x^5 + x^8 + x^9 + x^{10} + x^{14}$).

registers by moving their contents to the output $c(x)$.

Let us consider the BCH$(15, 11, 3)$ code having the generator polynomial[19]:

$$\begin{aligned} g &= 23_{\text{octal}} \\ &= 10011_{\text{bin}}, \\ g(x) &= x^4 + x + 1. \end{aligned} \tag{116}$$

The associated encoding circuit of Fig. 25 can be easily derived from Fig. 24 based on the generator polynomial of Eq. (116). We may observe in Eq. (116) that the coefficients can only have a value of 1 or 0. Consequently, the multiplier is replaced by a direct hard-wire connection, if the corresponding coefficient is 1, while no connection is made, when the coefficient is 0. Let us assume an 11-bit input sequence $d = 11001110001$, which may also be represented as $d(x) = 1 + x + x^4 + x^5 + x^6 + x^{10}$. The encoding process proceeds as follows:

1) The shift registers are initialized to the all-zero state. During the first $k = 11$ time instances, when the Switch 1 is closed, the input bits flow into the shift registers of Fig. 25. The resultant states are tabulated in Table X at each time instant.

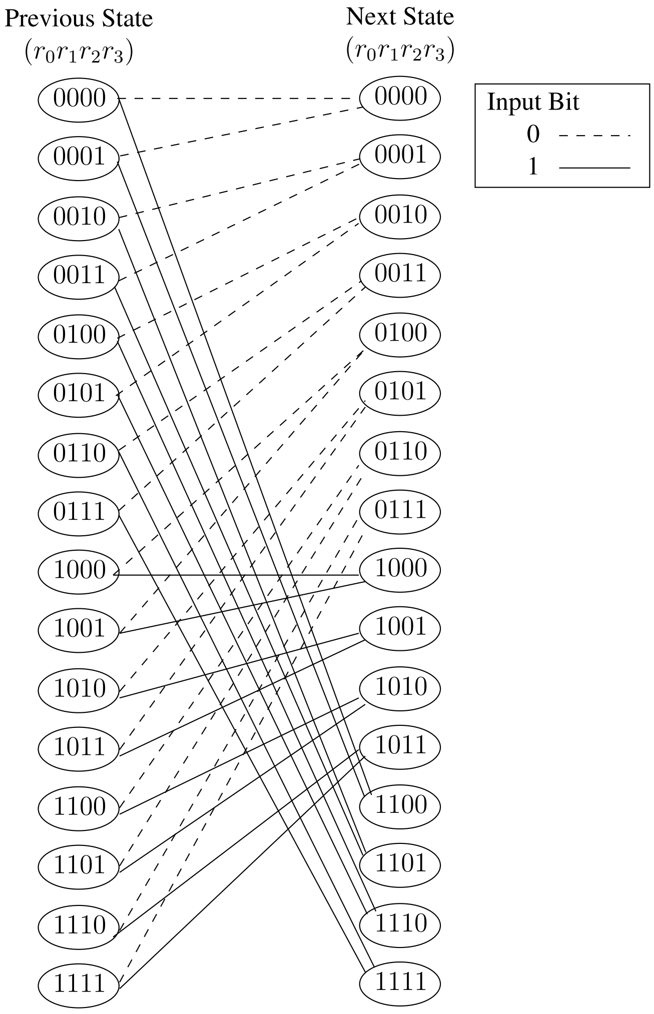


Fig. 26: State transition diagram for BCH$(15, 11, 3)$.

2) Furthermore, since Switch 2 is downward position for the first $k = 11$ time instances, the coded bits of $c(x)$ are the same as the information bits $d(x)$.
3) Thereafter, since Switch 1 is opened and Switch 2 is moved to the upper position, the values within the shift registers represent the coded bits, as demonstrated in Table X. Eventually, the shift registers are returned to the initial all-zero state.

Equivalently, the encoding process of Table X may also be represented by using the state transition diagram of Fig. 26, which shows all possible transitions for the BCH encoder of Fig. 25. In its *conceptually simplest form*, the decoding relies on a simple decoding table, which has a total of $2^{15} = 32768$ entries and $2^{11} = 2048$ legitimate codewords. Since this code has $d_{\text{min}} = 3$, the received corrupted codeword is readily corrected in case of a single error, but the wrong legitimate codeword is selected in case of two errors. The state transition diagram of Fig. 26 also facilitates trellis decoding [62] of

[19] The generator polynomial $g(x)$ is often represented by an octal number, so that when it is converted to the binary notation, the right-most bit constitutes the coefficient of x^0, i.e. the zero-degree coefficient.

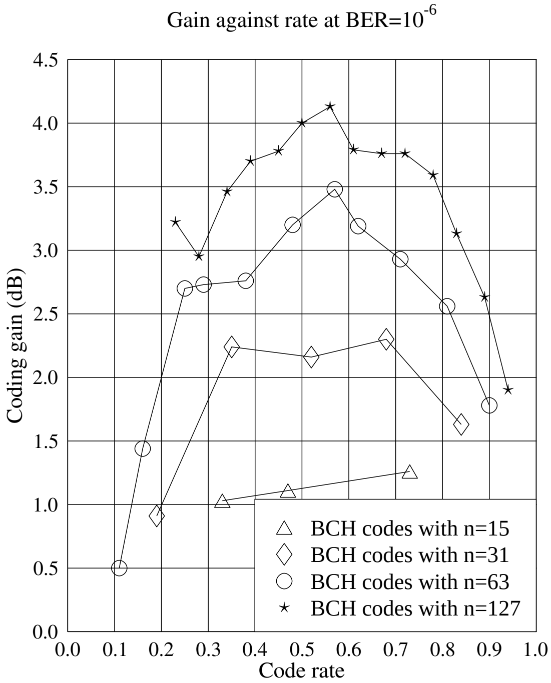


Fig. 27: Coding gain versus coding rate for various families of BCH codes at a BER of 10^{-6} over AWGN channel [134]. *Berlekamp-Massey algorithm was invoked for decoding.*

BCH codes. However, the number of trellis states increases exponentially with $(n-k)$, since the trellis has a total of $2^{(n-k)}$ states. As an alternative strategy, the Berlekamp-Massey algorithm [53]–[56] and Chase algorithm [60] are widely used for efficiently decoding BCH codes. Fig. 27 portrays the coding gain versus coding rate trend at a BER of 10^{-6} for different-rate BCH codes relying on the same codeword length, i.e. for $n = (15, 31, 63, 127)$. We may observe in Fig. 27 that the coding gain increases upon increasing the coding rate (or equivalently increasing k) until it reaches the maximum value. More specifically, the maximum coding gain is typically achieved when the coding rate is between 0.5 and 0.6.

2) Quantum Bose-Chaudhuri-Hocquenghem Codes: Quantum BCH codes [89]–[94] can be derived from the classical dual-containing binary BCH codes as well as self-orthogonal quaternary BCH codes. In this section, we will detail the construction of a dual-containing BCH code, based on our discussions of Section VII-A.

Let us recall from Section VII-A that if C is the classical code specified by the PCM $\mathbf{H}$ and having the dual code $C^{\perp}$, whose code space is subsumed by that of C ($C^{\perp} \subset C$), then the resultant $[n, k']$ dual-containing CSS code, having $k' = (2k-n)$, maps each of the $2^{k'}$ superimposed states of a k'-qubit information word onto a unique coset of the dual code $C^{\perp}$ in the code space of C. The cosets of $C^{\perp}$ in C may be obtained by adding a legitimate codeword of C to all the codewords of $C^{\perp}$, as previously shown in Eq. (94). However, only those codewords of C generate a unique coset of $C^{\perp}$, which do not differ by an element of $C^{\perp}$. Explicitly, the codewords x_1 and x_1' of C are said to differ by an element of $C^{\perp}$, if their bit-wise modulo-2 addition yields a codeword of $C^{\perp}$, i.e. $x_1 + x_1' = x_2$, where $x_2 \in C^{\perp}$. Consequently, such codewords of C yield the same coset of $C^{\perp}$.

Let us elaborate on this by constructing the single-error correcting QBCH$[15, 7]$ code from the dual-containing classical BCH$(15, 11)$ code of Fig. 25, whose PCM is:

$$\mathbf{H} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}. \tag{117}$$

The encoder of QBCH$[15, 7]$ may be derived using the method conceived by Mackay *et al.* in [146], which proceeds as follows:

1) The classical dual-containing PCM $\mathbf{H}$ is first transformed into the matrix $\tilde{\mathbf{H}} = [\mathbf{I}_{(n-k)}|\mathbf{P}]$ using elementary row operations as well as column permutations. Explicitly, the elementary row operations include row permutations and addition of one row to the other. Since $\mathbf{H}$ is an $(n-k) \times n$ matrix, the resultant matrix $\mathbf{I}_{(n-k)}$ has dimensions $(n-k) \times (n-k)$, while $\mathbf{P}$ is an $(n-k) \times k$ binary matrix. For the PCM $\mathbf{H}$ of Eq. (117), we have $\tilde{\mathbf{H}} = \mathbf{H}$.
2) As a next step, apply row operations to $\mathbf{P}$ so that it is reduced to $\tilde{\mathbf{P}} = [\mathbf{I}_{(n-k)}, \mathbf{Q}]$, where $\mathbf{Q}$ is an $(n-k) \times k'$ binary matrix. Therefore, we get

$$\tilde{\mathbf{P}} = \left(\begin{array}{cccc|ccccccc} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \end{array}\right). \tag{118}$$

3) The associated encoder may be implemented in two steps, as shown in Fig. 28. In the first step, the matrix $\mathbf{Q}$ acts on the second block of $(n-k) = 4$ auxiliary (or parity) qubits controlled by the last $k' = (2k-n) = 7$ information qubits, which constitute the information word. More explicitly, a Controlled NOT (CNOT) gate acts on the ith qubit of the second block of $(n-k)$ qubits, which is controlled by the jth information qubit, if $Q_{ij} = 1$. This may be formulated as follows

$$|0\rangle^{\otimes(n-k)}|0\rangle^{\otimes(n-k)}|q\rangle \rightarrow |0\rangle^{\otimes(n-k)}|\mathbf{Q}q\rangle|q\rangle. \tag{119}$$

The resultant states constitute the set of codewords in $\mathcal{C}$, which do not differ by any element of $\mathcal{C}^{\perp}$ and therefore are capable of generating unique cosets of $\mathcal{C}^{\perp}$.

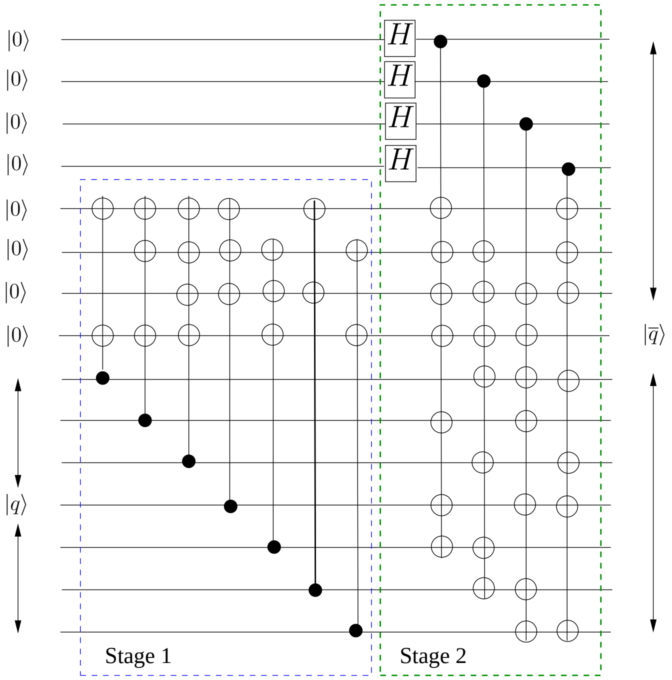


Fig. 28: Encoder of QBCH$[15, 7]$ [155].

TABLE XI: Stabilizers of the QBCH$[15, 7]$.

	Stabilizer
g_1	**ZIIIZZZZIZIZZII**
g_2	**IZIIIZZZZIZIZZI**
g_3	**IIZIIIZZZZIZIZZ**
g_4	**IIIZZZZIZIZZIIZ**
g_5	**XIIIXXXXIXIXXII**
g_6	**IXIIIXXXXIXIXXI**
g_7	**IIXIIIXXXXIXIXX**
g_8	**IIIXXXXIXIXXIIX**

4) The second stage adds the codewords of $\mathcal{C}^{\perp}$ to the codewords of $\mathcal{C}$ generated in the previous step. More specifically, the second stage on its own generates the code space of $\mathcal{C}^{\perp}$ according to the PCM $\tilde{\mathbf{H}}$. For a classical code $\mathcal{C}^{\perp}$, the first $(n-k)$ bits are the systematic information bits, which can have either the value of 0 or 1. Consequently, the first $(n-k) = 4$ auxiliary qubits undergo a Hadamard transformation for the sake of generating the complete code space of the classical code $\mathcal{C}^{\perp}$. Finally, the matrix $\mathbf{P}$ acts on the last k qubits controlled by the first $(n-k)$ qubits, hence generating the code space of $\mathcal{C}^{\perp}$. More explicitly, a CNOT gate acts on the jth qubit, which is controlled by the ith qubit, if $P_{ij} = 1$.

The stabilizers of the QBCH$[15, 7]$ code are constructed using the PCM of Eq. (117) by replacing the 1's with $\mathbf{Z}$ (or $\mathbf{X}$), while the 0's are replaced with $\mathbf{I}$. The resultant stabilizer generators are listed in Table XI. Furthermore, due to the cyclic nature of BCH codes, both the encoder of Fig. 28 as well as the stabilizer generators of Table XI can be implemented using quantum shift registers[20], which in turn makes the QBCH codes suitable for systems having cyclic symmetries, for example circular ion traps [156]. The binary syndrome values obtained by applying the stabilizers of Table XI are then fed to a classical Berlekamp-Massey decoder, which estimates the most likely error.

B. *Convolutional Codes*

1) Classical Convolutional Codes: Recall that an (n, k) block code encodes each block of k information bits independently into n coded bits. By contrast, an (n, k, m) convolutional code exemplified in Fig. 29 encodes the entire information sequence into a single coded sequence. More specifically, each k-bit input is encoded into n bits, so that the encoded output at each time instant also depends on the k information bits received in the m previous time instances. The resultant convolutional code has a memory of m, or equivalently a constraint length of $(m + 1)$, which is implemented using linear shift registers. Furthermore, the code is specified by n generator polynomials, which define the topology of modulo-2 gates for generating the required coded sequence. Explicitly, generator polynomials define the connectivity between the current and m previous input sequences, which in turn ensures that the encoded sequence is a legitimate coded sequence.

Let us consider the systematic $(2, 1, 2)$ convolutional code of Fig. 29, which is specified by the following generator polynomials:

$$\begin{aligned} g_0(x) &= 1 \\ g_1(x) &= 1 + x + x^2. \end{aligned} \tag{120}$$

The generator polynomials may also be expressed as a binary vector, where each bit signifies the presence or absence of a link. Consequently, the generator polynomials of Eq. (120) may also be expressed as:

$$\begin{aligned} g_0 &= (100) \\ g_1 &= (111), \end{aligned} \tag{121}$$

which are seen in Fig. 29. We may observe in Eq. (121) that g_0 has a single non-zero entry. This is because of the systematic nature of the code. By contrast, a non-systematic convolutional code would have more than one non-zero term. Consequently, the polynomial g_0 of a non-systematic code would impose more constraints on the encoded sequence, hence resulting in a more powerful code.

Let us consider a 10-bit input sequence $d = 0011011000$, which may also be represented as $d(x) = x^2 + x^3 + x^5 + x^6$. This input sequence is encoded into a 20-bit coded sequence using the encoder of Fig. 29. The associated encoding process is illustrated in Table XII. More explicitly, the shift register is initialized to the all-zero state. With each clock cycle, the state of register r_0 is updated with the incoming information

[20] Please note that implementation of quantum circuits is beyond the scope of this paper.

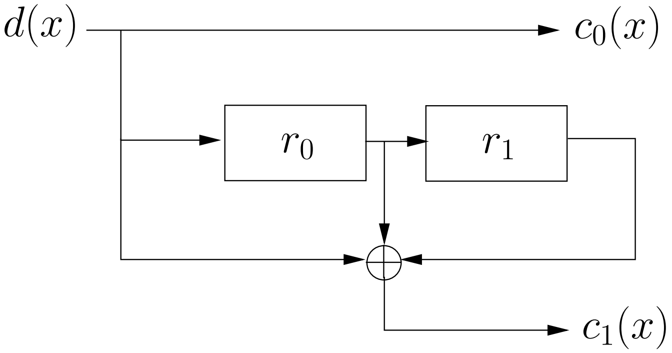


Fig. 29: Schematic of the systematic $(2, 1, 2)$ convolutional encoder.

Index	Input	State (r_0r_1)		Output
	Bit	Binary	Decimal	Bits
0	-	00	0	-
1	0	00	0	00
2	0	00	0	00
3	0	00	0	00
4	1	10	0	11
5	1	11	2	10
6	0	01	3	00
7	1	10	1	10
8	1	11	2	10
9	0	01	3	00
10	0	00	1	01

TABLE XII: Systematic $(2, 1, 2)$ convolutional code encoding process for $d = 0011011000$ ($d(x) = x^2+x^3+x^5+x^6$), which yields the codeword $c = 01001010001011000000$ ($c(x) = x + x^4 + x^6 + x^{10} + x^{12} + x^{13}$).

bit, while its previous value is shifted to the next register r_1. Furthermore, the incoming information bit d_i constitutes the systematic part of the coded bit c, while the output of the modulo-2 adder of Fig. 29 constitutes the parity part.

Analogous to BCH codes, the encoding operation of a convolution code may also be characterized using a state transition diagram, as demonstrated in Fig. 30 for the $(2, 1, 2)$ convolutional code of Fig. 29. Consequently, convolutional codes invoke trellis decoding techniques, for example the Viterbi [59] or MAP [61] algorithm, whose decoding complexity is proportional to the number of trellis states 2^m.

2) Quantum Convolutional Codes: Quantum Convolutional Codes (QCCs) may be designed from the classical convolutional codes by exploiting their semi-infinite block nature. Explicitly, convolutional codes may be represented as linear block codes having a semi-infinite length [157]. This equivalence in turn helps in constructing the stabilizer based counterparts of the known classical codes.

Let us first elaborate on the semi-infinite block structure of convolutional codes using a $(2, 1, m)$ classical convolutional code having the generators:

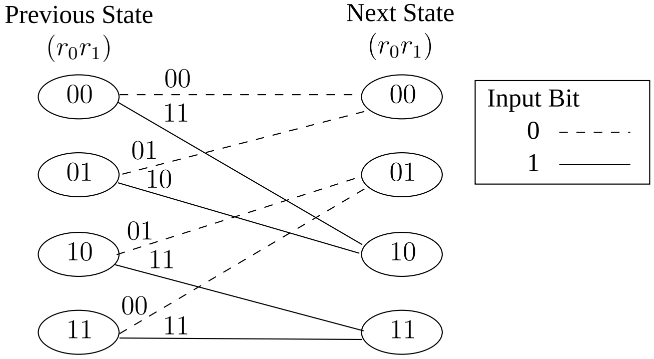


Fig. 30: State transition diagram for systematic $(2, 1, 2)$ convolutional code. *Broken lines indicate legitimate transitions due to a* 0*-valued input, while continuous lines represent a* 1*-valued input. Furthermore, transitions are labeled with the coded bits* (c_0c_1).

$$\begin{aligned} g_0 &= (g_0^{(0)} g_0^{(1)} \ldots g_0^{(m)}) \\ g_1 &= (g_1^{(0)} g_1^{(1)} \ldots g_1^{(m)}). \end{aligned} \tag{122}$$

In essence, the generator polynomials g_0 and g_1 describe the encoder's impulse response functions, which are convolved with the input sequence $[d = (d_0d_1d_2\ldots)]$ to yield the encoded bit sequences $[c_0 = (c_0^{(0)}c_0^{(1)}c_0^{(2)}\ldots)]$ and $[c_1 = (c_1^{(0)}c_1^{(1)}c_1^{(2)}\ldots)]$, respectively. This encoding process can be mathematically encapsulated as:

$$\begin{aligned} c_0 &= d \circledast g_0 \\ c_1 &= d \circledast g_1, \end{aligned} \tag{123}$$

where $\circledast$ represents discrete convolution (modulo 2). The convolution process of Eq. (123) may also be expressed as:

$$c_j^{(l)} = \sum_{i=0}^{m} d_{l-i} g_j^{(i)} = d_l g_j^{(0)} + d_{l-1} g_j^{(1)} + \cdots + d_{l-m} g_j^{(m)}, \tag{124}$$

where $j = 0, 1$, $l \geq 0$ and $u_{l-i} \triangleq 0$ for all $l < i$. Finally, the pair of encoded sequences c_0 and c_1 are multiplexed, yielding a single encoded sequence c as follows:

$$c = (c_0^{(0)} c_1^{(0)} c_0^{(1)} c_1^{(1)} c_0^{(2)} c_1^{(2)} \ldots). \tag{125}$$

The encoding process of Eq. (124) can also be represented in matrix notation as follows:

$$c = d\mathbf{G}, \tag{126}$$

where the generator matrix $\mathbf{G}$ is constructed as follows[21]:

$$\mathbf{G} = \begin{pmatrix} g_{01}^{(0)} & g_{01}^{(1)} & \dots & g_{01}^{(m)} & & & \\ & g_{01}^{(0)} & g_{01}^{(1)} & \dots & g_{01}^{(m)} & & \\ & & g_{01}^{(0)} & g_{01}^{(1)} & \dots & g_{01}^{(m)} & \\ & & & \ddots & & \dots & \ddots \end{pmatrix}, \tag{127}$$

and $g_{01}^{(i)} \triangleq \left(g_0^{(i)} g_1^{(i)}\right)$. The resultant matrix $\mathbf{G}$ of Eq. (127) has a semi-infinite length, since the input sequence d may have an arbitrary length. Furthermore, we may observe that the ith row of $\mathbf{G}$ is obtained by shifting the $(i-1)$th row to the right by $(n = 2)$ places. When d is truncated to have a finite length of N, then the matrix $\mathbf{G}$ of Eq. (127) is of size $(N \times 2(m+N))$. For a more general convolutional code, having the parameters (n, k, m), the generator matrix $\mathbf{G}$ can be expressed as:

$$\mathbf{G} = \begin{pmatrix} \mathbf{G}^{(0)} & \mathbf{G}^{(1)} & \dots & \mathbf{G}^{(m)} & & & \\ & \mathbf{G}^{(0)} & \mathbf{G}^{(1)} & \dots & \mathbf{G}^{(m)} & & \\ & & \mathbf{G}^{(0)} & \mathbf{G}^{(1)} & \dots & \mathbf{G}^{(m)} & \\ & & & \ddots & & \dots & \ddots \end{pmatrix}, \tag{128}$$

where $\mathbf{G}^{(l)}$ is defined as:

$$\mathbf{G}^{(l)} = \begin{pmatrix} g_{1,1}^{(l)} & g_{1,2}^{(l)} & \dots & g_{1,n-1}^{(l)} \\ g_{2,1}^{(l)} & g_{2,2}^{(l)} & \dots & g_{2,n-1}^{(l)} \\ \vdots & \vdots & & \vdots \\ g_{k,1}^{(l)} & g_{k,2}^{(l)} & \dots & g_{k,n-1}^{(l)} \end{pmatrix}. \tag{129}$$

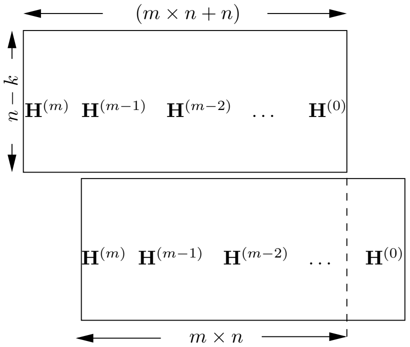
The PCM $\mathbf{H}$ of a convolutional code can also be expressed as a semi-infinite matrix similar to the generator matrix $\mathbf{G}$ of Eq. (128), as shown below:

$$\mathbf{H} = \begin{pmatrix} \mathbf{H}^{(0)} & & & & & \\ \mathbf{H}^{(1)} & \mathbf{H}^{(0)} & & & & \\ \mathbf{H}^{(2)} & \mathbf{H}^{(1)} & \mathbf{H}^{(0)} & & & \\ \vdots & \vdots & \vdots & & & \\ \mathbf{H}^{(m)} & \mathbf{H}^{(m-1)} & \mathbf{H}^{(m-2)} & \dots & \mathbf{H}^{(0)} & \\ & \mathbf{H}^{(m)} & \mathbf{H}^{(m-1)} & \mathbf{H}^{(m-2)} & \dots & \mathbf{H}^{(0)} \\ & & \vdots & \vdots & & \vdots \end{pmatrix}, \tag{130}$$

where $\mathbf{H}^{(l)}$ is a submatrix of size an $((n-k) \times n)$. The PCM $\mathbf{H}$ of Eq. (130) exhibits a block-band structure, which is also illustrated in Fig. 31. More specifically, if each row of submatrices $(\mathbf{H}^{(m)}\mathbf{H}^{(m-1)}\mathbf{H}^{(m-2)} \dots \mathbf{H}^{(0)})$ is viewed as a single block, then $\mathbf{H}$ has a block-band structure, so that each block is a time-shifted version of the previous block and the successive blocks have m overlapping submatrices. This block-band structure, which appears after the first m blocks, may be expressed as:

$$h_{j,i} = [\mathbf{0}^{j \times n}, h_{0,i}], \; 1 \leq i \leq (n-k), \; 0 \leq j, \tag{131}$$

where i denotes the row index within a block, while j is for the block index. Furthermore, $\mathbf{0}^{j \times n}$ is an all-zero row-vector of size $(j \times n)$. In duality to Eq. (131), the stabilizer group $\mathcal{H}$ of an $[n, k, m]$ QCC may be formulated as [149]:



$(m \times n + n)$
$n-k$
$\mathbf{H}^{(m)}$ $\mathbf{H}^{(m-1)}$ $\mathbf{H}^{(m-2)}$ $\dots$ $\mathbf{H}^{(0)}$
$\mathbf{H}^{(m)}$ $\mathbf{H}^{(m-1)}$ $\mathbf{H}^{(m-2)}$ $\dots$ $\mathbf{H}^{(0)}$
$m \times n$

Fig. 31: Semi-infinite classical PCM $\mathbf{H}$ having a block-band structure.

$$\mathcal{H} = sp\{g_{j,i} = I^{\otimes jn} \otimes g_{0,i}\}, \; 1 \leq i \leq (n-k), \; 0 \leq j, \tag{132}$$

where sp denotes a symplectic group.

Let us now design a CSS-type rate-$1/3$ QCC [150], [151] from a classical self-dual rate-$2/3$ binary convolution code having the PCM:

$$\mathbf{H} = \left(\begin{array}{ccc|ccc|ccc|ccc|c} 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & \dots \\ & & & & \dots & & & & & & & & \end{array} \right), \tag{133}$$

and a minimum distance of 3. The corresponding $\mathbf{X}$ and $\mathbf{Z}$ stabilizers of a CSS-type QCC may be obtained by replacing the 1's of Eq. (133) with Pauli $\mathbf{X}$ and $\mathbf{Z}$ operators, respectively. Hence, the stabilizers of the resultant $[3, 1]$ QCC are:

$$g_{0,1} = [\mathbf{XXX}, \mathbf{XII}, \mathbf{XXI}], \tag{134}$$

$$g_{0,2} = [\mathbf{ZZZ}, \mathbf{ZII}, \mathbf{ZZI}], \tag{135}$$

which can correct a single error. The associated stabilizer group $\mathcal{H}$ may be constructed using Eq. (132).

Next, we design a non-CSS, or more precisely CRSS, QCC given by Forney in [150], [151]. It is constructed from the classical rate-$2/3$ quaternary convolutional code having the PCM:

$$\mathbf{H} = \left(\begin{array}{ccc|ccc|ccc|c} 1 & 1 & 1 & 1 & w & \bar{w} & 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & w & \bar{w} & \dots \\ & & & & \dots & & & & & \end{array} \right), \tag{136}$$

which is self-orthogonal. The stabilizers of the corresponding $[3, 1]$ QCC may be constructed using Eq. (99). Explicitly, the stabilizers $g_{0,i}$, for $1 \leq i \leq 2$, are obtained by multiplying the $\mathbf{H}$ of Eq. (136) with the GF(4) elements w and $\bar{w}$, and mapping the resultant GF(4) elements onto the Pauli operators. Hence, the resultant stabilizers are:

$$g_{0,1} = (\mathbf{XXX}, \mathbf{XZY}), \tag{137}$$

$$g_{0,2} = (\mathbf{ZZZ}, \mathbf{ZYX}). \tag{138}$$

[21] Zeros indicate blank spaces in the matrix.

Analogous to other stabilizer codes, the binary syndrome values obtained using the stabilizers of a QCC are fed to a classical syndrome decoder. However, classical convolutional codes generally employ either the Viterbi [59] or the MAP [61] decoding algorithm operating over a code trellis for the sake of estimating the most likely codeword. By contrast, QCCs invoke the syndrome-based error trellis [158]–[162] for estimating the most likely error pattern rather than the most likely codeword. Explicitly, unlike the classic trellis of a convolutional code seen in Fig. 30, which is constructed using the encoding circuit, syndrome-based trellis is constructed using the PCM $\mathbf{H}$ of Eq. (130). Furthermore, the conventional trellis, for example the one obtained using the state transition diagram of Fig. 30, is known as a code trellis, because each path of it is a valid codeword. By contrast, each path of the error trellis is a legitimate error sequence for a given observed syndrome. Therefore, a code trellis is used for codeword decoding, while an error trellis is used for syndrome decoding. However, both trellis representations are equivalent, since every path in the error trellis corresponds to a path in the code trellis. Furthermore, a degenerate Viterbi decoding algorithm was also conceived for QCCs in [126], which takes into account degenerate quantum errors, hence improving the decoding process.

IX. Conclusions & Design Guidelines

QECCs are essential for rectifying the undesirable perturbations resulting from quantum decoherence. Unfortunately, the well-developed classical coding theory, which has evolved over seven decades, cannot be directly applied to the quantum regime. Explicitly, unlike a classical bit, a qubit cannot be copied and it collapses to a classical bit upon measurement. Furthermore, while bit flips are the only type of errors experienced during transmission over a classical channel, a quantum channel may inflict both bit-flips as well as phase-flips. Therefore, it is not feasible to directly map classical codes onto their quantum counterparts. Nevertheless, quantum codes may be designed from the existing classical codes by exploiting the subtle similarities between these two coding regimes. In particular, as detailed in Section II, quantum decoherence may be modeled using the quantum depolarizing channel, which is deemed equivalent to a pair of binary symmetric channels, or more specifically to a classical 4-ary channel. This similarity has helped researchers to develop the quantum versions of the known classical codes, as evident from our survey of Section III. For the sake of providing deeper insights into the transition from classical to quantum coding theory, we started our discussions in Section IV with a simple repetition code, which brought forth three fundamental design principles:

- The copying operation of classical codes is equivalent to quantum entanglement;
- Measurement of a qubit may be circumvented by invoking the classical syndrome decoding techniques;
- Phase-flips may be corrected by using the Hadamard basis.

Based on these design principles, we detailed the stabilizer formalism in Section V, which is in essence the quantum-domain counterpart of classical linear block codes. Since most of the classical codes rely on the basic construction of linear block codes, the stabilizer formalism has helped researchers to build on most of the known families of classical codes. In Section VI, we detailed the equivalence between the quantum and classical parity check matrices, focusing specifically on the Pauli-to-binary isomorphism as well as on the Pauli-to-quaternary isomorphism. The Pauli-to-binary isomorphism helps in designing quantum codes from arbitrary classical binary codes, if they meet the symplectic product criterion, while the Pauli-to-quaternary isomorphism allows us to harness arbitrary classical quaternary codes, if they satisfy the Hermitian inner product. Furthermore, based on this isomorphism, we presented the taxonomy of stabilizer codes in Section VII, namely the dual-containing and non-dual-containing Calderbank-Shor-Steane (CSS) codes non-CSS codes and entanglement-assisted codes, which are summarized in Table XIII. Finally, in Section VIII, we applied our discussions to a pair of popular code families of the classical world, namely the BCH codes and the convolutional codes, for designing their quantum counterparts.

References

[1] P. A. Dirac, *The Principles of Quantum Mechanics*. Oxford University Press, 1982.

[2] M. Born, *The Born-Einstein letters*. Walker, 1971.

[3] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[4] P. W. Shor, “Algorithms for quantum computation: discrete logarithms and factoring,” in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*. Washington, DC, USA: IEEE Computer Society, 1994, pp. 124–134. [Online]. Available: http://portal.acm.org/citation.cfm?id=1398518.1399018

[5] L. K. Grover, “A fast quantum mechanical algorithm for database search,” in *Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing*, ser. STOC ’96. New York, NY, USA: ACM, 1996, pp. 212–219. [Online]. Available: http://doi.acm.org/10.1145/237814.237866

[6] P. Botsinis, D. Alanis, Z. Babar, S. X. Ng, and L. Hanzo, “Noncoherent quantum multiple symbol differential detection for wireless systems,” *IEEE Access*, vol. 3, pp. 569–598, 2015.

[7] P. Botsinis, D. Alanis, Z. Babar, H. V. Nguyen, D. Chandra, S. X. Ng, and L. Hanzo, “Quantum-aided multi-user transmission in non-orthogonal multiple access systems,” *IEEE Access*, vol. 4, pp. 7402–7424, 2016.

[8] D. Alanis, P. Botsinis, Z. Babar, S. X. Ng, and L. Hanzo, “Non-dominated quantum iterative routing optimization for wireless multihop networks,” *IEEE Access*, vol. 3, pp. 1704–1728, 2015.

[9] D. Alanis, J. Hu, P. Botsinis, Z. Babar, S. X. Ng, and L. Hanzo, “Quantum-assisted joint multi-objective routing and load balancing for socially-aware networks,” *IEEE Access*, vol. 4, pp. 9993–10 028, 2016.

[10] T. J. Hastie, R. J. Tibshirani, and J. H. Friedman, *”The Elements of Statistical Learning : Data Mining, Inference, and Prediction”*. Springer, 2009. [Online]. Available: http://opac.inria.fr/record=b1127878

[11] J. Lu, G. Wang, and P. Moulin, “Human Identity and Gender Recognition From Gait Sequences With Arbitrary Walking Directions,” *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 1, pp. 51–61, Jan 2014.

Code Type	Parity Check Matrix	Design Criteria	Design Examples		Decoder
			Classical	Quantum	
Dual-containing CSS	$\left(\begin{array}{c\|c} \mathbf{H}'_z & \mathbf{0} \\ \mathbf{0} & \mathbf{H}'_z \end{array}\right)$	$\mathbf{H}'_z\mathbf{H}'^T_z = 0$	$(7,4)$ Hamming code $(15,11)$ BCH $(3,1,2)$ CC	$[7,1]$ Steane's code (Section VIII-B) $[15,7]$ QBCH code (Section VIII-A) $[3,1,2]$ QCC (Section VIII-B)	Binary
Non-dual-containing CSS	$\left(\begin{array}{c\|c} \mathbf{H}'_z & \mathbf{0} \\ \mathbf{0} & \mathbf{H}'_x \end{array}\right)$	$\mathbf{H}'_z \neq \mathbf{H}'_x$ and $\mathbf{H}'_z\mathbf{H}'^T_x = 0$	$(3,1)$ Repetition code	$[9,1]$Shor's code (Section VI-A)	Binary
Non-CSS	$(\mathbf{H}_z \vert \mathbf{H}_x)$	$\mathbf{H}_z\mathbf{H}_x^T + \mathbf{H}_x\mathbf{H}_z^T = 0$	$(5,3)$ Non-binary Hamming code $(3,1,2)$ Non-binary CC	$[5,1]$ Hamming code (Section VII-B) $[3,1,2]$ QCC (Section VIII-B)	Non-Binary
EA	$\left(\begin{array}{c\|c} \mathbf{H}'_z & \mathbf{0} \\ \mathbf{0} & \mathbf{H}'_z \end{array}\right)$ and $(\mathbf{H}_z \vert \mathbf{H}_x)$	Minimize the number of pre-shared qubits	-	Random EA-QSC (Section VII-C)	Binary & Non-Binary

TABLE XIII: Design guidelines for constructing stabilizer codes.

[12] D. S. Matovski, M. S. Nixon, S. Mahmoodi, and J. N. Carter, "The Effect of Time on Gait Recognition Performance," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 543–552, April 2012.

[13] S. Imre and F. Balazs, *Quantum Computing and Communications: An Engineering Approach*. John Wiley & Sons, 2005.

[14] S. Wiesner, "Conjugate coding," *SIGACT News*, vol. 15, pp. 78–88, January 1983. [Online]. Available: http://doi.acm.org/10.1145/1008908.1008920

[15] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*. New York: IEEE Press, 1984, pp. 175–179.

[16] A. Beige, B.-G. Englert, C. Kurtsiefer, and H. Weinfurter, "Secure communication with single-photon two-qubit states," *Journal of Physics A: Mathematical and General*, vol. 35, no. 28, p. L407, Jul 2002. [Online]. Available: http://stacks.iop.org/0305-4470/35/i=28/a=103

[17] K. Boström and T. Felbinger, "Deterministic secure direct communication using entanglement," *Phys. Rev. Lett.*, vol. 89, p. 187902, Oct 2002. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.89.187902

[18] C. Wang, F.-G. Deng, Y.-S. Li, X.-S. Liu, and G. L. Long, "Quantum secure direct communication with high-dimension quantum superdense coding," *Phys. Rev. A*, vol. 71, p. 044305, Apr 2005. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.71.044305

[19] R. A. Malaney, "Location-dependent communications using quantum entanglement," *Phys. Rev. A*, vol. 81, p. 042319, Apr 2010. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.81.042319

[20] R. Malaney, "The quantum car," *IEEE Wireless Communications Letters*, vol. PP, no. 99, pp. 1–1, 2016.

[21] ——, "Quantum geo-encryption," *arXiv:1604.05022*, Apr. 2016.

[22] H. J. Kimble, "The quantum internet," *Nature*, vol. 453, no. 7198, pp. 1023–1030, June 2008. [Online]. Available: http://dx.doi.org/10.1038/nature07127

[23] L. Jiang, J. M. Taylor, A. S. Sørensen, and M. D. Lukin, "Distributed quantum computation based on small quantum registers," *Phys. Rev. A*, vol. 76, p. 062323, Dec 2007. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.76.062323

[24] C. Monroe, R. Raussendorf, A. Ruthven, K. R. Brown, P. Maunz, L.-M. Duan, and J. Kim, "Large-scale modular quantum-computer architecture with atomic memory and photonic interconnects," *Phys. Rev. A*, vol. 89, p. 022317, Feb 2014. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.89.022317

[25] S. Muralidharan, L. Li, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, "Optimal architectures for long distance quantum communication," *Scientific Reports*, vol. 6, pp. 20 463 EP –, Feb 2016, article. [Online]. Available: http://dx.doi.org/10.1038/srep20463

[26] M. Takeoka, S. Guha, and M. M. Wilde, "Fundamental rate-loss tradeoff for optical quantum key distribution," *Nature Communications*, vol. 5, pp. 5235 EP –, Oct 2014, article. [Online]. Available: http://dx.doi.org/10.1038/ncomms6235

[27] Z. Babar, S. X. Ng, and L. Hanzo, "Near-capacity code design for entanglement-assisted classical communication over quantum depolarizing channels," *IEEE Transactions on Communications*, vol. 61, no. 12, pp. 4801–4807, December 2013.

[28] ——, "EXIT-chart aided code design for symbol-based entanglement-assisted classical communication over quantum channels," in *IEEE Vehicular Technology Conference (VTC Fall)*, Sept 2014, pp. 1–5.

[29] C. H. Bennett, "Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states," *Physical Review Letters*, vol. 69, no. 20, p. 2881, 1992. [Online]. Available: http://dx.doi.org/%7B10.1103/PhysRevLett.69.2881%7D

[30] G. Brassard and L. Salvail, *Secret-Key Reconciliation by Public*

Discussion. Berlin, Heidelberg: Springer Berlin Heidelberg, 1994, pp. 410–423.

[31] W. T. Buttler, S. K. Lamoreaux, J. R. Torgerson, G. H. Nickel, C. H. Donahue, and C. G. Peterson, "Fast, efficient error reconciliation for quantum cryptography," *Phys. Rev. A*, vol. 67, p. 052303, May 2003. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.67.052303

[32] D. G. Cory, M. D. Price, W. Maas, E. Knill, R. Laflamme, W. H. Zurek, T. F. Havel, and S. S. Somaroo, "Experimental quantum error correction," *Phys. Rev. Lett.*, vol. 81, pp. 2152–2155, Sep 1998. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.81.2152

[33] M. D. Reed, L. DiCarlo, S. E. Nigg, L. Sun, L. Frunzio, S. M. Girvin, and R. J. Schoelkopf, "Realization of three-qubit quantum error correction with superconducting circuits," *Nature*, vol. 482, no. 7385, pp. 382–385, Feb. 2012. [Online]. Available: http://dx.doi.org/10.1038/nature10786

[34] G. Arrad, Y. Vinkler, D. Aharonov, and A. Retzker, "Increasing sensing resolution with error correction," *Phys. Rev. Lett.*, vol. 112, p. 150801, Apr 2014. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.112.150801

[35] I. L. Chuang, D. W. Leung, and Y. Yamamoto, "Bosonic quantum codes for amplitude damping," *Phys. Rev. A*, vol. 56, pp. 1114–1125, Aug 1997. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.56.1114

[36] J. Preskill, "Quantum information and computation," *Lecture Notes for Physics 229*, 1998.

[37] J. Ghosh, A. G. Fowler, and M. R. Geller, "Surface code with decoherence: An analysis of three superconducting architectures," *Phys. Rev. A*, vol. 86, p. 062318, Dec 2012. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.86.062318

[38] P. K. Sarvepalli, A. Klappenecker, and M. Rötteler, "Asymmetric quantum codes: constructions, bounds and performance," *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, vol. 465, no. 2105, pp. 1645–1672, 2009. [Online]. Available: http://rspa.royalsocietypublishing.org/content/465/2105/1645

[39] L. M. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang, "Experimental realization of shor's quantum factoring algorithm using nuclear magnetic resonance," *Nature*, vol. 414, no. 6866, pp. 883–887, 2001.

[40] H. V. Nguyen, Z. Babar, D. Alanis, P. Botsinis, D. Chandra, S. X. Ng, and L. Hanzo, "EXIT-chart aided quantum code design improves the normalised throughput of realistic quantum devices," *IEEE Access*, vol. 4, pp. 10 194–10 209, 2016.

[41] C. Shannon, "A mathematical theory of communication, bell system technical journal 27: 379-423 and 623–656," *Mathematical Reviews (MathSciNet): MR10, 133e*, 1948.

[42] R. W. Hamming, "Error detecting and error correcting codes," *Bell Labs Technical Journal*, vol. 29, no. 2, pp. 147–160, 1950.

[43] I. Reed, "A class of multiple-error-correcting codes and the decoding scheme," *Transactions of the IRE Professional Group on Information Theory*, vol. 4, no. 4, pp. 38–49, September 1954.

[44] D. E. Muller, "Application of boolean algebra to switching circuit design and to error detection," *Transactions of the IRE Professional Group on Electronic Computers*, no. 3, pp. 6–12, 1954.

[45] R. Silverman and M. Balser, "Coding for constant-data-rate systems," *Transactions of the IRE Professional Group on Information Theory*, vol. 4, no. 4, pp. 50–63, September 1954.

[46] P. Elias, "Coding for noisy channels," in *IRE International Convention Record*, 1955, pp. 37–46.

[47] E. Prange, *Cyclic Error-Correcting codes in two symbols*. Air force Cambridge research center, 1957.

[48] A. Hocquenghem, "Codes Correcteurs d'Erreurs," *Chiffres (Paris)*, vol. 2, pp. 147–156, Sept. 1959.

[49] R. C. Bose and D. K. Ray-Chaudhuri, "On a class of error correcting binary group codes," *Information and control*, vol. 3, no. 1, pp. 68–79, 1960.

[50] I. S. Reed and G. Solomon, "Polynomial codes over certain finite fields," *Journal of the society for industrial and applied mathematics*, vol. 8, no. 2, pp. 300–304, 1960.

[51] D. Gorenstein and N. Zierler, "A class of error-correcting codes in p^m symbols," *Journal of the Society for Industrial and Applied Mathematics*, vol. 9, no. 2, pp. 207–214, 1961.

[52] R. Gallager, "Low-density parity-check codes," *IRE Transactions on Information Theory*, vol. 8, no. 1, pp. 21–28, January 1962.

[53] E. Berlekamp, "On decoding binary Bose-Chadhuri-Hocquenghem codes," *IEEE Transactions on Information Theory*, vol. 11, no. 4, pp. 577–579, 1965.

[54] E. R. Berlekamp, "Algebraic coding theory," 1968.

[55] J. Massey, "Step-by-step decoding of the Bose-Chaudhuri-Hocquenghem codes," *IEEE Transactions on Information Theory*, vol. 11, no. 4, pp. 580–585, 1965.

[56] ——, "Shift-register synthesis and BCH decoding," *IEEE transactions on Information Theory*, vol. 15, no. 1, pp. 122–127, 1969.

[57] R. W. Watson and C. W. Hastings, "Self-checked computation using residue arithmetic," *Proceedings of the IEEE*, vol. 54, no. 12, pp. 1920–1931, 1966.

[58] N. S. Szabo and R. I. Tanaka, *Residue arithmetic and its applications to computer technology*. McGraw-Hill, 1967.

[59] A. Viterbi, "Error bounds for convolutional codes and an asymptotically optimum decoding algorithm," *IEEE transactions on Information Theory*, vol. 13, no. 2, pp. 260–269, 1967.

[60] D. Chase, "Class of algorithms for decoding block codes with channel measurement information," *IEEE Transactions on Information theory*, vol. 18, no. 1, pp. 170–182, 1972.

[61] L. Bahl, J. Cocke, F. Jelinek, and J. Raviv, "Optimal decoding of linear codes for minimizing symbol error rate (corresp.)," *Information Theory, IEEE Transactions on*, vol. 20, no. 2, pp. 284 – 287, mar 1974.

[62] J. Wolf, "Efficient maximum likelihood decoding of linear block codes using a trellis," *IEEE Transactions on Information Theory*, vol. 24, no. 1, pp. 76 – 80, jan 1978.

[63] G. Ungerboeck, "Channel coding with multilevel/phase signals," *IEEE Transactions on Information Theory*, vol. 28, no. 1, pp. 55 – 67, Jan. 1982.

[64] ——, "Trellis-coded modulation with redundant signal sets part I: Introduction," *IEEE Communications Magazine*, vol. 25, no. 2, pp. 5–11, February 1987.

[65] ——, "Trellis-coded modulation with redundant signal sets part II: State of the art," *IEEE Communications Magazine*, vol. 25, no. 2, pp. 12–21, February 1987.

[66] J. Hagenauer and P. Hoeher, "A Viterbi algorithm with soft-decision outputs and its applications," in *IEEE Global Telecommunications Conference (GLOBECOM)*. IEEE, 1989, pp. 1680–1686.

[67] W. Koch and A. Baier, "Optimum and sub-optimum detection of coded data disturbed by time-varying intersymbol interference (applicable to digital mobile radio receivers)," in *IEEE Global Telecommunications Conference (GLOBECOM)*. IEEE, 1990, pp. 1679–1684.

[68] E. Zevahi, "8-PSK trellis codes for a Rayleigh fading channel," *IEEE Transactions on Communications*, vol. 40, pp. 873–883, 1992.

[69] G. Caire, G. Taricco, and E. Biglieri, "Bit-interleaved coded modulation," *IEEE transactions on information theory*, vol. 44, no. 3, pp. 927–946, 1998.

[70] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: Turbo-codes. 1," in *Technical Program of the IEEE International Conference on Communications, ICC '93 Geneva*, vol. 2, May 1993, pp. 1064–1070 vol.2.

[71] C. Berrou and A. Glavieux, "Near optimum error correcting coding and decoding: Turbo-codes," *IEEE Transactions on communications*, vol. 44, no. 10, pp. 1261–1271, 1996.

[72] R. Pyndiah, A. Glavieux, A. Picart, and S. Jacq, "Near optimum decoding of product codes," in *IEEE Global Telecommunications Conference (GLOBECOM)*. IEEE, 1994, pp. 339–343.

[73] R. M. Pyndiah, "Near-optimum decoding of product codes: Block turbo codes," *IEEE Transactions on communications*, vol. 46, no. 8, pp. 1003–1010, 1998.

[74] P. Robertson, E. Villebrun, and P. Hoeher, "A comparison of optimal and sub-optimal map decoding algorithms operating in the log domain," in *IEEE International Conference on Communications (ICC)*, vol. 2. IEEE, 1995, pp. 1009–1013.

[75] D. MacKay and R. M. Neal, "Good codes based on very sparse matrices," *Cryptography and Coding*, pp. 100–111, 1995.

[76] D. J. MacKay and R. M. Neal, "Near Shannon limit performance of low density parity check codes," *Electronics letters*, vol. 32, no. 18, p. 1645, 1996.

[77] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," *Physical Review A*, vol. 52, no. 4, pp. R2493–R2496, Oct. 1995. [Online]. Available: http://dx.doi.org/10.1103/PhysRevA.52.R2493

[78] J. Hagenauer, E. Offer, and L. Papke, "Iterative decoding of binary block and convolutional codes," *IEEE Transactions on information theory*, vol. 42, no. 2, pp. 429–445, 1996.

[79] A. Steane, "Multiple-particle interference and quantum error correction," *Royal Society of London Proceedings Series A*, vol. 452, pp. 2551–2577, Nov. 1995.

[80] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Phys. Rev. A*, vol. 54, no. 2, pp. 1098–1105, Aug 1996.

[81] A. M. Steane, "Error correcting codes in quantum theory," *Phys. Rev. Lett.*, vol. 77, no. 5, pp. 793–797, Jul 1996.

[82] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, "Mixed-state entanglement and quantum error correction," *Phys. Rev. A*, vol. 54, pp. 3824–3851, Nov 1996. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.54.3824

[83] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, "Perfect quantum error correcting code," *Phys. Rev. Lett.*, vol. 77, pp. 198–201, Jul 1996. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.77.198

[84] D. Gottesman, "Class of quantum error-correcting codes saturating the quantum Hamming bound," *Phys. Rev. A*, vol. 54, no. 3, pp. 1862–1868, Sep 1996.

[85] ——, "Stabilizer codes and quantum error correction," Ph.D. dissertation, California Institute of Technology, 1997.

[86] H. Nickl, J. Hagenauer, and F. Burkert, "Approaching Shannon's capacity limit by 0.2 dB using simple Hamming codes," *IEEE Communications Letters*, vol. 1, no. 5, pp. 130–132, 1997.

[87] X. Li and J. A. Ritcey, "Bit-interleaved coded modulation with iterative decoding," *IEEE Communications Letters*, vol. 1, no. 6, pp. 169–171, 1997.

[88] S. Lloyd, "Capacity of the noisy quantum channel," *Phys. Rev. A*, vol. 55, pp. 1613–1622, Mar 1997. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.55.1613

[89] A. M. Steane, "Simple quantum error-correcting codes," *Physical Review A*, vol. 54, no. 6, p. 4741, 1996.

[90] M. Grassl, T. Beth, and T. Pellizzari, "Codes for the quantum erasure channel," *Phys. Rev. A*, vol. 56, pp. 33–38, Jul 1997. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.56.33

[91] A. Calderbank, E. Rains, P. Shor, and N. J. A. Sloane, "Quantum error correction via codes over GF(4)," *IEEE Transactions on Information Theory*, vol. 44, no. 4, pp. 1369–1387, Jul 1998.

[92] M. Grassl and T. Beth, "Quantum BCH Codes," *Proceedings of International Symposium on Theoretical Electrical Engineering Magdeburg*, pp. 207–212, Oct. 1999. [Online]. Available: http://arxiv.org/abs/quant-ph/9910060

[93] A. Steane, "Enlargement of Calderbank-Shor-Steane quantum codes," *IEEE Transactions on Information Theory*, vol. 45, no. 7, pp. 2492–2495, Nov 1999.

[94] L. Xiaoyan, "Quantum cyclic and constacyclic codes," *IEEE Transactions on Information Theory*, vol. 50, no. 3, pp. 547–549, 2004.

[95] A. Y. Kitaev, "Quantum computations: algorithms and error correction," *Russian Mathematical Surveys*, vol. 52, no. 6, pp. 1191–1249, 1997.

[96] ——, "Fault-tolerant quantum computation by anyons," *Annals of Physics*, vol. 303, no. 1, pp. 2–30, 2003.

[97] P. Robertson and T. Worz, "Bandwidth-efficient turbo trellis-coded modulation using punctured component codes," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 2, pp. 206 – 218, Feb. 1998.

[98] O. F. Acikel and W. E. Ryan, "Punctured turbo-codes for BPSK/QPSK channels," *IEEE Transactions on Communications*, vol. 47, no. 9, pp. 1315–1323, 1999.

[99] A. Steane, "Quantum Reed-Muller codes," *IEEE Transactions on Information Theory*, vol. 45, no. 5, pp. 1701–1703, Jul 1999.

[100] M. Grassl, W. Geiselmann, and T. Beth, "Quantum Reed-Solomon codes," in *Proceedings Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (AAECC-13)*. Springer. See, 1999, pp. 231–244.

[101] D. Divsalar, S. Dolinar and F. Pollara, "Serial concatenated trellis coded modulation with rate-1 inner code," in *Proc. IEEE Global Telecommun. Conf.*, San Francisco, CA, Nov 2000, pp. 777–782.

[102] S. ten Brink, "Convergence behaviour of iteratively decoded parallel concatenated codes," *IEEE Transactions on Communications*, vol. 49, no. 10, pp. 1727–1737, October 2001.

[103] M. S. Postol, "A proposed quantum low density parity check code," *arXiv:quant-ph/0108131v1*, 2001.

[104] M. Tüchler and J. Hagenauer, "EXIT charts of irregular codes," in *Proceedings of Conference on Information Science and Systems*, Princeton University, 20-22 March 2002, pp. 748–753.

[105] G. Bowen, "Entanglement required in achieving entanglement-assisted channel capacities," *Phys. Rev. A*, vol. 66, p. 052313, Nov 2002. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.66.052313

[106] H. Ollivier and J.-P. Tillich, "Description of a quantum convolutional code," *Phys. Rev. Lett.*, vol. 91, p. 177902, Oct 2003. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.91.177902

[107] J. Kliewer, S. X. Ng, and L. Hanzo, "Efficient computation of EXIT functions for non-binary iterative decoding," *IEEE Transactions on Communications*, vol. 54, no. 12, pp. 2133–2136, December 2006.

[108] T. A. Brun, I. Devetak, and M.-H. Hsieh, "Correcting quantum errors with entanglement," *Science*, vol. 314, no. 5798, oct. 2006.

[109] ——, "General entanglement-assisted quantum error-correcting codes," in *IEEE International Symposium on Information Theory*, june 2007, pp. 2101 –2105.

[110] M.-H. Hsieh, I. Devetak, and T. Brun, "General entanglement-assisted quantum error-correcting codes," *Phys. Rev. A*, vol. 76, p. 062313, Dec 2007. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.76.062313

[111] S. X. Ng, O. Alamri, Y. Li, J. Kliewer, and L. Hanzo, "Near-capacity turbo trellis coded modulation design based on EXIT charts and union bounds," *IEEE Transactions on Communications*, vol. 56, no. 12, pp. 2030 –2039, December 2008.

[112] D. Poulin, J.-P. Tillich, and H. Ollivier, "Quantum serial turbo-codes," in *IEEE International Symposium on Information Theory*, July 2008, pp. 310–314.

[113] D. Poulin, J. Tillich, and H. Ollivier, "Quantum serial turbo codes," *IEEE Transactions on Information Theory*, vol. 55, no. 6, pp. 2776–2798, June 2009.

[114] D. Poulin and Y. Chung, "On the iterative decoding of sparse quantum codes," *Quantum Info. Comput.*, vol. 8, no. 10, pp. 987–1000, Nov. 2008. [Online]. Available: http://dl.acm.org/citation.cfm?id=2016985.2016993

[115] Y.-J. Wang, B. Sanders, B.-M. Bai, and X.-M. Wang, "Enhanced feedback iterative decoding of sparse quantum codes," *IEEE Transactions on Information Theory*, vol. 58, no. 2, pp. 1231 –1241, feb. 2012.

[116] Z. Babar, P. Botsinis, D. Alanis, S. X. Ng, and L. Hanzo, "Fifteen years of quantum LDPC coding and improved decoding strategies," *IEEE Access*, vol. 3, pp. 2492–2519, 2015.

[117] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Transactions on Information Theory*, vol. 55, no. 7, pp. 3051–3073, July 2009.

[118] R. Tee, R. Maunder, and L. Hanzo, "EXIT-chart aided near-capacity irregular bit-interleaved coded modulation design," *IEEE Transactions on Wireless Communications*, vol. 8, no. 1, pp. 32–37, 2009.

[119] M.-H. Hsieh, T. A. Brun, and I. Devetak, "Entanglement-assisted quantum quasicyclic low-density parity-check codes," *Phys. Rev. A*, vol. 79, p. 032340, Mar 2009. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.79.032340

[120] M. M. Wilde and T. A. Brun, "Entanglement-assisted quantum convolutional coding," *Phys. Rev. A*, vol. 81, p. 042333, Apr 2010. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.81.042333

[121] M. M. Wilde and M.-H. Hsieh, "Entanglement boosts quantum turbo codes," in *IEEE International Symposium on Information Theory*, Aug. 2011, pp. 445 – 449.

[122] M. Wilde, M.-H. Hsieh, and Z. Babar, "Entanglement-assisted quantum turbo codes," *IEEE Transactions on Information Theory*, vol. 60, no. 2, pp. 1203–1222, Feb 2014.

[123] M. Wilde and S. Guha, "Polar codes for classical-quantum channels," *IEEE Transactions on Information Theory*, vol. 59, no. 2, pp. 1175 –1187, feb. 2013.

[124] ——, "Polar codes for degradable quantum channels," *IEEE Transactions on Information Theory*, vol. 59, no. 7, pp. 4718–4729, July 2013.

[125] J. M. Renes, F. Dupuis, and R. Renner, "Efficient polar coding of quantum information," *Phys. Rev. Lett.*, vol. 109, p. 050504, Aug 2012. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.109.050504

[126] E. Pelchat and D. Poulin, "Degenerate Viterbi decoding," *IEEE Transactions on Information Theory*, vol. 59, no. 6, pp. 3915–3921, 2013.

[127] Z. Babar, S. X. Ng, and L. Hanzo, "EXIT-chart aided near-capacity quantum turbo code design," *IEEE Transactions on Vehicular Technology*, vol. PP, no. 99, pp. 1–1, 2014.

[128] R. Maunder, "A fully-parallel turbo decoding algorithm," *IEEE Transactions on Communications*, vol. 63, no. 8, pp. 2762–2775, Aug 2015.

[129] Z. Babar, P. Botsinis, D. Alanis, S. X. Ng, and L. Hanzo, "The road from classical to quantum codes: A hashing bound approaching design procedure," *IEEE Access*, vol. 3, pp. 146–176, 2015.

[130] J. M. Renes, D. Sutter, F. Dupuis, and R. Renner, "Efficient quantum polar codes requiring no preshared entanglement," *IEEE Transactions on Information Theory*, vol. 61, no. 11, pp. 6395–6414, 2015.

[131] Z. Babar, H. V. Nguyen, P. Botsinis, D. Alanis, D. Chandra, S. X. Ng, and L. Hanzo, "Serially concatenated unity-rate codes improve quantum codes without coding-rate reduction," *IEEE Communications Letters*, vol. 20, no. 10, pp. 1916–1919, 2016.

[132] Z. Babar, H. V. Nguyen, P. Botsinis, D. Alanis, D. Chandra, S. X. Ng, R. G. Maunder, and L. Hanzo, "Fully-parallel quantum turbo decoder," *IEEE Access*, vol. 4, pp. 6073–6085, 2016.

[133] L. Hanzo, *Near-capacity variable-length coding: regular and EXIT-chart-aided irregular designs*. John Wiley & Sons, 2010, vol. 20.

[134] L. Hanzo, T. H. Liew, B. L. Yeap, R. Y. S. Tee and S. X. Ng, *Turbo Coding, Turbo Equalisation and Space-Time Coding: EXIT-Chart-Aided Near-Capacity Designs for Wireless Channels, 2nd Edition*. New York, USA: John Wiley IEEE Press, March 2011.

[135] R. C. Bose and D. K. Ray-Chaudhuri, "Further results on error correcting binary group codes," *Information and Control*, vol. 3, no. 3, pp. 279–290, 1960.

[136] *Blue Book: Recommendations for Space Data System Standards: Telemetry Channel Coding*. Consultative Committee for Space Data Systems, May 1984.

[137] M. El-Hajjar and L. Hanzo, "EXIT charts for system design and analysis," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 127–153, First 2014.

[138] *Universal Mobile Telecommunications System (UMTS); Multiplexing and Channel Coding (FDD), V9.3.0*. ETSI TS 125 222, 2012.

[139] *LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Multiplexing and Channel Coding, V13.1.0*. ETSI TS 136 212, 2016.

[140] K. Niu, K. Chen, J. Lin, and Q. T. Zhang, "Polar codes: Primary concepts and practical decoding algorithms," *IEEE Communications Magazine*, vol. 52, no. 7, pp. 192–203, July 2014.

[141] P. W. Shor, "The quantum channel capacity and coherent information," *Lecture Notes, MSRI Workshop on Quantum Computation*, 2002.

[142] I. Devetak, "The private classical capacity and quantum capacity of a quantum channel," *IEEE Transactions on Information Theory*, vol. 51, no. 1, pp. 44–55, Jan 2005.

[143] D. P. DiVincenzo, P. W. Shor, and J. A. Smolin, "Quantum-channel capacity of very noisy channels," *Phys. Rev. A*, vol. 57, pp. 830–839, Feb 1998. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.57.830

[144] G. Smith and J. A. Smolin, "Degenerate quantum codes for Pauli channels," *Phys. Rev. Lett.*, vol. 98, p. 030501, Jan 2007. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.98.030501

[145] C.-Y. Lai, T. Brun, and M. Wilde, "Dualities and identities for entanglement-assisted quantum codes," *Quantum Information Processing*, vol. 13, no. 4, pp. 957–990, 2014. [Online]. Available: http://dx.doi.org/10.1007/s11128-013-0704-8

[146] D. MacKay, G. Mitchison, and P. McFadden, "Sparse-graph codes for quantum error correction," *IEEE Transactions on Information Theory*, vol. 50, no. 10, pp. 2315–2330, Oct 2004.

[147] T. Camara, H. Ollivier, and J.-P. Tillich, "Constructions and performance of classes of quantum LDPC codes," *arXiv:quant-ph/0502086v2*, 2005.

[148] ——, "A class of quantum LDPC codes: construction and performances under iterative decoding," in *IEEE International Symposium on Information Theory*, June 2007, pp. 811–815.

[149] H. Ollivier and J. P. Tillich, "Quantum convolutional codes: fundamentals," *quant-ph/0401134*, 2004.

[150] G. D. Forney and S. Guha, "Simple rate-1/3 convolutional and tail-biting quantum error-correcting codes," in *IEEE International Symposium on Information Theory*, Sept. 2005, pp. 1028 –1032.

[151] G. D. Forney, M. Grassl, and S. Guha, "Convolutional and tail-biting quantum error-correcting codes," *IEEE Transactions on Information Theory*, vol. 53, no. 3, pp. 865–880, March 2007.

[152] M. Houshmand and M. Wilde, "Recursive quantum convolutional encoders are catastrophic: A simple proof," *IEEE Transactions on Information Theory*, vol. 59, no. 10, pp. 6724–6731, 2013.

[153] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, Oct. 1982. [Online]. Available: http://dx.doi.org/10.1038/299802a0

[154] L. Hanzo, T. H. Liew, and B. L. Yeap, *Turbo coding, turbo equalisation and space-time coding*. John Wiley & Sons, 2002.

[155] P. Botsinis, Z. Babar, D. Alanis, D. Chandra, H. Nguyen, S. X. Ng, and L. Hanzo, "Quantum error correction protects quantum search algorithms against decoherence," *Scientific Reports*, vol. 6, 2016.

[156] M. Grassl and T. Beth, "Cyclic quantum error–correcting codes and quantum shift registers," in *Proceedings of the Royal Society of London*

A: Mathematical, Physical and Engineering Sciences, vol. 456, no. 2003. The Royal Society, 2000, pp. 2689–2706.

[157] S. Lin and D. J. Costello, *Error Control Coding*. New Jersey, USA: Pearson-Prentice Hall, 2004.

[158] J. Schalkwijk and A. Vinck, "Syndrome decoding of convolutional codes," *IEEE Transactions on Communications*, vol. 23, no. 7, pp. 789 – 792, jul 1975.

[159] ——, "Syndrome decoding of binary rate-1/2 convolutional codes," *IEEE Transactions on Communications*, vol. 24, no. 9, pp. 977 – 985, sep 1976.

[160] J. Schalkwijk, A. Vinck, and K. Post, "Syndrome decoding of binary-rate k/n convolutional codes," *IEEE Transactions on Information Theory*, vol. 24, no. 5, pp. 553 – 562, sep 1978.

[161] M. Ariel and J. Snyders, "Soft syndrome decoding of binary convolutional codes," *IEEE Transactions on Communications*, vol. 43, no. 234, pp. 288 – 297, Feb./Mar./Apr. 1995.

[162] V. Sidorenko and V. Zyablov, "Decoding of convolutional codes using a syndrome trellis," *Information Theory, IEEE Transactions on*, vol. 40, no. 5, pp. 1663 –1666, sep 1994.

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received May 7, 2017, accepted June 8, 2017, date of publication June 16, 2017, date of current version July 17, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2716367

Quantum Coding Bounds and a Closed-Form Approximation of the Minimum Distance Versus Quantum Coding Rate

DARYUS CHANDRA, (Student Member, IEEE), ZUNAIRA BABAR, HUNG VIET NGUYEN, (Member, IEEE), DIMITRIOS ALANIS, (Student Member, IEEE), PANAGIOTIS BOTSINIS, (Member, IEEE), SOON XIN NG, (Senior Member, IEEE), AND LAJOS HANZO, (Fellow, IEEE)

School of Electronics and Computer Science, University of Southampton, Southampton, SO17 1BJ, U.K.

Corresponding author: Lajos Hanzo (lh@ecs.soton.ac.uk)

This work was supported in part by EPSRC under Grant EP/L018659/1, in part by the European Research Council, Advanced Fellow Grant, and in part by the Royal Society's Wolfson Research Merit Award. The research data of this paper can be found at http://doi.org/10.5258/SOTON/D0131.

ABSTRACT The tradeoff between the quantum coding rate and the associated error correction capability is characterized by the quantum coding bounds. The unique solution for this tradeoff does not exist, but the corresponding lower and the upper bounds can be found in the literature. In this treatise, we survey the existing quantum coding bounds and provide new insights into the classical to quantum duality for the sake of deriving new quantum coding bounds. Moreover, we propose an appealingly simple and invertible analytical approximation, which describes the tradeoff between the quantum coding rate and the minimum distance of quantum stabilizer codes. For example, for a half-rate quantum stabilizer code having a code word length of $n = 128$, the minimum distance is bounded by $11 < d < 22$, while our formulation yields a minimum distance of $d = 16$ for the above-mentioned code. Ultimately, our contributions can be used for the characterization of quantum stabilizer codes.

INDEX TERMS Quantum error correction codes, quantum stabilizer codes, quantum coding bound.

NOMENCLATURE

LIST OF ACRONYMS

CNOT	Controlled-NOT
CSS	Calderbank-Shor-Steane
EA	Entanglement-Assisted
GV	Gilbert-Varshamov
PCM	Parity Check Matrix
QBCH	Quantum Bose-Chaudhuri-Hocquenghem
QBER	QuBit Error Rate
QECC	Quantum Error Correction Code
QGF(4)	Quantum code from $GF(4)$
QRM	Quantum Reed-Muller
QSC	Quantum Stabilizer Code

LIST OF SYMBOLS

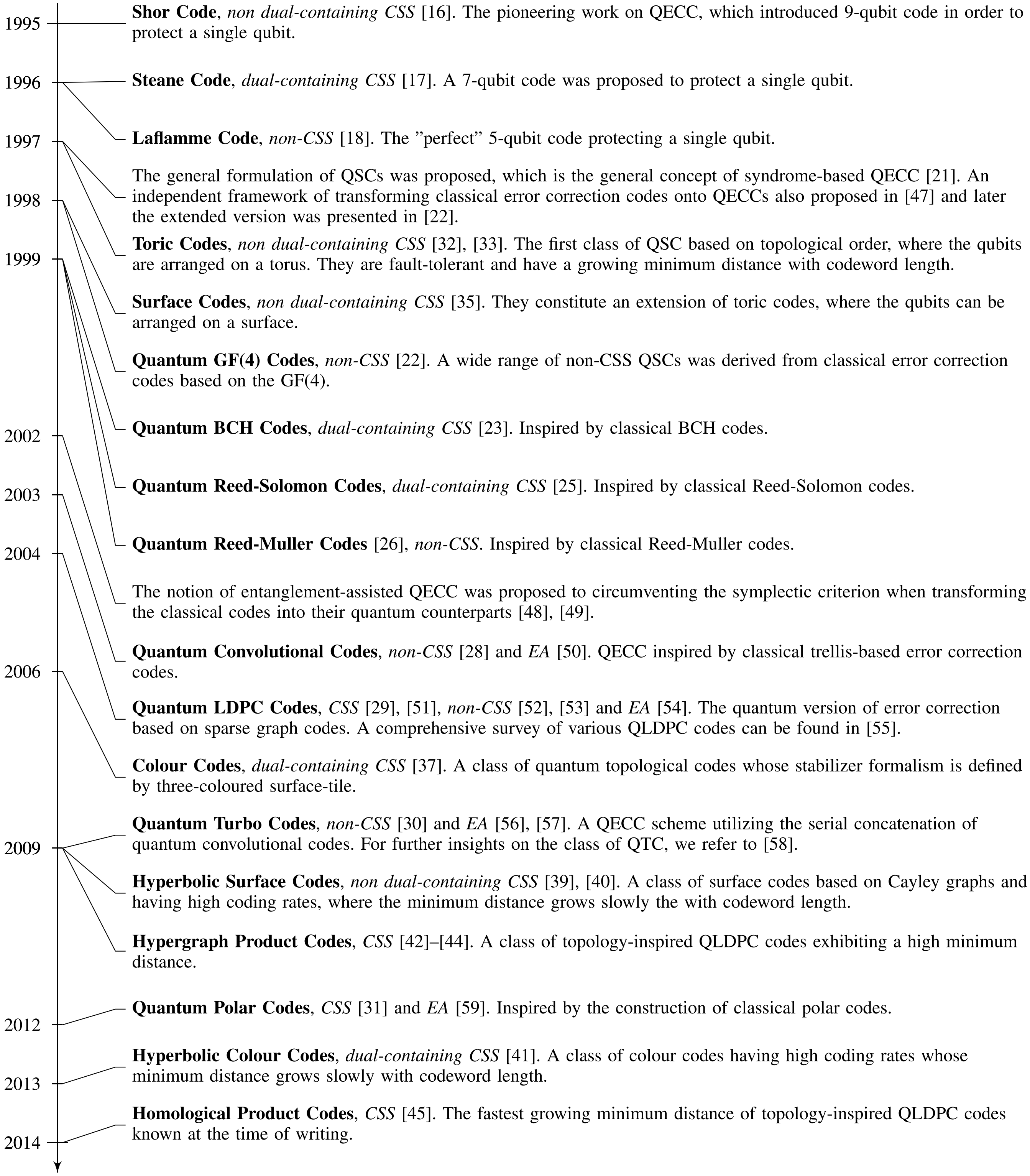
c	Number of Preshared Entangled Pair of Qubits
d	Minimum Distance
d_{ea}	Minimum Distance of Entanglement-Assisted Code
E	Entanglement Consumption Rate
$\mathcal{E}$	Pauli Error Pattern
$\mathbf{e}$	Error Vector
g	Stabilizer Operator
$\mathbf{G}$	Generator Matrix
$H(x)$	Binary Entropy of x
$\mathbf{H}$	Parity Check Matrix, Hadamard Transformation
k	Information Bit Length, Number of Logical Qubits
n	Codeword Length, Number of Physical Qubits
r	Classical Coding Rate
r_Q	Quantum Coding Rate
$\mathbf{s}$	Syncrome Vector
t	Error Correction Capability
U	Unitary Transformation
δ	Normalized Minimum Distance
θ	Entanglement Ratio
$\otimes$	Kronecker Tensor Product
$\vert\psi\rangle$	Quantum State ψ

I. INTRODUCTION

Moore's Law has remained valid for five decades, but based on its prediction at the time of writing the classical integrated circuits are expected to enter the nano-scale domain, where the laws of quantum mechanics prevail [1], [2]. Quantum computers potentially offer substantial benefits over classical computers owing to their inherent parallel processing capability [3]–[14]. However, quantum computers are susceptible to the deleterious effect of quantum decoherence. Hence, quantum error correction codes (QECCs) have been proposed for correcting the bit-flips and phase-flips imposed by the decoherence effects. Furthermore, the employment of QECC in quantum computers is also capable of extending the coherence time of qubits [15]. The concept of protecting quantum information is similar to that of its classical counterpart by attaching redundancy to the information, which is then invoked later for error correction. The quest for finding the "good" QECCs was inspired by Shor, who introduced the 9-qubit code, which is often referred to as the Shor's code [16]. Shor's code encodes a single information qubit, which is also referred to as ''logical qubit'', into nine encoded qubits or "physical qubits". The Shor's code construction is capable of protecting the nine physical qubits from any type of single qubit error. Following the discovery of Shor's code, another QECC scheme, namely the Steane's code, was proposed [17]. The latter is capable of protecting any single qubit error by encoding a single logical qubit into seven physical qubits, instead of nine qubits. The question about what the minimum number of physical qubits is required in order to protect the physical qubits from any type of single qubit error was answered when Laflamme *et al.* proposed the 5-qubit quantum code [18]. This 5-qubit code may be referred to as Laflamme's code or also shown as the "perfect code", since the code construction achieves the quantum Hamming bound, which is the upper bound of quantum coding rate given the minimum diatance of any QECC construction [19], [20].

The field of QECCs entered its golden age following the invention of quantum stabilizer codes (QSCs) [21], [22]. The QSC paradigm allows us to transform the classical error correction codes into their quantum counterparts. The QSCs also circumvent the problem of estimating both the number and the position of quantum-domain errors imposed by quantum decoherence without observing the actual quantum states, since observing the quantum states would collapse the qubits into classical bits. This extremely beneficial error estimation was achieved by introducing the syndrome-measurement based approach [21], [22]. In classical error correction codes, the syndrome-measurement based approach has been widely exploited for invoking the error detection and correction procedure. Therefore, the formulation of QSCs expanded the search space of good QECCs to a broader horizon. This new paradigm of incorporating the classical to quantum isomorphisms, led to the transformation of classical codes to their quantum domain duals, such as Quantum Bose-Chaudhuri-Hocquenghem (QBCH) codes [23], [24], Quantum Reed-Solomon (QRS) codes [25], Quantum Reed-Muller (QRM) codes [26], Quantum Convolutional Codes (QCC) [27], [28], Quantum Low-Density Parity-Check (QLDPC) codes [29], Quantum Turbo Codes (QTC) [30] and Quantum Polar Codes (QPC) [31]. Apart from exploiting the above isomorphism, there are also significant contributions on directly developing code constructions solely based on the pure quantum topology and homology, as exemplified by the family of toric codes [32]–[34], surface codes [35], [36], colour codes [37], cubic codes [38], hyperbolic surface codes [39], [40], hyperbolic color codes [41], hypergraph product codes [42]–[44] and homological product codes [45]. A timeline that portrays the milestones of QSCs, at a glance is depicted in Fig. 1. Although the QSC formulation creates an important class of QECCs, we note that there are also other classes of QECCs beside the QSCs, such as the class of decoherence-free subspace (DFS) codes. DFS codes can be viewed as passive QECCs, while the QSCs are a specific example of the active ones. To elaborate a little further, DFS codes constitute a highly degenerate class of QECCs, which rely on the fact that the error patterns may preserve the state of physical qubits and therefore they do not neccessarily require a recovery procedure [46]. Due to their strong reliance on the degeneracy property exhibited by QECCs without a classical counterpart, the class of DFS codes bears no resemblance to any classical error correction codes. Therefore, in this treatise we focus our discussions purely on QSCs, which exhibit strong analogies with classical error correction codes.

Even though intensive research efforts have been invested in exploring the QSCs field, one of the mysteries still remains unresolved. Since the development of the first QSC, one of the open problems has been how to determine the realistically achievable size of the codebook $|\mathcal{C}| = 2^k$, given the number of physical qubits n, the minimum distance of d, and the quantum coding rate of $r_Q = k/n$, where k denotes the number of logical qubits. The minimum distance d is the parameter that defines the error correction capability of the corresponding code. The complete formulation of the realistically achievable minimum distance d, given the number of physical qubits n and the quantum coding rate r_Q is unknown at the time of writing, but several theoretical lower and upper bounds can be found in the literature. Naturally, finding code constructions associated with growing minimum distances upon reducing the coding rate is desirable, since an increased minimum distance improves the reliability of quantum computation [60]–[64]. From the implementational perspective, the so-called quantum topological codes are popular in the field of fault-tolerant quantum computing. Nonetheless, one of the substantial drawbacks of quantum topological codes is their potentially very low quantum coding rate, tends towards zero for long codewords. Another class suitable for fault-tolerant QSCs is constituted by the family of QLDPC codes, which is a benefit of their sparse parity check matrices (PCMs), since the sparseness of the PCM guarantees having a limited error propagation of the qubits within a



Shor Code, *non dual-containing CSS* [16]. The pioneering work on QECC, which introduced 9-qubit code in order to protect a single qubit.

Steane Code, *dual-containing CSS* [17]. A 7-qubit code was proposed to protect a single qubit.

Laflamme Code, *non-CSS* [18]. The ”perfect” 5-qubit code protecting a single qubit.

The general formulation of QSCs was proposed, which is the general concept of syndrome-based QECC [21]. An independent framework of transforming classical error correction codes onto QECCs also proposed in [47] and later the extended version was presented in [22].

Toric Codes, *non dual-containing CSS* [32], [33]. The first class of QSC based on topological order, where the qubits are arranged on a torus. They are fault-tolerant and have a growing minimum distance with codeword length.

Surface Codes, *non dual-containing CSS* [35]. They constitute an extension of toric codes, where the qubits can be arranged on a surface.

Quantum GF(4) Codes, *non-CSS* [22]. A wide range of non-CSS QSCs was derived from classical error correction codes based on the GF(4).

Quantum BCH Codes, *dual-containing CSS* [23]. Inspired by classical BCH codes.

Quantum Reed-Solomon Codes, *dual-containing CSS* [25]. Inspired by classical Reed-Solomon codes.

Quantum Reed-Muller Codes [26], *non-CSS*. Inspired by classical Reed-Muller codes.

The notion of entanglement-assisted QECC was proposed to circumventing the symplectic criterion when transforming the classical codes into their quantum counterparts [48], [49].

Quantum Convolutional Codes, *non-CSS* [28] and *EA* [50]. QECC inspired by classical trellis-based error correction codes.

Quantum LDPC Codes, *CSS* [29], [51], *non-CSS* [52], [53] and *EA* [54]. The quantum version of error correction based on sparse graph codes. A comprehensive survey of various QLDPC codes can be found in [55].

Colour Codes, *dual-containing CSS* [37]. A class of quantum topological codes whose stabilizer formalism is defined by three-coloured surface-tile.

Quantum Turbo Codes, *non-CSS* [30] and *EA* [56], [57]. A QECC scheme utilizing the serial concatenation of quantum convolutional codes. For further insights on the class of QTC, we refer to [58].

Hyperbolic Surface Codes, *non dual-containing CSS* [39], [40]. A class of surface codes based on Cayley graphs and having high coding rates, where the minimum distance grows slowly the with codeword length.

Hypergraph Product Codes, *CSS* [42]–[44]. A class of topology-inspired QLDPC codes exhibiting a high minimum distance.

Quantum Polar Codes, *CSS* [31] and *EA* [59]. Inspired by the construction of classical polar codes.

Hyperbolic Colour Codes, *dual-containing CSS* [41]. A class of colour codes having high coding rates whose minimum distance grows slowly with codeword length.

Homological Product Codes, *CSS* [45]. The fastest growing minimum distance of topology-inspired QLDPC codes known at the time of writing.

FIGURE 1. Timeline of important milestones in QECC field, specifically in the development of QSCs. The code construction is highlighted with bold fonts, while the associated code type is printed in *italics*.

codeword. Although the QLDPC codes are capable of achieving a good performance at an adequate coding rate, they actually have a modest minimum distance [29]. The trade-off between the quantum coding rate and the minimum distance as well as the codeword length is widely recognized, but the achievable minimum distance d of a quantum code given the quantum coding rate r_Q and codeword length n still remained unresolved. For example, for a given codeword length of $n = 128$ and quantum coding rate of $r_Q = 1/2$, the achievable minimum distance is losely bounded by $11 < d < 22$, while for $n = 1024$ and $r_Q = 1/2$, the achievable minimum distance is bounded by $78 < d < 157$. Naturally, having such a wide range of minimum distance is undesirable. For binary classical codes, this problem has been circumvented by the closed-form approximation proposed by Akhtman *et al.* [65].

The challenge of creating the quantum counterpart of error correction codes lies in the fact that QSC constructions have to mitigate not only bit-flip errors, but also phase-flip errors or in fact both bit-flip and phase-flip errors. Based on how we mitigate those different types of errors, we can simply categorize QSCs as being in the class of Calderbank-Shor-Steane (CSS) codes [17], [66], [67] or as being non-CSS codes [22]. The CSS codes handle the qubit errors by treating the bit-flip errors and phase-flip errors as separate entities. By contrast, the class of non-CSS codes treat both bit-flip errors and phase-flip errors simultaneously. Since the CSS codes treat the bit-flip and phase-flip error correction procedures separately, in general, they exhibit a lower coding rate than their non-CSS counterparts having the same error correction capability. Furthermore, if we also consider the presence of quantum entanglement, we may conceive more powerful quantum code constructions. To elaborate, the family of entanglement-assisted quantum stabilizer codes (EA-QSCs) is capable of operating at a higher quantum coding rate than the unassisted QSC constructions at a given error correction capability, provided that error-free maximally-entangled qubits have already been pre-shared [48], [49].

Against this background, our contributions are summarized as follows:

- *We provide a survey of the existing quantum coding bounds found in the literature, along with their relationship to the existing quantum stabilizer code constructions. Moreover, to bridge the gap between the classical and quantum coding bounds, we provide further insights into the classical to quantum isomorphism in the context of the associated coding bound formulations.*
- *We formulate a simple invertible formulation of $r(n, \delta)$ characterizing the relationship between the quantum coding rate and the associated achievable minimum distance of quantum stabilizer codes. The resultant closed-form approximation of quantum coding bound is suitable both for idealized infinite and practical finite-length codewords. More specifically, we show that using our closed-form approximation, we become able to estimate the realistically achievable minimum distance of quantum stabilizer codes.*
- *We then derive the bounds for maximally-entangled quantum stabilizer codes in conjunction with arbitrary entanglement ratios and relate them to those of unassisted quantum stabilizer codes. More explicitly, for the entanglement ratio of $\theta = 0$, we arrive at the bounds of unassisted quantum stabilizer codes while for $\theta = 1$, we generate the quantum coding bounds for their maximally-entangled counterparts.*

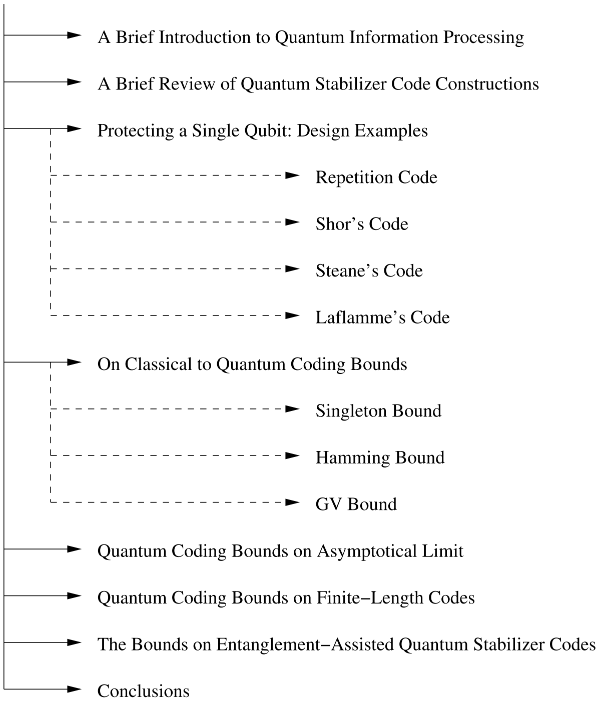

A Brief Introduction to Quantum Information Processing
A Brief Review of Quantum Stabilizer Code Constructions
Protecting a Single Qubit: Design Examples
Repetition Code
Shor's Code
Steane's Code
Laflamme's Code
On Classical to Quantum Coding Bounds
Singleton Bound
Hamming Bound
GV Bound
Quantum Coding Bounds on Asymptotical Limit
Quantum Coding Bounds on Finite–Length Codes
The Bounds on Entanglement–Assisted Quantum Stabilizer Codes
Conclusions

FIGURE 2. The structure of the paper.

The structure of the paper is described in Fig. 2 and the rest of this paper is organized as follows. In Section II, we commence with a brief fundamentals background on quantum states. A review of QSC constructions is presented in Section III, followed by Section IV, where we illustrate the Pauli-to-Binary isomorphism in the context of QSCs that are capable of correcting single qubit errors. By incorporating the classical to quantum duality, we show how to derive quantum coding bounds from their classical counterparts and we also contrast them in Section V. We then proceed with the study of quantum coding bounds derived both for asymptotical infinite and practical finite-length codewords in Section VI and Section VII, respectively. We then provide further insights into the quantum coding bounds of entanglement-assisted quantum stabilizer codes in Section VIII. Finally, we conclude in Section IX.

II. A BRIEF INTRODUCTION TO QUANTUM INFORMATION PROCESSING

In classical computation, the information is conveyed by a binary digit or "bit". Each bit has a value of either logical "0" or "1". Similarly, in a quantum computer, a single element of information is represented by a quantum bit (qubit). Each of the qubits is in a superposition of the "0" and "1". The state of a single qubit can be represented mathematically as

$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle, \tag{1}$$

where we have $\alpha_0, \alpha_1 \in \mathbb{C}$ and $|\alpha_0|^2 + |\alpha_1|^2 = 1$. For a single qubit in the state of Eq. (1), the probability of obtaining $|0\rangle$ upon observation is $P_0 = |\alpha_0|^2$ and for the state $|1\rangle$, it is $P_1 = |\alpha_1|^2$. Representing the state of a qubit as shown in Eq. (1) is also known as the Dirac notation or ''bra-ket'' notation [68]. Apart from using the Dirac notation, we may represent the state of a single qubit as a 2-component vector as follows:

$$\begin{aligned}|\psi\rangle &= \alpha_0|0\rangle + \alpha_1|1\rangle \\ &= \alpha_0\begin{pmatrix}1\\0\end{pmatrix} + \alpha_1\begin{pmatrix}0\\1\end{pmatrix} \\ &= \begin{pmatrix}\alpha_0\\\alpha_1\end{pmatrix}.\end{aligned} \tag{2}$$

Basically, a single qubit system may be viewed as a two-component vector in the two-dimensional Hilbert space and correspondingly an N-qubit string lies within the 2^N-dimensional Hilbert space. More specifically, for example, a two-qubit operand is in a superposition of four states of 00, 01, 10, and 11 simultaneously, which can be written as

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle, \tag{3}$$

where the constraints of $\alpha_{00}, \alpha_{01}, \alpha_{10}, \alpha_{11} \in \mathbb{C}$ and $|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$ still hold. If the binary representations of 00, 01, 10 and 11 are translated to their decimal representations of 0, 1, 2 and 3 respectively, the resultant N-qubit state can be encapsulated as

$$|\psi\rangle = \sum_{i=0}^{2^N-1} \alpha_i|i\rangle \text{ where } \alpha_i \in \mathbb{C}, \sum_{i=0}^{2^N-1} |\alpha_i|^2 = 1. \tag{4}$$

The Pauli group $\mathcal{G}_1$ defines the unitary transformation of a single qubit, which is closed under multiplication. The Pauli group $\mathcal{G}_1$ is defined as

$$\mathcal{G}_1 = \{eP : P \in \{\mathbf{I}, \mathbf{X}, \mathbf{Y}, \mathbf{Z}\}, e \in \{\pm 1, \pm i\}\}, \tag{5}$$

where $\mathbf{I}$, $\mathbf{X}$, $\mathbf{Y}$ and $\mathbf{Z}$ are the Pauli matrices, which manipulate the two-dimensional single qubit state and each of them is defined as follows:

$$\mathbf{I} = \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}, \quad \mathbf{X} = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}, \\ \mathbf{Y} = \begin{pmatrix}0 & -i\\i & 0\end{pmatrix}, \quad \mathbf{Z} = \begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}. \tag{6}$$

In the context of quantum information processing, each Pauli matrix represents the discrete set of errors that may corrupt a single qubit state. Physically, they represent a bit-flip error ($\mathbf{X}$), a phase-flip error ($\mathbf{Z}$), as well as a joint bit-flip and phase-flip error ($i\mathbf{XZ} = \mathbf{Y}$), while Pauli-$\mathbf{I}$ represents the identity operator corresponding to the absence of errors. However, it is always important to bear in mind that the nature of quantum decoherence is continuous and it can be modeled as a linear combination of $\mathbf{X}$, $\mathbf{Z}$, and $\mathbf{Y}$ type errors. Fortunately, due to the effect of stabilizer measurement, we can model the continuous nature of quantum decoherence with the aid of the bit-flip ($\mathbf{X}$), phase-flip ($\mathbf{Z}$), as well as a simultaneous bit-flip and phase flip ($\mathbf{Y}$) errors.

For an N-qubit operator, the general Pauli group $\mathcal{G}_n$ is represented by an n-fold tensor product of $\mathcal{G}_1$, as defined below:

$$\mathcal{G}_n = \{P_1 \otimes P_2 \cdots \otimes P_n | P_j \in \mathcal{G}_1\}. \tag{7}$$

The Pauli channel inflicts an error $\mathcal{P} \in \mathcal{G}_n$ on an N-qubit string, where each qubit may independently experience either a bit-flip error ($\mathbf{X}$), a phase-flip error ($\mathbf{Z}$), or both bit-flip and phase-flip error ($i\mathbf{XZ} = \mathbf{Y}$). For instance, let us assume having a single qubit in the state of $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$. A Pauli matrix $\mathbf{X}$ transforms a single qubit in the state of $|\psi\rangle$ into the following state:

$$\begin{aligned}|\psi'\rangle &= \mathbf{X}|\psi\rangle \\ &= \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\cdot\begin{pmatrix}\alpha_0\\\alpha_1\end{pmatrix} \\ &= \begin{pmatrix}\alpha_1\\\alpha_0\end{pmatrix} \\ &\equiv \alpha_1|0\rangle + \alpha_0|1\rangle.\end{aligned} \tag{8}$$

The transformation by the Pauli matrix $\mathbf{Z}$ of a single qubit state results in a phase-flip, which is defined by

$$\begin{aligned}|\psi'\rangle &= \mathbf{Z}|\psi\rangle \\ &= \begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}\cdot\begin{pmatrix}\alpha_0\\\alpha_1\end{pmatrix} \\ &= \begin{pmatrix}\alpha_0\\-\alpha_1\end{pmatrix} \\ &\equiv \alpha_0|0\rangle - \alpha_1|1\rangle.\end{aligned} \tag{9}$$

By following the same method, we can readily determine the manipulated state of a single qubit by the Pauli matrix $\mathbf{Y}$ resulting both in a simultaneous bit-flip and phase-flip as follows:

$$\begin{aligned}|\psi'\rangle &= \mathbf{Y}|\psi\rangle \\ &= \begin{pmatrix}0 & -i\\i & 0\end{pmatrix}\cdot\begin{pmatrix}\alpha_0\\\alpha_1\end{pmatrix} \\ &= \begin{pmatrix}i\alpha_1\\-i\alpha_0\end{pmatrix} \\ &\equiv i\alpha_1|0\rangle - i\alpha_0|1\rangle,\end{aligned} \tag{10}$$

Let us now proceed by applying the unitary transformation to a multi-qubit state of Eq. 7. For instance, let us assume a two-qubit operand in the state of Eq. 3, which can be represented as a 4-element vector as follows:

$$|\psi\rangle = \begin{pmatrix}\alpha_{00}\\\alpha_{01}\\\alpha_{10}\\\alpha_{11}\end{pmatrix}. \tag{11}$$

For example, the quantum decoherence inflicts the two-qubit unitary transformation of $(\mathbf{X} \otimes \mathbf{I})$[1] upon a two-qubit state,

[1] For the sake of simplifying the notation, a set of Pauli matrices for defining a multi-qubit unitary transformation usually does not include the "$\otimes$" operator. For example, a unitary transformation ($\mathbf{X} \otimes \mathbf{Z} \otimes \mathbf{X} \otimes \mathbf{I}$) acting upon a 4-qubit operand can simply be rewritten as $\mathbf{XZXI}$. In the rest of the paper, the latter representation is used.

which can be described as follows:

$$\begin{aligned}|\psi'\rangle &= (\mathbf{X}\otimes\mathbf{I})\,|\psi\rangle\\ &= \left(\begin{pmatrix}0&1\\1&0\end{pmatrix}\otimes\begin{pmatrix}1&0\\0&1\end{pmatrix}\right)\cdot\begin{pmatrix}\alpha_{00}\\\alpha_{01}\\\alpha_{10}\\\alpha_{11}\end{pmatrix}\\ &= \begin{pmatrix}0 & \begin{pmatrix}1&0\\0&1\end{pmatrix}\\ \begin{pmatrix}1&0\\0&1\end{pmatrix} & 0\end{pmatrix}\cdot\begin{pmatrix}\alpha_{00}\\\alpha_{01}\\\alpha_{10}\\\alpha_{11}\end{pmatrix}\\ &= \begin{pmatrix}0&0&1&0\\0&0&0&1\\1&0&0&0\\0&1&0&0\end{pmatrix}\cdot\begin{pmatrix}\alpha_{00}\\\alpha_{01}\\\alpha_{10}\\\alpha_{11}\end{pmatrix}\\ &= \begin{pmatrix}\alpha_{10}\\\alpha_{11}\\\alpha_{00}\\\alpha_{01}\end{pmatrix}\\ &\equiv \alpha_{10}|00\rangle+\alpha_{11}|01\rangle+\alpha_{00}|10\rangle+\alpha_{01}|11\rangle. \end{aligned}\tag{12}$$

The final state of Eq. (12) can also be obtained without expanding the tensor product of the unitary transformation by flipping the state of the first qubit, since the unitary transformation of **XI** means that a bit-flip error occurs on the first qubit, while the second qubit does not experience any impairment. More explicitly, due to the unitary transformation **XI**, the state of $|00\rangle$ is changed to state of $|10\rangle$. The same transformation is also applied to the states of $|01\rangle$, $|10\rangle$, and $|11\rangle$, where they are transformed to the states of $|11\rangle$, $|00\rangle$, $|10\rangle$, respectively. Hence, the magnitude associated with the state of $|00\rangle$ is no longer α_{00} and now it becomes α_{10}. Therefore, the magnitudes associated with the states of $|01\rangle$, $|10\rangle$, and $|11\rangle$ are α_{11}, α_{00}, and α_{01}, respectively.

Since we focus our discussions on the family of QSCs, the quantum coding bounds can be derived from their classical counterparts. Even though most of the well-known bounds on quantum codes are derived on the basis of the classical-to-quantum isomorphism, the pure quantum code constructions not relying on the classical-to-quantum isomorphism, but rather based on topological and homological orders still obey to these quantum coding bounds, provided that they belong to the family of non-degenerate quantum codes. To elaborate a little further, degeneracy is one of the distinctive characteristics of quantum codes, which cannot be found in their classical counterpart. More explicitly, quantum codes inherently exhibit a degeneracy property implying that different error patterns of $\mathcal{P}\in\mathcal{G}_n$ may yield an identical corrupted state. For example, let us assume a two-qubit operand in the following state:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle+|11\rangle\right), \tag{13}$$

and consider two different error patterns, which can be described as a pair of two-qubit unitary transformations given by $\mathcal{E}_1 = \mathbf{IZ}$ and $\mathcal{E}_2 = \mathbf{ZI}$. The resultant state after the error pattern $\mathcal{E}_1$ is imposed to the two-qubit system can be described as follows:

$$\begin{aligned}|\psi_1'\rangle &= \mathbf{IZ}|\psi\rangle\\ &= \begin{pmatrix}1&0&0&0\\0&-1&0&0\\0&0&1&0\\0&0&0&-1\end{pmatrix}\cdot\begin{pmatrix}\frac{1}{\sqrt{2}}\\0\\0\\\frac{1}{\sqrt{2}}\end{pmatrix}=\begin{pmatrix}\frac{1}{\sqrt{2}}\\0\\0\\-\frac{1}{\sqrt{2}}\end{pmatrix}\\ &\equiv \frac{1}{\sqrt{2}}\left(|00\rangle-|11\rangle\right),\end{aligned}\tag{14}$$

while the acts of $\mathcal{E}_2$ upon the state of $|\psi\rangle$ will result in the following state:

$$\begin{aligned}|\psi_2'\rangle &= \mathbf{ZI}|\psi\rangle\\ &= \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&-1&0\\0&0&0&-1\end{pmatrix}\cdot\begin{pmatrix}\frac{1}{\sqrt{2}}\\0\\0\\\frac{1}{\sqrt{2}}\end{pmatrix}=\begin{pmatrix}\frac{1}{\sqrt{2}}\\0\\0\\-\frac{1}{\sqrt{2}}\end{pmatrix}\\ &\equiv \frac{1}{\sqrt{2}}\left(|00\rangle-|11\rangle\right).\end{aligned}\tag{15}$$

Since the error patterns $\mathcal{E}_1 = \mathbf{IZ}$ and $\mathcal{E}_2 = \mathbf{ZI}$ yield an identical corrupted states $|\psi_1'\rangle$ and $|\psi_2'\rangle$, they undoubtly require an identical recovery procedure. Indeed, exploiting the degeneracy property may potentially increase the error correction capability of quantum codes. However, the question as to whether there exist degenerate quantum codes that are capable of operating beyond the quantum Hamming bound remains unresolved at the time of writing. Therefore, we limit our discussions in this treatise to the non-degenerate QSCs, although some research on finding the bounds of degenerate quantum codes can be found in [19], [69], and [70].

III. A BRIEF REVIEW OF QUANTUM STABILIZER CODE CONSTRUCTIONS

Let us recall the fact that qubits collapse to classical bits upon measurement [71]. This prevents us from directly transplanting the classical error correction procedures to the quantum domain. Inspired by the PCM-based syndrome decoding philosophy, the notion of QSCs was introduced in [21], where the terminology of *quantum stabilizer codes* (QSCs) represents the quantum domain counterpart of syndrome-based classical error correction codes. Almost at the same time, an independent framework of transforming classical error correction codes to QECCs was proposed in [47] and later the extended version was presented in [22]. The aforementioned proposals are similar in terms of their concept and the terminology of *quantum stabilizer codes* (QSCs) is widely recognized, unifying both framewoks. The QSCs formulation allows us to transform every PCM-based classical error correction code into its quantum counterpart. Considering that QSCs have to handle several different types of errors, namely bit-flip errors ($\mathbf{X}$), phase-flip errors ($\mathbf{Z}$), as well as both bit-flip and phase-flip errors ($i\mathbf{XZ} = \mathbf{Y}$), the PCM of $\mathcal{C}[n, k]^2$ of QSCs, in general, can be formulated as

$$\mathbf{H} = (\mathbf{H}_z|\mathbf{H}_x) \,. \tag{16}$$

The stabilizer formalism given in Eq. (16), can be interpreted as a pair of binary PCMs $\mathbf{H}_z$ and $\mathbf{H}_x$. However, a pair of $\mathbf{H}_z$ and $\mathbf{H}_x$ only can be translated into quantum stabilizer codes, if they satisfy the *symplectic criterion* given by [21], [22]

$$\mathbf{H}_z\mathbf{H}_x^T + \mathbf{H}_x\mathbf{H}_z^T = 0. \tag{17}$$

The CSS codes constitute a special class of QSCs. More specifically, the construction of a $\mathcal{C}[n, k_1 - k_2]$ CSS code, which is capable of correcting t qubit errors including the bit-flip as well as phase-flip errors, can be derived from the pair of classical linear block codes $\mathcal{C}_1(n_1, k_1)$ and $\mathcal{C}_2(n_2, k_2)$ if $\mathcal{C}_2 \subset \mathcal{C}_1$, where both $\mathcal{C}_1$ and the dual pair of $\mathcal{C}_2$,[3] denoted by $\mathcal{C}_2^\perp$, are capable of correcting t bit errors. For the CSS code constructions, the PCM $\mathbf{H}_z$ is obtained from the PCM of $\mathcal{C}_1$ invoked for handling bit-flip errors, while the the PCM $\mathbf{H}_x$ is obtained from the dual $\mathcal{C}_2^\perp$ is used for correcting the phase-flip errors. Since the phase-flip and bit-flip errors are treated separately in quantum CSS code constructions, the corresponding PCMs for stabilizer matrices of $\mathbf{H}_z$ and $\mathbf{H}_x$ are given by $\mathbf{H}_z = \begin{pmatrix} \mathbf{H}'_z \\ 0 \end{pmatrix}$ and $\mathbf{H}_x = \begin{pmatrix} 0 \\ \mathbf{H}'_x \end{pmatrix}$, respectively. Consequently, the binary PCM $\mathbf{H}$ is defined as

$$\mathbf{H} = \left(\begin{array}{c|c} \mathbf{H}'_z & \mathbf{0} \\ \mathbf{0} & \mathbf{H}'_x \end{array}\right). \tag{18}$$

Moreover, since we have $\mathcal{C}_2 \subset \mathcal{C}_1$, the symplectic criterion of Eq. (17) can be reduced to $\mathbf{H}'_z\mathbf{H}'^T_x = 0$. Furthermore, if the construction satisfies $\mathbf{H}'_z = \mathbf{H}'_x$, the resultant codes are defined as dual-containing quantum CSS codes, or self-orthogonal quantum CSS codes because $\mathbf{H}'_z\mathbf{H}'^T_z = 0$, or equivalent to $\mathcal{C}_1^\perp \subset \mathcal{C}_1$.

Again, the classical code constructions can be readily transformed into their quantum version provided that they satisfy the symplectic criterion of Eq. (17). The latter constraint prevents us from transplanting some well-known classical codes into the quantum domain. However, fortunately this limitation can be relaxed by utilizing the family of entanglement-assisted quantum stabilizer codes (EA-QSCs) [48], [49]. The luxury of being able to transform every type of classsical codes into quantum codes does not come without cost. Invoking the EA-QSC construction requires preshared maximally-entangled qubits before encoding procedure as detailed in [49]. However, the mechanism of presharing the maximally-entangled qubits allows us to transform a set of non-symplectic QSCs into their symplectic counterpart. For a crystal clear illustration, the classification and characterization of the QSCs is summarized in Fig. 3. For more a detailed history and important milestones of the QSCs field, please refer to [55] and [58].

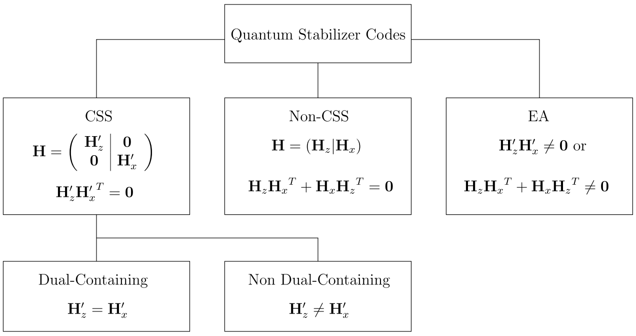

Quantum Stabilizer Codes
CSS
$\mathbf{H} = \left(\begin{array}{c|c} \mathbf{H}'_z & \mathbf{0} \\ \mathbf{0} & \mathbf{H}'_x \end{array}\right)$
$\mathbf{H}'_z\mathbf{H}'^T_x = \mathbf{0}$
Non-CSS
$\mathbf{H} = (\mathbf{H}_z|\mathbf{H}_x)$
$\mathbf{H}_z\mathbf{H}_x^T + \mathbf{H}_x\mathbf{H}_z^T = \mathbf{0}$
EA
$\mathbf{H}'_z\mathbf{H}'_x \neq \mathbf{0}$ or
$\mathbf{H}_z\mathbf{H}_x^T + \mathbf{H}_x\mathbf{H}_z^T \neq \mathbf{0}$
Dual-Containing
$\mathbf{H}'_z = \mathbf{H}'_x$
Non Dual-Containing
$\mathbf{H}'_z \neq \mathbf{H}'_x$

FIGURE 3. The classification and characterization of QSCs, where CSS stands for *Calderbank-Shor-Steane* and EA for *entanglement assisted*.

IV. PROTECTING A SINGLE QUBIT: DESIGN EXAMPLES

In Section I, we have already mentioned the three pioneering contributions on QSCs, which are only capable of handling a single qubit error, while in Section III, we briefly highlighted the different types of QSC constructions. In this section, we will link up both ideas in a more concrete context.

A. CLASSICAL AND QUANTUM 1/3-RATE REPETITION CODES

Before we delve deeper into the aforementioned QSCs, let us commence with a simple 1/3-rate classical repetition codes, which maps a binary digit of "0" or "1" into a vector that contains three replicas of each binary digit as

$$\begin{aligned} 0 &\xrightarrow{\mathbf{G}} \begin{pmatrix} 0 & 0 & 0 \end{pmatrix}, \\ 1 &\xrightarrow{\mathbf{G}} \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}. \end{aligned} \tag{19}$$

In classical codes, the mapping of information words into codewords may be described using the generator matrix $\mathbf{G}$ as encapsulated below:

$$\mathbf{y} = \mathbf{x} * \mathbf{G}, \tag{20}$$

where $\mathbf{y}$ denotes the vector of an n-bit codeword, $\mathbf{x}$ is the k-bit original information word and $*$ represents the matrix multiplication over modulo-2. Hence, the generator matrix $\mathbf{G}$ is a $(k \times n)$-element matrix, which may be decomposed into a systematic form as

$$\mathbf{G} = (\mathbf{I}_k|\mathbf{P}) \,, \tag{21}$$

where $\mathbf{I}_k$ is a $(k \times k)$ identity matrix and $\mathbf{P}$ is a $k \times (n-k)$-element matrix. The form given in Eq. (21) represents systematic linear block codes since, the codeword consists of k-bit information word followed by $(n-k)$ parity bits. Each

[2] To avoid ambiguity concerning the classical and quantum coding notation, the notation $\mathcal{C}(n, k)$ will be used to address classical codes and $\mathcal{C}[n, k]$ for quantum codes.

[3] The dual pair of the linear binary code $C_1 \subset \mathbb{F}_2^n$ is defined by a linear binary code $C_2 = \{c_2 \in \mathbb{F}_2^n | \langle c_1, c_2 \rangle = 0, \forall c_1 \in C_1\}$, where $\langle c_1, c_2 \rangle$ represents the inner product between c_1 and c_2.

generator matrix $\mathbf{G}$ corresponds to an $(n-k) \times n$-element PCM $\mathbf{H}$, which is defined as

$$\mathbf{H} = \left(\mathbf{P}^T | \mathbf{I}_{n-k}\right). \tag{22}$$

The PCM of $\mathbf{H}$ is constructed for ensuring that $\mathbf{y}$ is a valid codeword if and only if

$$\mathbf{y} * \mathbf{H}^T = \mathbf{0}. \tag{23}$$

A received word $\widehat{\mathbf{y}}$ may be contaminated by an error vector $\mathbf{e}$ due to the channel impairments, so that $\widehat{\mathbf{y}} = \mathbf{y} + \mathbf{e}$. The error syndrome $\mathbf{s}$ is a vector of length $(n-k)$ that is obtained by following calculation:

$$\begin{aligned} \mathbf{s} = \widehat{\mathbf{y}} * \mathbf{H}^T &= (\mathbf{y} + \mathbf{e}) * \mathbf{H}^T \\ &= \mathbf{y} * \mathbf{H}^T + \mathbf{e} * \mathbf{H}^T \\ &= \mathbf{0} + \mathbf{e} * \mathbf{H}^T \\ &= \mathbf{e} * \mathbf{H}^T. \end{aligned} \tag{24}$$

In simple terms, we have 2^k legitimate codewords representing k information bits, 2^n possible received bit patterns of $\widehat{\mathbf{y}}$, and $2^{(n-k)}$ syndromes of $\mathbf{s}$ each unambiguously identifying one of the $2^{(n-k)}$ error patterns, including the error-free scenario.

Hence, from this brief description of basic classical codes, the mapping in Eq. (19) can be encapsulated into a generator matrix $\mathbf{G}$ as given below:

$$\mathbf{G} = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}. \tag{25}$$

From the generator matrix $\mathbf{G}$ given in Eq. (25) and the PCM formulation given in Eq. (21), we obtain the PCM $\mathbf{H}$ for a $1/3$-rate classical repetition code encapsulated by

$$\mathbf{H} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \tag{26}$$

where the first row returns the first bit of the two bits syndrome value and acccordingly the second row evaluates the second bit. Thus, it can be easily checked by using the syndrome computation of Eq. (24) that the syndrome value of (0 0) is obtained if the received word $\widehat{\mathbf{y}}$ is equal to the valid codeword, either (0 0 0) or (1 1 1). The syndrome computation yields a syndrome vector with $(n-k)$-element and in this case for a $1/3$-rate classical repetition code, it generates a synfrome vector with two elements. Therefore, there are four possible outcomes from the syndrome computation and one of them indicates the error-free received word, which is the (0 0) syndrome. Since a $1/3$-rate classical repetition code is considered as a short block code, the syndrome computation and the associated error pattern is readily checked using a look-up table, namely Table. 1.

Next, we proceed with with a simple $1/3$-rate quantum repetition code that capable of recovering a bit-flip error. Let us assume that we have a quantum state $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$. As the consequence of the *No Cloning Theorem* of quantum mechanics, there is no unitary transformation U capable of mapping an arbitrary quantum state $|\psi\rangle$ onto a state of $|\overline{\psi}\rangle = |\psi\rangle^{\otimes 3}$. Hence, the code mapping of quantum state $|0\rangle$ and $|1\rangle$ by a unitary transformation U is defined by

TABLE 1. Syndrome computation and the associated error pattern for a 1/3-rate classical repetition code.

Syndrome (s)	Error Pattern (e)	Index of Corrupted Bit
(0 0)	(0 0 0)	-
(0 1)	(0 0 1)	3
(1 0)	(0 1 0)	2
(1 1)	(1 0 0)	1

$$\begin{aligned} |0\rangle &\rightarrow |000\rangle, \\ |1\rangle &\rightarrow |111\rangle. \end{aligned} \tag{27}$$

In a more general scenario, the mapping of k logical qubits to n physical qubits is encapsulated as follows:

$$|\psi\rangle \otimes |0\rangle^{\otimes(n-k)} \xrightarrow{U} |\overline{\psi}\rangle = \alpha_0|0\rangle_L + \alpha_1|1\rangle_L, \tag{28}$$

where $|0\rangle_L$ denotes the encoded state of the logical qubit $|0\rangle$, $|1\rangle_L$ denotes the encoded state of logical qubit $|1\rangle$, while $|0\rangle^{\otimes n-k}$ represents the auxiliary or the redundant qubits (*ancillas*), and the superscript of $\otimes$ $(n-k)$ represents $(n-k)$-fold of tensor products. Hence, for $1/3$-rate quantum repetition codes, the state of the logical qubit $|\psi\rangle$ corresponds to the state of the physical qubit $|\overline{\psi}\rangle$ as given by

$$(\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes |0\rangle^{\otimes 2} \xrightarrow{U} |\overline{\psi}\rangle = \alpha_0|000\rangle + \alpha_1|111\rangle, \tag{29}$$

where the $|000\rangle$ defines the encoded logical qubit $|0\rangle_L$ and $|111\rangle$ defines the $|1\rangle_L$. Again, it is important to bear in mind that the state of $|\overline{\psi}\rangle = \alpha_0|000\rangle + \alpha_1|111\rangle$ is not equal to $|\overline{\psi}\rangle = |\psi\rangle^{\otimes 3}$. More explicitly, this relationship can also be expressed as $|\overline{\psi}\rangle = \alpha_0|000\rangle + \alpha_1|111\rangle \neq |\psi\rangle^{\otimes 3}$. The state of the physical qubits of the $1/3$-rate quantum repetition code is stabilized, or synonymously 'parity-checked' by the pair of stabilizer operators $g_1 = \mathbf{ZZI}$ and $g_2 = \mathbf{ZIZ}$. A valid codeword or a valid encoded state, which is not affected by the stabilizer operators g_1 and g_2, has an input state of $|\overline{\psi}\rangle$ and returns the state of $|\overline{\psi}\rangle$, hence it yields the so-called eigenvalues of $+1$, and more explicitly, it is described below:

$$\begin{aligned} g_1|\overline{\psi}\rangle &= \alpha_0|000\rangle + \alpha_1|111\rangle \equiv |\overline{\psi}\rangle, \\ g_2|\overline{\psi}\rangle &= \alpha_0|000\rangle + \alpha_1|111\rangle \equiv |\overline{\psi}\rangle. \end{aligned} \tag{30}$$

By contrast, if the stabilizer operators g_1 and g_2 are applied to the corrupted states $|\widehat{\psi}\rangle$, they both yield eigenvalues that are not in the all one state. For instance, let us assume that we received a corrupted state having a bit-flip error imposed on the first qubit of $|\overline{\psi}\rangle$ yielding $|\widehat{\psi}\rangle = \alpha_0|100\rangle + \alpha_1|011\rangle$. Then, upon applying the stabilizer operators $g_1 = \mathbf{ZZI}$ and $g_2 = \mathbf{ZIZ}$ to the state of $|\widehat{\psi}\rangle$, it may be readily showed after few steps that we arrive at the following

TABLE 2. Single qubit bit-flip errors along with the associated eigenvalues in 1/3-rate quantum repetition where the eigenvalues act similarly with the syndrome values in classical linear block codes.

Received States ($\|\widehat{\psi}\rangle$)	Eigenvalue $g_1\|\widehat{\psi}\rangle$	Eigenvalue $g_2\|\widehat{\psi}\rangle$	Syndrome (s)	Index of Corrupted Qubit
$\alpha_0\|000\rangle + \alpha_1\|111\rangle$	$+1$	$+1$	(0 0)	-
$\alpha_0\|001\rangle + \alpha_1\|110\rangle$	$+1$	-1	(0 1)	3
$\alpha_0\|010\rangle + \alpha_1\|101\rangle$	-1	$+1$	(1 0)	2
$\alpha_0\|100\rangle + \alpha_1\|011\rangle$	-1	-1	(1 1)	1

eigenvalues:

$$\begin{aligned}
&g_1|\widehat{\psi}\rangle \\
&= \mathbf{ZZI}(\alpha_0|100\rangle + \alpha_1|011\rangle) \\
&= \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 0 \\ 0 \\ \alpha_1 \\ \alpha_0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \\
&= \begin{pmatrix} 0 \\ 0 \\ 0 \\ -\alpha_1 \\ -\alpha_0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \equiv -\alpha_0|100\rangle - \alpha_1|011\rangle \equiv -|\widehat{\psi}\rangle, \qquad (31)
\end{aligned}$$

$$\begin{aligned}
&g_2|\widehat{\psi}\rangle \\
&= \mathbf{ZIZ}(\alpha_0|100\rangle + \alpha_1|011\rangle) \\
&= \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 0 \\ 0 \\ \alpha_1 \\ \alpha_0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \\
&= \begin{pmatrix} 0 \\ 0 \\ 0 \\ -\alpha_1 \\ -\alpha_0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \equiv -\alpha_0|100\rangle - \alpha_1|011\rangle \equiv -|\widehat{\psi}\rangle. \qquad (32)
\end{aligned}$$

The resultant eigenvalues of ±1 act similarly to the syndrome vector of classical codes, where the eigenvalue +1 is associated with the classical syndrome value 0 and the eigenvalue −1 with the classical syndrome value 1. More explicitly, the single qubit error patterns imposed on the 1/3-rate quantum repetition codes and the associated eigenvalues are portrayed in Table. 2. However, this specific construcion is only capable of detecting and correcting a single bit-flip error imposed by the Pauli channel on the physical qubits, but no phase-flips.

Since the physical qubits may experience not only bit-flip errors, but also phase-flip errors as well as both bit-flip and phase-flip errors, different mapping is necessitated to protect the physical qubits from phase-flip error. In order to protect the physical qubits from a phase-flip error, we may require a different basis but we can still invoke a similar approach. To elaborate further, the Hadamard transformation (**H**) maps the computational basis of $\{|0\rangle, |1\rangle\}$ onto the Hadamard basis of $\{|+\rangle, |-\rangle\}$, where the state of $|+\rangle$ and $|-\rangle$ are defined as

$$|+\rangle \equiv \mathbf{H}|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \qquad (33)$$

$$|-\rangle \equiv \mathbf{H}|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \qquad (34)$$

and the unitary Hadamard transformation **H**, which acts on a single qubit state, is given by

$$\mathbf{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \qquad (35)$$

A phase-flip error defined over the Hadamard basis of $\{|+\rangle, |-\rangle\}$ acts similarly to the bit-flip error defined over the computational basis of $\{|0\rangle, |1\rangle\}$. Hence, for handling of a single phase-flip error, the code mapping of 1/3-rate quantum repetition codes are given by

$$\begin{aligned} |0\rangle &\rightarrow |+++\rangle, \\ |1\rangle &\rightarrow |---\rangle. \end{aligned} \qquad (36)$$

Hence, the logical qubit of $|\psi\rangle$ corresponding to the physical qubits $|\overline{\psi}\rangle$ is given by

$$|\psi\rangle \otimes |0\rangle^{\otimes 2} \xrightarrow{U} |\overline{\psi}\rangle = \alpha_0|+++\rangle + \alpha_1|---\rangle. \qquad (37)$$

The state of physical qubits given in Eq. (37) can be stabilized by the operators $g_1 = \mathbf{XXI}$ and $g_2 = \mathbf{XIX}$. The detection and correction of a phase flip error can be carried out in analogy with the 1/3-rate quantum repetition code for handling the bit-flip error.

As seen in Eq. (16), the stabilizer operators can be derived from the classical PCM **H** by mapping the Pauli

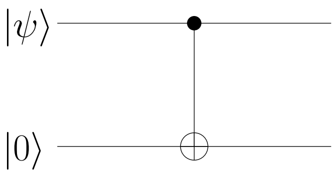


FIGURE 4. The circuit representation of the CNOT unitary transformation.

matrices **I**, **X**, **Y** and **Z** onto $(\mathbb{F}_2)^2$ as follows:

$$\begin{aligned}\mathbf{I} &\rightarrow \left(0 \quad | \quad 0\right),\\ \mathbf{X} &\rightarrow \left(0 \quad | \quad 1\right),\\ \mathbf{Y} &\rightarrow \left(1 \quad | \quad 1\right),\\ \mathbf{Z} &\rightarrow \left(1 \quad | \quad 0\right).\end{aligned} \tag{38}$$

Each row of **H** is associated with a stabilizer operator $g_i \in \mathcal{H}$, where the i-th column of both $\mathbf{H}_z$ and $\mathbf{H}_x$ corresponds to the i-th qubit and the binary 1 locations represent the **Z** and **X** positions in the PCMs $\mathbf{H}_z$ and $\mathbf{H}_x$, respectively. For instance, for the $1/3$-rate quantum repetition code, which is stabilized by the operators $g_1 = \mathbf{ZZI}$ and $g_2 = \mathbf{ZIZ}$, the PCM **H** is given as follows:

$$\mathbf{H} = \left(\begin{array}{ccc|ccc} 1 & 1 & 0 & 0 & 0 & 0\\ 1 & 0 & 1 & 0 & 0 & 0\end{array}\right). \tag{39}$$

Since the $1/3$-rate quantum repetition code in this example can only correct a bit-flip (**X**) error, which is stabilized by the **Z** operators, the PCM $\mathbf{H}_x$ contains only zero elements. The same goes for a $1/3$-rate quantum repetition code conceived for handling a phase-flip (**Z**) error, which is stabilized by the operators $g_1 = \mathbf{XXI}$ and $g_2 = \mathbf{XIX}$. The PCM **H** corresponding to this particular QSC is defined as follows:

$$\mathbf{H} = \left(\begin{array}{ccc|ccc} 0 & 0 & 0 & 1 & 1 & 0\\ 0 & 0 & 0 & 1 & 0 & 1\end{array}\right). \tag{40}$$

It is clearly shown in Eq. (39) and (40) that the PCM of a $1/3$-rate quantum repetition code is similar to that of the $1/3$-rate classical repetition code given in Eq. (26).

In order to encode the logical qubits into physical qubits, we require the unitary transformation U acting as the quantum encoding circuit. To represent the quantum encoding circuit, one of the essential components is the controlled-NOT (CNOT) quantum gate. A CNOT quantum gate manipulates the state of a two-qubit system and it can be represented by a unitary transformation as follows:

$$\mathbf{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{pmatrix}. \tag{41}$$

The circuit representation of the CNOT quantum gate is depicted in Fig 4, which manipulates the state of two qubits and it can be formulated as follows:

$$\mathbf{CNOT}(|a_0, a_1\rangle) \equiv |a_0, (a_0 \oplus a_1)\rangle, \tag{42}$$

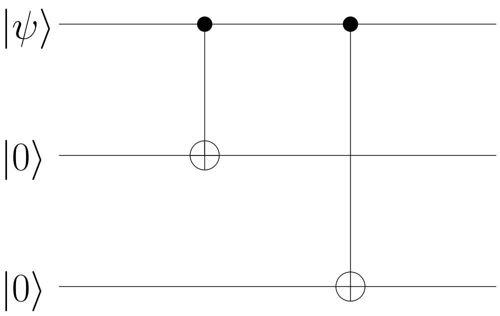


FIGURE 5. The encoding circuit of the 1/3-rate quantum repetition code protecting the physical qubits from a bit-flip error.

where the notation of $\oplus$ represents the modulo-2 addition. For instance, by using the CNOT representation in Eq. (41), a logical qubit in the superimposed state of $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ and a qubit in the pure state of $|0\rangle$ are manipulated by the quantum CNOT gate into following state:

$$\begin{aligned}\mathbf{CNOT}(|\psi\rangle, |0\rangle) &= \mathbf{CNOT}(\alpha_0|0\rangle + \alpha_1|1\rangle, |0\rangle)\\ &= \mathbf{CNOT}(\alpha_0|00\rangle + \alpha_1|10\rangle)\\ &= \begin{pmatrix} 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{pmatrix} \cdot \begin{pmatrix}\alpha_{00}\\ 0\\ \alpha_{10}\\ 0\end{pmatrix}\\ &= \begin{pmatrix}\alpha_0\\ 0\\ 0\\ \alpha_1\end{pmatrix} \equiv \alpha_0|00\rangle + \alpha_1|11\rangle.\end{aligned} \tag{43}$$

Similarly, we may also use the CNOT definition given in Eq. (42) to determine the resultant state as described below:

$$\begin{aligned}\mathbf{CNOT}(|\psi\rangle, |0\rangle) &= \mathbf{CNOT}(\alpha_0|0\rangle + \alpha_1|1\rangle, |0\rangle)\\ &= \mathbf{CNOT}(\alpha_0|00\rangle + \alpha_1|10\rangle)\\ &= \alpha_0|0, (0 \oplus 0)\rangle + \alpha_1|1, (1 \oplus 0)\rangle\\ &= \alpha_0|00\rangle + \alpha_1|11\rangle.\end{aligned} \tag{44}$$

In this configuration, the first qubit is referred to as the *control qubit*, while the second one is referred to as the *target qubit*. The value of the target qubit is flipped if the value of the control qubit is equal to "1". We can observe that the CNOT quantum gate behaves similarly to the exclusive OR (XOR) gate of the classical computer.

For the sake of creating the encoded state of $1/3$-rate quantum repetition code, we require a single logical qubit and two ancillas prepared in the pure state of $|0\rangle$, as described in Eq. (29). In the first step, the CNOT unitary transformation is performed between the logical qubit and the first ancilla, in which the logical qubit acts as the control qubit and the ancilla as the target qubit. The same step is repeated during the second stage between the logical qubit and the second ancilla, where the second ancilla is also preserved as the target qubit. Therefore, the encoding circuit of the $1/3$-rate quantum repetition code can be represented as in Fig 5, which was

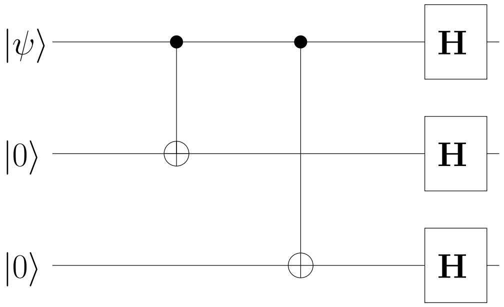


FIGURE 6. The encoding circuit of the 1/3-rate quantum repetition code protecting the physical qubits from a phase-flip error.

designed for protecting the physical qubits from a single bit-flip error, as also seen in the mapping given in Eq. (27). For its 1/3-rate quantum repetition code counterpart protecting the physical qubits from a phase-flip error, we require the Hadamard transformation to obtain the mapping given in Eq. (36). Hence, we can readily create the encoding circuit for a 1/3-rate quantum repetition code for protecting the physical qubits from a phase-flip error by placing the Hadamard transformations after the second stage as portrayed in Fig. 6.

B. SHOR's 9-QUBIT CODE

Since, we have elaborated briefly on the construction of QSCs along with the Pauli to binary isomorphism, we may now proceed with the corresponding examples of different QSC constructions conceived for protecting the physical qubits from any type of a single qubit error. Firstly, we start with the Shor's code [16]. In order to protect the qubits from any type of single qubit error, a logical qubit is mapped onto nine physical qubits. This code may also be viewed as a concatenated version of two 1/3-rate quantum repetition codes, where the first stage is dedicated to the protection of the physical qubits from phase-flip errors, while the second stage is invoked for handling the bit-flip errors. To elaborate further, at the first stage of Shor's code, the state of a logical qubit is encoded by using the following mapping: $|0\rangle \rightarrow |{+}{+}{+}\rangle$, $|1\rangle \rightarrow |{-}{-}{-}\rangle$. At the second stage, we encode each of the states of $|+\rangle$ to the state of $(|000\rangle + |111\rangle)/\sqrt{2}$, while the state of $|-\rangle$ is mapped to the state of $(|000\rangle - |111\rangle)/\sqrt{2}$. Therefore, the final state of the encoded logical qubits $|0\rangle_L$ and $|1\rangle_L$ are encapsulated as follows:

$$\begin{aligned}|0\rangle_L &= \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \otimes \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)\\ &\quad \otimes \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)\\ &= \frac{1}{2\sqrt{2}}(|000000000\rangle + |000000111\rangle + |000111000\rangle\\ &\quad + |000111111\rangle + |111000000\rangle + |111000111\rangle\\ &\quad + |111111000\rangle + |111111111\rangle), \qquad (45)\\ |1\rangle_L &= \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle) \otimes \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)\\ &\quad \otimes \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)\\ &= \frac{1}{2\sqrt{2}}(|000000000\rangle - |000000111\rangle - |000111000\rangle\\ &\quad + |000111111\rangle - |111000000\rangle + |111000111\rangle\\ &\quad + |111111000\rangle - |111111111\rangle). \qquad (46)\end{aligned}$$

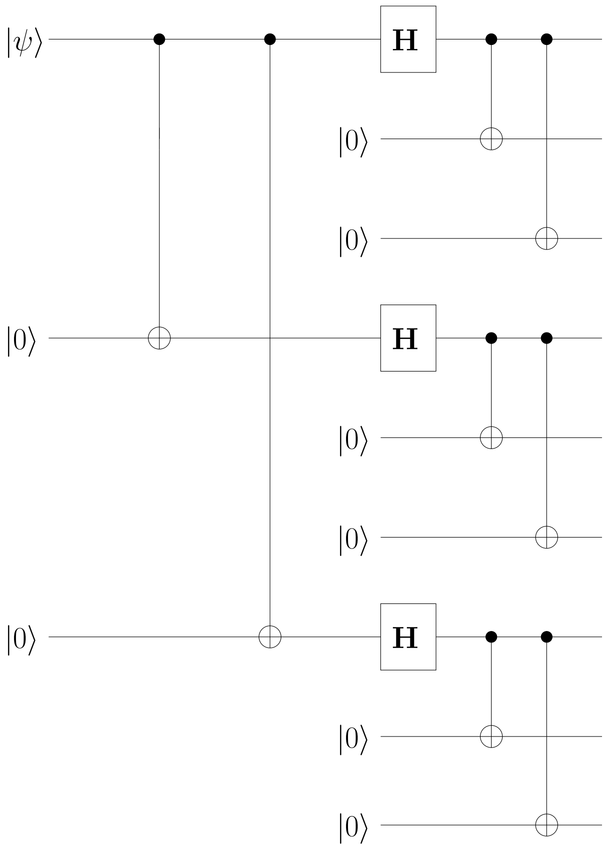


FIGURE 7. The encoding circuit of Shor's 9-qubit code.

TABLE 3. The eight stabilizer operators g_1 to g_8 of Shor's 9-qubit code, which stabilizes a single logical qubit with the aid of eight auxiliary qubits.

g_i	Stabilizer Operator
g_1	ZZIIIIIII
g_2	IZZIIIIII
g_3	IIIZZIIII
g_4	IIIIZZIII
g_5	IIIIIIZZI
g_6	IIIIIIIZZ
g_7	XXXXXXIII
g_8	IIIXXXXXX

Based on the given description, the encoding circuit of Shor's code is portrayed in Fig. 7. The state determined by the nine physical qubits of Shor's code, where the latter defined in Eq. (45) and (46), is stabilized by the eight stabilizer operators which are listed in Table 3.

To elaborate a little further, Shor's code is a member of the class of non-dual-containing CSS codes. Explicitly, it belongs to the class of CSS codes because the stabilizer formalism of Shor's code implies that the code handles the **Z** error and the **X** error separately, whilst it is a non-dual-containing because the PCMs $\mathbf{H}_z$ and $\mathbf{H}_x$ are not identical. Based on the list of stabilizer operators given in Table 3, the PCM **H** of Shor's code is given in Eq. (47), as shown at the bottom of this page, where each row of the PCM corresponds to each of the stabilizer operators listed in Table 3.

The quantum coding rate (r_Q) of a quantum code $\mathcal{C}[n,k]$ is defined by the ratio of the number of logical qubits k to the number of physical qubits n, which can be formulated as

$$r_Q = \frac{k}{n}. \tag{48}$$

Hence again, for a Shor's 9-qubit code the quantum coding rate is $r_Q = 1/9$.

C. STEANE's 7-QUBIT CODE

Steane's code was proposed to protect a single qubit from any type of error by mapping a logical qubit onto seven physical qubits, instead of nine qubits. In contrast to Shor's code, Steane's code is a dual-containing CSS code, since the PCMs $\mathbf{H}_z$ and $\mathbf{H}_x$ are equal to that of clasical Hamming code $\mathbf{H}_{Ham}$, which is given by

$$\mathbf{H}_{Ham} = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}. \tag{49}$$

It can be confimed that the classical Hamming code is a dual-containing code, because it satisfies the condition $\mathbf{H}_{Ham}.\mathbf{H}^T_{Ham} = 0$. Therefore, the PCM **H** of Steane's code is defined as shown in Eq. (50), as shown at the bottom of this page.

Since Steane's code is a member of the dual-containing CSS codes, the encoded state of the logical qubit $|0\rangle_L$ and $|1\rangle_L$ may be determined from its classical code counterpart. Let $\mathcal{C}_1(7,4)$ be the Hamming code and $\mathcal{C}_2(7,3)$ be its dual. Both of the codes are capable of corrrecting one bit error.

TABLE 4. The code space of $\mathcal{C}_1$ and $\mathcal{C}_2$ for determining the encoded state of the Steane's code.

$x \in \mathcal{C}_1, \mathcal{C}_2$	$x \in \mathcal{C}_1, x \notin \mathcal{C}_2$
0000000	1111111
0111001	1000110
1011010	0100101
1100011	0011100
1101100	0010011
1010101	0101010
0110110	1001001
0001111	1110000

Hence, the resultant CSS quantum code derived from these codes, namely the $\mathcal{C}[n, k_1 - k_2] = \mathcal{C}[7,1]$, also capable of correcting a single qubit error. For Steane's code the states of encoded logical qubit of $|0\rangle_L$ and $|1\rangle_L$ are defined as follows:

$$|0\rangle_L = \frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{x \in \mathcal{C}_1, \mathcal{C}_2} |x\rangle, \tag{51}$$

$$|1\rangle_L = \frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{x \in \mathcal{C}_1, x \notin \mathcal{C}_2} |x\rangle. \tag{52}$$

Since $\mathcal{C}_2$ is the dual of $\mathcal{C}_1$, by definition the PCM of $\mathcal{C}_2$, denoted by $\mathbf{H}(\mathcal{C}_2)$ is the generator matrix of $\mathcal{C}_1$, denoted by $\mathbf{G}(\mathcal{C}_1)$. Hence, the parity-check matrix of $\mathcal{C}_2$ can be written as

$$\mathbf{H}(\mathcal{C}_2) = \mathbf{G}(\mathcal{C}_1) = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}. \tag{53}$$

Based on the PCM given in Eq. (49) and (53), we can define the code space of $\mathcal{C}_1$ and $\mathcal{C}_2$, which is described in Table 4. Finally, using Eq. (51), (52), and also the code space given in Table 4, the encoded states of the logical qubit $|0\rangle_L$

$$\mathbf{H}_{Shor} = \left(\begin{array}{ccccccccc|ccccccccc} 1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1 \end{array}\right). \tag{47}$$

$$\mathbf{H}_{Steane} = \left(\begin{array}{c|c} \mathbf{H}_{Ham} & \mathbf{0} \\ \mathbf{0} & \mathbf{H}_{Ham} \end{array}\right) = \left(\begin{array}{ccccccc|ccccccc} 1&1&0&1&1&0&0&0&0&0&0&0&0&0 \\ 1&0&1&1&0&1&0&0&0&0&0&0&0&0 \\ 0&1&1&1&0&0&1&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&1&1&0&1&1&0&0 \\ 0&0&0&0&0&0&0&1&0&1&1&0&1&0 \\ 0&0&0&0&0&0&0&0&1&1&1&0&0&1 \end{array}\right). \tag{50}$$

TABLE 5. The stabilizer formalism of the Steane's 7-qubit code.

g_i	Stabilizer Operator
g_1	**ZZIZZII**
g_2	**ZIZZIZI**
g_3	**IZZZIIZ**
g_4	**XXIXXII**
g_5	**XIXXIXI**
g_6	**IXXXIIX**

TABLE 6. The stabilizer formalism of the perfect 5-qubit code.

g_i	Stabilizer Operator
g_1	**XZZXI**
g_2	**IXZZX**
g_3	**XIXZZ**
g_4	**ZXIXZ**

and $|1\rangle_L$ of the Steane's code are as follows:

$$\begin{aligned} |0\rangle_L = \frac{1}{2\sqrt{2}}(&|0000000\rangle + |0111001\rangle + |1011010\rangle \\ &+ |1100011\rangle + |1101100\rangle + |1010101\rangle \\ &+ |0110110\rangle + |0001111\rangle), \end{aligned} \tag{54}$$

$$\begin{aligned} |1\rangle_L = \frac{1}{2\sqrt{2}}(&|1111111\rangle + |1000110\rangle + |0100101\rangle \\ &+ |0011100\rangle + |0010011\rangle + |0101010\rangle \\ &+ |1001001\rangle + |1110000\rangle). \end{aligned} \tag{55}$$

It can be readily seen that the quantum coding rate of Steane's 7-qubit code is $1/7$. The encoding circuit of the Steane's $1/7$-rate code can be found in [72].

D. LAFLAMME's 5-QUBIT CODE - THE PERFECT CODE

Laflamme's code maps a single logical qubit onto a five physical qubits. Laflamme's code is also referred to as the "perfect code", because it has been proven that in order to protect a logical qubit, the lowest number of physical qubits required is five [19], [20]. The perfect 5-qubit code is a non-CSS code, since the stabilizer formalism is designed to handle the **Z** errors and **X** errors simultaneously. There are several existing designs related to the perfect 5-qubit code [18], [71] and in this treatise, we use the PCM formulation given in [71]. Explicitly, its non-CSS characteristics can be readily observed from the PCM $\mathbf{H}_{perfect}$ of the 5-qubit perfect code, which is specified as follows:

$$\mathbf{H}_{perfect} = \left(\begin{array}{ccccc|ccccc} 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{array}\right). \tag{56}$$

TABLE 7. List of valid stabilizer operators for determining the encoded state of the 5-qubit code.

Stabilizer	State	Stabilizer	State
g_0	$\|00000\rangle$	g_2g_3	$-\|11101\rangle$
g_1	$\|10010\rangle$	g_2g_4	$-\|00011\rangle$
g_2	$\|01001\rangle$	g_3g_4	$-\|11110\rangle$
g_3	$\|10100\rangle$	$g_1g_2g_3$	$-\|01111\rangle$
g_4	$\|01010\rangle$	$g_1g_2g_4$	$-\|10001\rangle$
g_1g_2	$-\|11011\rangle$	$g_1g_3g_4$	$-\|01100\rangle$
g_1g_3	$-\|00110\rangle$	$g_2g_3g_4$	$-\|10111\rangle$
g_1g_4	$-\|11000\rangle$	$g_1g_2g_3g_4$	$\|00101\rangle$

Hence, the stabilizer operators of the 5-qubit code may be explicitly formulated as in Table 6. In general, the states of encoded logical qubit of QSCs are defined as follows:

$$|0\rangle_L = \sum_{g_i \in \mathcal{S}} g_i |0\rangle^{\otimes N}, \tag{57}$$

$$|1\rangle_L = \overline{\mathbf{X}}|0\rangle_L. \tag{58}$$

The stabilizers $g_i \in \mathcal{S}$ includes all the valid stabilizer operators of the quantum code $\mathcal{C}$, which covers not only the stabilizer operators that are listed in Table 6. Because of the commutative property of the stabilizer formalism, the product of any two stabilizer operators generates another valid stabilizer operator. Table 7 provides a list of all the possible combinations of the stabilizer operators, which includes the stabilizer operator of $g_0 = \mathbf{IIIII}$, and also the respective transformation upon the state of $|0\rangle^{\otimes 5} = |00000\rangle$. The notation of $\overline{\mathbf{X}}$ denotes the logical operator $\mathbf{X}$. Explicitly, in this case for the 5-qubit code the logical operator representing the encoded state of the logical qubit is $\overline{\mathbf{X}} = \mathbf{XXXXX}$. The logical operator is represented by an N-fold application of Pauli matrices that commutes with all stabilizer operators, but it is not a part of the set of valid stabilizer operators $\mathcal{S}$. The resultant quantum coding rate of the 5-qubit code is $r_Q = 1/5$. The encoded state mapping for the 5-qubit quantum code based on the Eq. (57), (58). Hence, the corresponding states, which are described in Table 7, are defined below:

$$\begin{aligned} |0\rangle_L = \frac{1}{4}(&|00000\rangle + |10010\rangle + |01001\rangle + |10100\rangle \\ &+ |01010\rangle - |11011\rangle - |00110\rangle - |11000\rangle \\ &- |11101\rangle - |00011\rangle - |11110\rangle - |01111\rangle \\ &- |10001\rangle - |01100\rangle - |10111\rangle + |00101\rangle), \end{aligned} \tag{59}$$

$$\begin{aligned} |1\rangle_L = \frac{1}{4}(&|11111\rangle + |01101\rangle + |10110\rangle + |01011\rangle \\ &+ |10101\rangle - |00100\rangle - |11001\rangle - |00111\rangle \\ &- |00010\rangle - |11100\rangle - |00001\rangle - |10000\rangle \\ &- |01110\rangle - |10011\rangle - |01000\rangle + |11010\rangle). \end{aligned} \tag{60}$$

The same method can be utilized for determining the encoded state of logical qubit for Shor's code and Steane's code. However, both Shor's code and Steane's code offer a more simplistic approach for determining their corresponding encoded states. The description for the efficient encoding circuit of the $1/5$-rate Laflamme's code can be found in [18], [73], and [74].

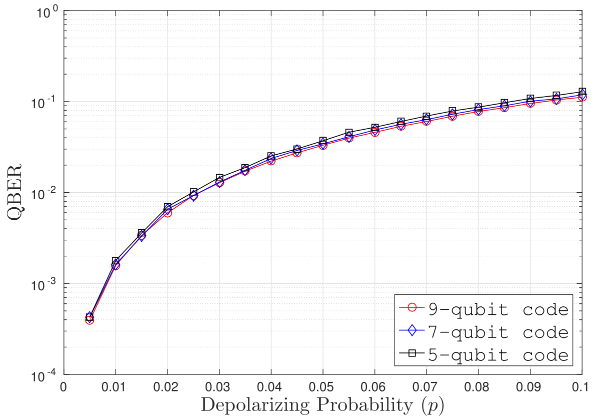


FIGURE 8. **QBER performance of the QSCs protecting a single qubit, namely Shor's 9-qubit code, Steane's 7-qubit code, and the perfect 5-qubit code, recorded for the quantum depolarizing channel. The similarity of performances is due to the fact that all of the QSCs rely on hard-decision syndrome decoding and they all have the same error correction capabilities.**

Based on the aforementioned constructions, we evaluated the performance of the QSCs by simulation, in the context of quantum depolarizing channel. The performance of 9-qubit Shor's code, 7-qubit Steane's code and 5-qubit Laflamme's code are portrayed in Fig. 8 in terms of the qubit error rate (QBER) on given depolarizing probability (p). From the simulation result, it can be observed clearly that the performance of all three QSCs are quite similar. The similarity in performances are expected because all of the codes have the same error correction capability of correcting single qubit error. In addition, they utilize the hard decision decoding based on syndrome measurement. From this result, we may conclude that for different codes with the same error correction capability, where in classical coding theory it will be translated into the minimum distance property, they are associated with similar performances eventhough all of the codes have different codeword length. In this case, all of the QSCs have a single qubit error correction capability ($t = 1$), and it may be translated as the minimum distance of three ($d = 3$), but having different codeword length, 9-qubit, 7-qubit and 5-qubit for Shor's code, Steane's code and Laflamme's code, respectively. Another fact that we should point out that the three codes exhibit different code constructions. Shor's code belongs to non dual-containing CSS codes, while Steane's code is a member of dual-containing CSS codes, and finally, Laflamme's code or the perfect 5-qubit code has a construction of non-CSS codes.

V. ON CLASSICAL TO QUANTUM CODING BOUNDS

In this section, we present the classical to quantum transformation of the most well-known coding bounds, namely the Singleton bound [75] and Hamming bound [76], which serve as the upper bounds, as well as the Gilbert-Varshamov (GV) bound [77], which acts as the lower bound. Although, there are several ways of deriving the coding bounds in the quantum domain, we are interested exploring the duality of coding bounds in classical and quantum domain. Therefore, we present the derivation of quantum coding bounds using the classical to quantum isomorphism approach and demonstrate that the final results agree with the coding bounds that are derived from a purely quantum domain perspective.

A. SINGLETON BOUND

The Singleton bound of classical binary code constructions $\mathcal{C}(n,k)$ is defined as

$$n - k \geq d - 1, \tag{61}$$

where the notation n denotes the codeword length, k for the length of information bits, and d for minimum distance amongst the codewords in codebook $\mathcal{C}$. Singleton bound acts as an upper bound in classical code constructions. The bound implies that the number of rows in a PCM associated with the length of syndrome vector, which is equal to $(n-k)$, has to be greater than $(d-1)$. For the QSC $\mathcal{C}[n,k]$, the rows of PCM correspond to the number stabilizer operators. Since the stabilizer formalism has to correct both the bit-flip errors and the phase-flip errors, the classical Singleton bound of Eq. (61) can be readily transformed into the quantum Singleton bound as follows:

$$n - k \geq 2(d-1), \tag{62}$$

where n now may also be referred to as the number of physical qubits and k as the number of logical qubits. In order to show explicitly the trade-off between the minimum distance and the quantum coding rate, Eq. (62) can be modified to

$$\frac{k}{n} \leq 1 - 2\left(\frac{d-1}{n}\right). \tag{63}$$

In the quantum domain, the Singleton bound is also known as the Knill-Laflamme bound [78]. The QSCs achieving the quantum Singleton bound by satisfying the equality are classified as the quantum Maximum Separable Distance (MDS) codes. One of the well-known QSCs having a minimum distance $d = 3$ that reaches the quantum Singleton bound is the perfect 5-qubit code $\mathcal{C}[n,k,d] = \mathcal{C}[5,1,3]$.

B. HAMMING BOUND

In classical binary coding, a codebook $\mathcal{C}(n,k)$ maps the information words containing k bits into a codeword of length n bits. The maximal number of errors, which is denoted by t that can be corrected by codebook $\mathcal{C}$ is given by

$$t = \lfloor \frac{d-1}{2} \rfloor. \tag{64}$$

Therefore the maximum size of a binary codebook $|\mathcal{C}| = 2^k$ is bounded by the sphere-packing bound which is defined as:

$$2^k \leq \frac{2^n}{\sum\limits_{j=0}^{t=\lfloor \frac{d-1}{2} \rfloor} \binom{n}{j}}. \tag{65}$$

Since the QSCs have to correct three different types of error namely the bit-flip errors ($\mathbf{X}$), phase-flip errors ($\mathbf{Z}$), as well as both bit-flip and phase-flip errors ($\mathbf{Y}$), the size of the codebook for a quantum code $\mathcal{C}[n, k]$ is now bounded by

$$2^k \leq \frac{2^n}{\sum_{j=0}^{t=\lfloor \frac{d-1}{2} \rfloor} \binom{n}{j} 3^j}. \tag{66}$$

By modifying Eq. (66), we can express explicitly the bound of the quantum coding rate as a function of the minimum distance d and codeword length n, as shown below:

$$\frac{k}{n} \leq 1 - \frac{1}{n} \log_2 \left(\sum_{j=0}^{t=\lfloor \frac{d-1}{2} \rfloor} \binom{n}{j} 3^j \right). \tag{67}$$

If n tends to ∞, we obtain

$$\frac{k}{n} \leq 1 - \left(\frac{d}{2n}\right) \log_2 3 - H\left(\frac{d}{2n}\right), \tag{68}$$

where $H(x)$ is the binary entropy of x formulated as $H(x) = -x \log_2 x - (1-x)\log_2(1-x)$. Equation (67) and (68) are also known as the quantum Hamming bound [20], which also constitutes the upper bound of quantum code constructions.

C. GILBERT-VARSHAMOV BOUND

The same analogy exploited to derive the quantum Hamming bound may also be used for transforming the classical Gilbert-Varshamov (GV) bound, namely the lower bound for classical code constructions, into its quantum counterpart. In the classical domain, the GV bound is formulated as

$$2^k \geq \frac{2^n}{\sum_{j=0}^{d-1} \binom{n}{j}}. \tag{69}$$

Considering that the quantum codes have to tackle three different types of errors, the size of the codebook $\mathcal{C}[n, k]$ is bounded by

$$2^k \geq \frac{2^n}{\sum_{j=0}^{d-1} \binom{n}{j} 3^j}. \tag{70}$$

Hence, we can readily derive the quantum GV bound, the lower bound of the quantum coding rate as a function of the minimum distance d and codeword length n as follows:

$$\frac{k}{n} \geq 1 - \frac{1}{n} \log_2 \left(\sum_{j=0}^{d-1} \binom{n}{j} 3^j \right). \tag{71}$$

Again, if n aprroaches ∞, we obtain

$$\frac{k}{n} \geq 1 - \left(\frac{d}{n}\right) \log_2 3 - H\left(\frac{d}{n}\right), \tag{72}$$

where $H(x)$ is the binary entropy of x. The quantum GV bounds in Eq. (71) and (72) are valid for non-CSS QSCs. However, a special case should be considered for dual-containing quantum CSS codes. It will be shown in Section VII that for some dual-containing CSS codes the code constructions violate the quantum GV bound. Hence, a special bound has to be derived to accomodate the dual-containing CSS codes. In the classical domain, a binary code $\mathcal{C}(n, k)$ maps a k-bit information word into an n-bit encoded codeword. The number of syndrome measurement operators is determined by the number of rows in the parity-check matrix $\mathcal{C}(n, k)$, which is equal to $(n-k)$. With a simple modification of Eq. (69), the number of syndrome measurement operators in $\mathcal{C}(n, k)$ is bounded by

$$2^{(n-k)} \leq \left(\sum_{j=0}^{d-1} \binom{n}{j} \right). \tag{73}$$

Recall that the dual-containing quantum CSS codes rely on dual-containing classical binary codes, which satisfy the symplectic criterion of Eq. (17) and also comply with the constraint of $\mathbf{H}_z = \mathbf{H}_x$. Explicitly, half portion of the stabilizer operators of $\mathcal{C}[n, k]$ are mapped onto $\mathbf{H}_z$, while the other half are mapped onto $\mathbf{H}_x$. Therefore, the number of the stabilizer operators of a dual-containing quantum CSS code are bounded by

$$2^{\frac{(n-k)}{2}} \leq \left(\sum_{j=0}^{d-1} \binom{n}{j} \right). \tag{74}$$

Based on Eq. (74), we may formulate the lower bound on the quantum coding rate of a dual-containing quantum CSS code as follows:

$$\frac{k}{n} \geq 1 - \frac{2}{n} \log_2 \left(\sum_{j=0}^{d-1} \binom{n}{j} \right). \tag{75}$$

As n approaches ∞, we obtain the quantum GV bound for CSS codes, as suggested in [66], which is formulated as

$$\frac{k}{n} \geq 1 - 2H\left(\frac{d}{n}\right), \tag{76}$$

where $H(x)$ is the binary entropy of x. Based on the discussions above, we compare the asymptotic classical and quantum coding bounds in Table. 8 as well as in Fig. 9. Since the QSCs are designed to mitigate both bit-flip errors as well as phase-flip errors, the bounds of QSCs are significantly lower than those of their classical counterparts. Nevertheless, the general conception still holds, the Singleton bound serves as the loose upper bound, whilst the Hamming bound is the tighter upper bound.

VI. QUANTUM CODING BOUNDS ON ASYMPTOTICAL LIMIT

Although the classical to binary isomorphism assists us in the development of QSCs from the well-known classical code designs, the issue of determining the actual achieavable minimum distance, given the coding rate and the codeword length still remains unresolved. In the classical domain as we described previously, finding the unique solution to the realistically achievable minimum distance of binary classical codes is still an open problem, even though the upper

TABLE 8. Comparison of various classical and quantum coding bounds.

Coding Bound	Asymptotic	
	Classical	Quantum
Singleton	$\frac{k}{n} \leq 1 - \left(\frac{d}{n}\right)$	$\frac{k}{n} \leq 1 - 2\left(\frac{d}{n}\right)$
Hamming	$\frac{k}{n} \leq 1 - H\left(\frac{d}{2n}\right)$	$\frac{k}{n} \leq 1 - \left(\frac{d}{2n}\right)\log_2 3 - H\left(\frac{d}{2n}\right)$
GV	$\frac{k}{n} \geq 1 - H\left(\frac{d}{n}\right)$	$\frac{k}{n} \geq 1 - \left(\frac{d}{n}\right)\log_2 3 - H\left(\frac{d}{n}\right)$
Coding Bound	Finite-length	
	Classical	Quantum
Singleton	$\frac{k}{n} \leq 1 - \left(\frac{d-1}{n}\right)$	$\frac{k}{n} \leq 1 - 2\left(\frac{d-1}{n}\right)$
Hamming	$\frac{k}{n} \leq 1 - \frac{1}{n}\log_2\left(\sum_{j=0}^{t=\lfloor\frac{d-1}{2}\rfloor}\binom{n}{j}\right)$	$\frac{k}{n} \leq 1 - \frac{1}{n}\log_2\left(\sum_{j=0}^{t=\lfloor\frac{d-1}{2}\rfloor}\binom{n}{j}3^j\right)$
GV	$\frac{k}{n} \geq 1 - \frac{1}{n}\log_2\left(\sum_{j=0}^{d-1}\binom{n}{j}\right)$	$\frac{k}{n} \geq 1 - \frac{1}{n}\log_2\left(\sum_{j=0}^{d-1}\binom{n}{j}3^j\right)$

TABLE 9. The coding bounds for classical code constructions, with a minor modification from [65].

Classical Coding Bound	**Finite**	**Asymptotic**	**Notes**
Singleton [75]	$\frac{k}{n} \leq 1 - \left(\frac{d-1}{n}\right)$	$\frac{k}{n} \leq 1 - \left(\frac{d}{n}\right)$	a loose upper bound
Hamming [76]	$\frac{k}{n} \leq 1 - \frac{1}{n}\log_2\left(\sum_{j=0}^{t=\lfloor\frac{d-1}{2}\rfloor}\binom{n}{j}\right)$	$\frac{k}{n} \leq 1 - H\left(\frac{d}{2n}\right)$	tight upper bound for very high code rate
MRRW [79]		$\frac{k}{n} \leq H\left(\frac{1}{2} - \sqrt{\frac{d}{n}\left(1 - \frac{d}{n}\right)}\right)$	tightest known asymptotic upper bound for medium and low rate codes
Plotkin [80]	$\frac{k}{n} \leq \frac{1}{n}\left(1 - \log_2\left(2 - \frac{n}{d}\right)\right)$		tight upper bound for finite-length at $\delta > \frac{1}{2}$
GV [77]	$\frac{k}{n} \geq 1 - \frac{1}{n}\log_2\left(\sum_{j=0}^{d-1}\binom{n}{j}\right)$	$\frac{k}{n} \geq 1 - H\left(\frac{d}{n}\right)$	tightest known lower bound

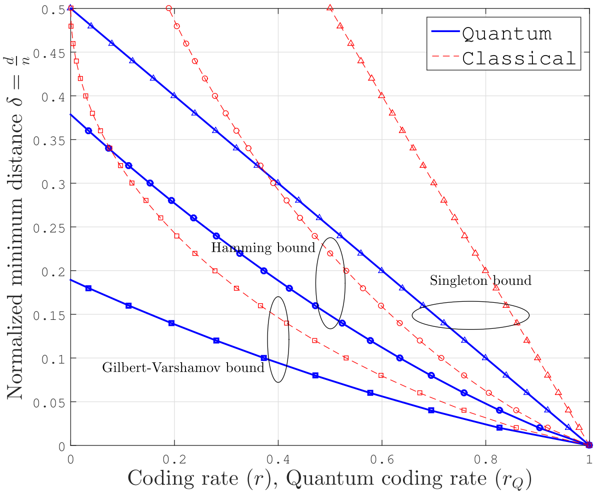


FIGURE 9. The evolution from asymptotic classical binary coding bounds to the asymptotic quantum coding bounds.

bound and lower bound of the quantum coding rate versus the achievable minimum distance can be found in the literature [75]–[77], [79], [80]. The bounds for the classical code constructions are listed in Table. 9, while the corresponding asymptotic bounds are also plotted in Fig. 10. In the classical domain, the tightest lower bound was derived by Gilbert [77]. The Hamming bound [76] serves as a tight upper bound for high coding rates, while the McEliece-Rodemich-Rumsey-Welch (MRRW) bound [79] serves as the tightest upper bound for moderate and low coding rates. As seen in Fig. 10, the gap between the tight upper bounds and the lower bound is quite narrow. It was observed in [65] that a simple quadratic expression $r(\delta) = (2\delta - 1)^2$, where δ denotes the normalized minimum distance d/n, satisfies all the known asymptotic bounds.

The well-known bounds for QSC constructions are listed in Table. 10 and they are also portrayed in Fig. 11. The quantum Singleton bound serves as the loose upper bound, the quantum Hamming bound as a tighter upper bound, and quantum GV bound as the tightest lower bound. However, a wide discrepancy can be observed between the upper bound and the lower bound. For the sake of narrowing this gap, the quantum Rain bound was derived using quantum weight enumerators [81]. To elaborate a little further, the quantum Rain bound states that any quantum code of length n can correct at most $\lfloor\frac{n-1}{6}\rfloor$ errors. The resultant bound is only a function of codeword length n. Hence, under the asymptotic

TABLE 10. The well-known quantum coding bounds found in the literature.

Quantum Coding Bound	Finite-Length	Asymptotic	Notes
Singleton [78]	$\frac{k}{n} \leq 1 - 2\left(\frac{d-1}{n}\right)$	$\frac{k}{n} \leq 1 - 2\left(\frac{d}{n}\right)$	very loose upper bound
Hamming [20]	$\frac{k}{n} \leq 1 - \frac{1}{n}\log_2\left(\sum_{j=0}^{t=\lfloor\frac{d-1}{2}\rfloor} \binom{n}{j} 3^j\right)$	$\frac{k}{n} \leq 1 - \left(\frac{d}{2n}\right)\log_2 3 - H\left(\frac{d}{2n}\right)$	tight upper bound for moderate and high coding rate
Griesmer-Rain [70], [81]	$\frac{k}{n} \leq 1 - \left(\frac{3d-4}{n}\right)$	$\frac{k}{n} \leq 1 - 3\left(\frac{d}{n}\right)$	tighter upper bound for low coding rates CSS codes
Linear Programming [82]		$\frac{k}{n} \leq H(\tau) + \tau\log_2 3 - 1$ $\tau = \frac{3}{4} - \frac{1}{2}\delta - \frac{1}{2}\sqrt{3\delta(1-\delta)}$	strengthen the upper bound
GV [20]	$\frac{k}{n} \geq 1 - \frac{1}{n}\log_2\left(\sum_{j=0}^{d-1} \binom{n}{j} 3^j\right)$	$\frac{k}{n} \geq 1 - \left(\frac{d}{n}\right)\log_2 3 - H\left(\frac{d}{n}\right)$	tight lower bound for general stabilizer codes
GV for CSS [66]		$\frac{k}{n} \geq 1 - 2H\left(\frac{d}{n}\right)$	tight lower bound for CSS codes
	$\frac{k}{n} \geq 1 - \frac{2}{n}\log_2\left(\sum_{j=0}^{d-1} \binom{n}{j}\right)$		lower bound for dual-containing CSS codes

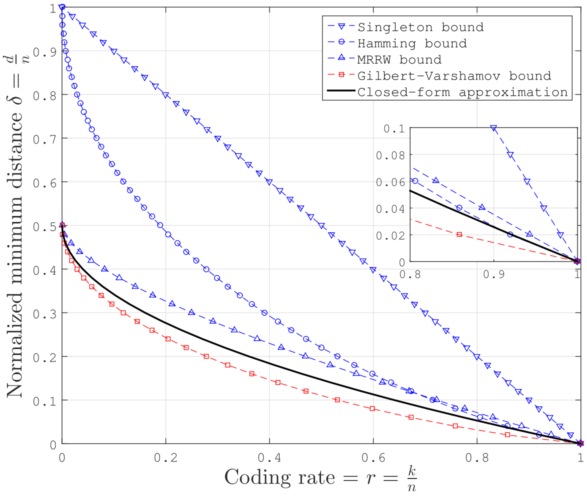


FIGURE 10. The trade-off between classical coding rate *r* and normalized minimum distance δ as described by classical binary coding bounds. A simple quadratic function $r(\delta) = (2\delta - 1)^2$, which satisfies all of the bounds, acts as a closed-form approximation for classical binary error correction codes as suggested in [65].

limit, the quantum Rain bound is a straigthline at $\delta = 1/3$, which does not exhibit any further trade-off between the quantum coding rate and the minimum distance. In order to enhance the accuracy of the quantum Rain bound, Sarvepalli and Klappenecker derived a quantum version of Griesmer bound [70]. By utilizing the quantum Griesmer bound and also the quantum Rain bound, a stronger bound was created for CSS type constructions. In this treatise we will refer to this particular bound as the quantum Griesmer-Rain bound. For the sake of tightening the upper bound, Ashikhmin and Litsyn generalized the classical linear programming approach to the quantum domain using the MacWilliams identities [82]. The resultant quantum linear programming bound was proven to be tighter than the quantum Hamming bound in the low coding rate domain. As the quantum coding rate approaches zero, the achievable mormalized minimum distance returned by the quantum Griesmer-Rain bound becomes $\delta = 0.3333$ and that of quantum linear programming bound becomes $\delta = 0.3152$.

Recall from Section III that the QSCs may exhibit either a CSS or non-CSS structure. For CSS codes, the minimum distance is upper-bounded by the quantum Hamming bound for moderate to high quantum coding rates and by the quantum Griesmer-Rain bound for low coding rates region, while it is also lower-bounded by the quantum GV bound for CSS codes. On the other hand, for non-CSS QSCs, the minimum distance is upper-bounded by the quantum Hamming bound for moderate to high coding rates and by the quantum linear-programming bound for low coding rates. It is also lower-bounded by the quantum GV bound for general quantum stabilizer codes. Even though substantial efforts have been invested tightening the gap between the upper and lower bounds, a significant amount of discrepancy persists. Hence, creating a simple approximation may be beneficial for giving us further insights into the realistic construction of QSCs.

Analogous to the classical closed-form approximation of [65], we also found that there exists a simple closed-form quadratic approximation, which satisfies all the well-known quantum coding bounds. Explicitly for quantum stabilizer codes, the following quadratic function was found to satisfy all the quantum coding bounds:

$$r_Q(\delta) = \frac{32}{9}\delta^2 - \frac{16}{3}\delta + 1 \text{ for } 0 \leq \delta \leq 0.2197. \quad (77)$$

We will further elaborate on the selection of this function in Section VIII. It is important to note that the closed-form approximation is subject to the asymptotical bound for either CSS type or non-CSS type quantum code constructions. The closed-form approximation in Eq. (77) offers the benefit of simplicity and it has the inverse function as given by

$$\delta(r_Q) = \frac{3\left(\sqrt{2} - \sqrt{r_Q + 1}\right)}{4\sqrt{2}} \text{ for } 0 \leq r_Q \leq 1. \quad (78)$$

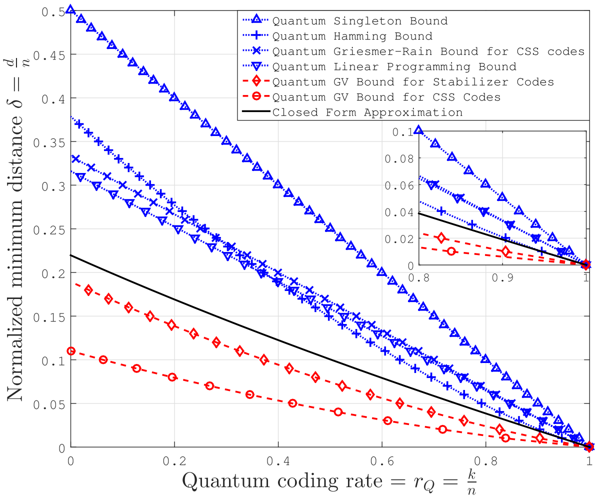


FIGURE 11. The trade-off between quantum coding rate r_Q and normalized minimum distance δ is characterized using quantum coding bounds. A simple quadratic closed-form $r_Q(\delta) = \frac{32}{9}\delta^2 - \frac{16}{3}\delta + 1$ satisfies all of the well-known quantum coding bounds, which is portrayed by black solid lines. The blue dashed lines portrays the upper bounds, while the red dashed lines denotes the lower bounds.

This closed-form approximation suggests that it is possible to create a code construction whose minimum distance grows linearly with the codeword length at the asymptotical limit since for a given quantum coding rate r_Q, it will correspond to a unique constant value of δ.

VII. QUANTUM CODING BOUNDS ON FINITE-LENGTH CODES

The asymptotic limits are only relevant for $n \rightarrow \infty$. For practical applications, we require code constructions with shorter codeword length, which necessitates a different formulation for the quantum coding bounds. Finding a closed-form approximation will be beneficial for determining the realistically attainable minimum distance for the given code parameters. The well-known quantum coding bounds are listed in Table 10 and also portrayed in Fig. 11. It is clearly seen that a simple quadratic approximation can satisfy all the well-known bounds. For the finite-length quantum codes, we propose the closed-form approximation of

$$r_Q(n, \delta) = a\delta^2 + b\delta + c. \tag{79}$$

To arrive at the closed-form approximation in Eq. (79), we have to determine three definitive points corresponding to realistic quantum code constructions. As an example in this treatise, we use three QSC constructions from the literature as listed below:

- For uncoded logical qubits and unity rate codewords, we have

$$r_Q(n, \delta) = r(n, \frac{1}{n}) = 1. \tag{80}$$

- For a high coding rate, we will use the construction given in [19]. For $n = 2^j$, there is a quantum stabilizer code construction $[n, k, d] = [n, n - j - 2, 3]$, which can be used to correct $t = 1$ error. This code construction reaches the quantum Hamming bound. For arbitrary n, it can be written as

$$r_Q(n, \delta) = r(n, \frac{3}{n}) = 1 - \frac{1}{n}\log_2(n) - \frac{2}{n}. \tag{81}$$

- For a very low coding rate, we are using the quantum stabilizer code constructions derived from quadratic residues [83], [84]. By using simple linear regression, we arrive at

$$r_Q(n, \delta) = r(n, \frac{2}{n} + \frac{1}{4}) = \frac{1}{n}. \tag{82}$$

Using the three definitive points from the constructions given in Eq. (80), (81) and (82), we arrive at a system of three linear equations, which have a unique value of a, b and c for an arbitrary value of n. More explicitly, we have

$$r_1 = a\delta_1^2 + b\delta_1 + c, \tag{83}$$

$$r_2 = a\delta_2^2 + b\delta_2 + c, \tag{84}$$

$$r_3 = a\delta_3^2 + b\delta_3 + c. \tag{85}$$

The analytical solution of Eq. (83), (84), and (85) is based on the following unique parameter values:

$$a = \frac{(r_3 - r_2)\,\delta_1 + (r_1 - r_3)\,\delta_2 + (r_2 - r_1)\,\delta_3}{(\delta_2 - \delta_1)\,(\delta_3 - \delta_2)\,(\delta_1 - \delta_3)}, \tag{86}$$

$$b = \frac{(r_2 - r_3)\,\delta_1^2 + (r_3 - r_1)\,\delta_2^2 + (r_1 - r_2)\,\delta_3^2}{(\delta_2 - \delta_1)\,(\delta_3 - \delta_2)\,(\delta_1 - \delta_3)}, \tag{87}$$

$$c = \frac{(r_3\delta_2 - r_2\delta_3)\,\delta_1^2 + (r_1\delta_3 - r_3\delta_1)\,\delta_2^2 + (r_2\delta_1 - r_1\delta_2)\,\delta_3^2}{(\delta_2 - \delta_1)\,(\delta_3 - \delta_2)\,(\delta_1 - \delta_3)}. \tag{88}$$

Despite the cluttered appearance of the analytical solution, it contains a simple closed-form approximation, because the value of r_1, r_2, r_3, δ_1, δ_2 and δ_3 may be easily calculated using Eq. (80), (81) and (82). Furthermore, the closed-form approximation derived for finite-length codewords has an inverse function of

$$\delta(n, r_Q) = \frac{-b - \sqrt{b^2 - 4a(c - r_Q)}}{2a}. \tag{89}$$

The accuracy of the proposed method is now tested for QSCs having codeword length of $n = \{31, 32, 63, 64, 127, 128\}$ as shown in Fig. 12. The list of practical QSC constructions which are used in these plots can be seen in Table. 11.[4] The closed-form approximation lies entirely between the upper and the lower quantum coding bounds. The practical QSCs are also plotted in the same figure to show the relative position with respect to the quantum coding bounds. The QSCs based on [22], [26] lays perfectly on approximation curves, but it has been observed in [85] that as the codeword length increases and the quantum coding rate is reduced, the exact value of the minimum distance becomes unclear. As depicted in Fig. 12b and 12c, we can

[4] A comprehensive list of practical quantum stabilizer codes can be found online at [85]. In this treatise, we only consider quantum stabilizer codes with definitive minimum distance in the list.

TABLE 11. The list of QSC constructions that are used to plot practical code in Fig. 12.

$\mathcal{C}[n,k,d]$ for $n=31$ and $n=32$	
QBCH [23]	[31,1,7], [31,11,5], [31,21,3]
QRM [26]	[32,10,6], [32,25,3]
QGF(4) [22]	[31,1,11], [31,2,10], [31,21,4], [31,26,2], [32,1,11], [32,16,6], [32,22,4], [32,25,3], [32,30,2]
$\mathcal{C}[n,k,d]$ for $n=63$ and $n=64$	
QBCH [23]	[63,27,7], [63,39,5], [63,45,4], [63,51,3], [63,57,2]
QRM [26]	[64,35,6], [64,56,3]
QGF(4) [22]	[63,51,4], [63,55,3], [63,60,2], [64,44,6], [64,48,5], [64,52,4], [64,56,3], [64,62,2]
$\mathcal{C}[n,k,d]$ for $n=127$ and $n=128$	
QBCH [23]	[127,1,19], [127,15,16], [127,29,15], [127,43,13], [127,57,11], [127,71,9], [127,85,7], [127,99,5], [127,113,3]
QRM [26]	[128,35,12], [128,91,6], [128,119,3]
QGF(4) [22]	[127,114,4], [127,118,3], [127,124,2], [128,105,6], [128,110,5], [128,114,4], [128,119,3], [128,126,2]

hardly find definitive points associated with actual codes to plot in the low quantum coding-rate region constructed from quantum $GF(4)$. Meanwhile, the QBCH code constructions lie quite close to the GV lower bound for dual-containing CSS codes. As predicted, since the constructions of QBCH codes rely on dual-containing CSS type constructions, which employ two separate PCMs for their stabilizer operators, we expect a lower coding rate compared to their non-CSS relatives.

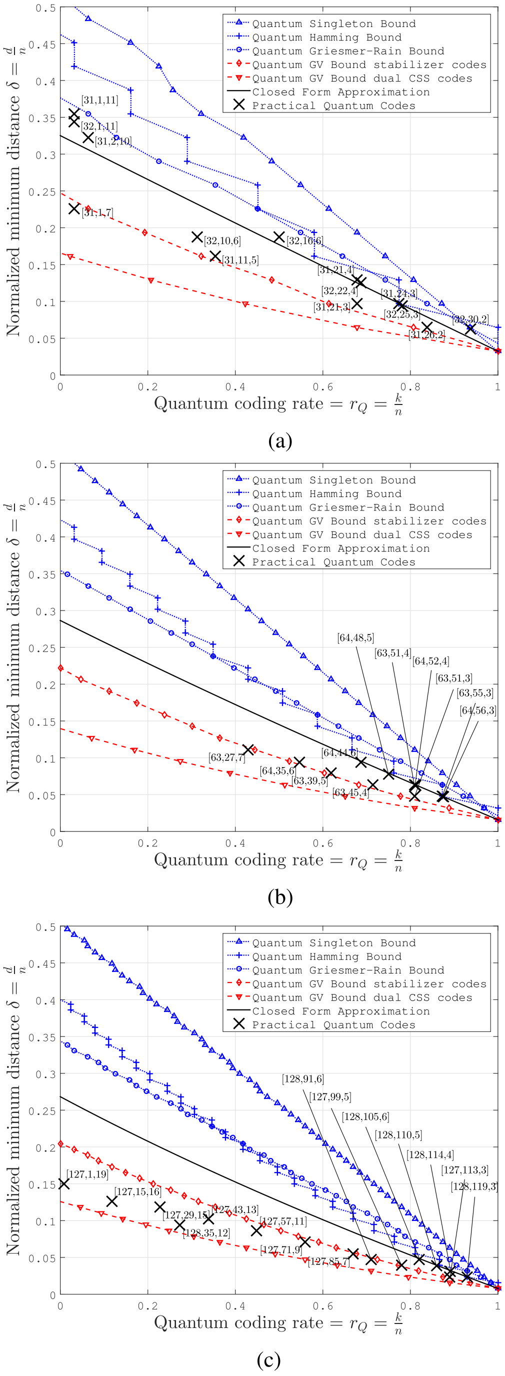
The proposed closed-form approximation offers substantial benefits for the development of QSCs. We can readily find a fairly precise approximation of the realistically achievable minimum distance for given code parameters. For instance, for half-rate quantum stabilizer codes of length 128, the minimum distance is bounded by $11 < d < 22$. By using our formulation, we obtain $d(n = 128, r_Q = 1/2) = 16$ from our finite-length approximation. Likewise, for half-rate quantum stabilizer codes of length 1024, the minimum distance is bounded by $78 < d < 157$. Using our method, we can obtain $d(n = 1024, r_Q = 1/2) = 103$ from our asymptotic bound approximation. One of the logical questions that may arise concerns the existence of the corresponding codes. For example, does a half-rate QSCs relying on $n = 128$ physical qubits and a minimum distance of $d = 16$ exist? The answer to this question is not definitive. Let us refer to the code table given in [85], which is mainly based on the QSC constructions of [22]. Due to space limitations, we are unable to capture the entire table and the associated PCM formulation. However, it is shown in [85] that a half-rate QSC relying on $n = 128$ physical qubits indeed exists, although the minimum distance is only loosely specified by the bounds of $11 < d < 20$. The bound is similar to the quantum GV bound and to the quantum Hamming bound of the minimum distance given by $11 < d < 22$. By contrast, upon using our approximation, we have a minimum distance of $d = 16$, which is again only an approximation and it does not imply the existence of a quantum code having a similar minimum distance. Nonetheless, we believe that our approximation is beneficial for approximating the attainable QBER performance of QSCs based on hard-decision syndrome decoding for short to moderate codeword length as follows (without considering degeneracy):

$$\text{QBER}(n, d, p) = 1 - \sum_{i=0}^{t=\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i} p^i (1-p)^{n-i}, \qquad (90)$$

where the realistically achievable value of d is obtained from our approximation. In our view, the combination of our closed-form approximation and the QBER of Eq. (90) constitutes a useful benchmarker for the future development of QSCs, since it quantifies the realistically achievable QBER performance based on hard-decision syndrome-based decoding.

The evolution of our closed-form approximation as the codeword length increases for $n = \{31, 32, 63, 64, 127, 128\}$ can be seen in Fig. 13. By using our example, it can be clearly observed that as the codeword length increases, the derived approximation for finite-length codes slowly approaches the closed-form approximation of the asymptotic bound. However, inaccuracies emerge as the codeword length increases. This phenomenon is due to the fact that we do not have a definitive QSC constructions to rely on in the low coding rate region. In our approximation example, we are using the QSCs from quadratic residues construction for low coding rate region and the number of QSC constructions are very limited only for a handful codeword lengths. Meanwhile in the classsical domain, in the low coding rate region, we have the simple repetition codes, with construction $\mathcal{C}(n, 1)$ having a normalized minimum distance of $\delta(n, r) = \delta(n, \frac{1}{n}) = 1$.

Albeit the finite and infinite-length-based approximation curves start to deviate for a very long codeword $n \gg 100$, the minimum distance still grows as the codeword length increases as portrayed in Fig. 14. Both the finite-length approximation and asymptotic approximation follow the same trend. For $n \gg 100$, we can simply utilize the asymptotic formulation given in Eq. (77) for calculating the quantum coding rate for a certain desired minimum distance, or the inverse of the asymptotic formulation in Eq. (78) to determine the realistically achievable minimum distance given the quantum coding rate. We can conclude from this figure that it is indeed possible to have a QSC construction



(a)

(b)

(c)

FIGURE 12. Quantum coding rate r_Q versus normalized minimum distance δ for finite-length QSCs. The points for portraying the practical QSCs are taken from QBCH codes [23], QRM codes [26] and quantum codes from *GF*(4) formulation [22]. (a) ($n = 31$) and ($n = 32$). (b) ($n = 63$) and ($n = 64$). (c) ($n = 127$) and ($n = 128$).

with a growing minimum distance, as the codeword length increases.

VIII. THE BOUNDS ON ENTANGLEMENT-ASSISTED QUANTUM STABILIZER CODES

One of the distinctive characteristics of quantum systems, which does not bear any resemblance with the classical

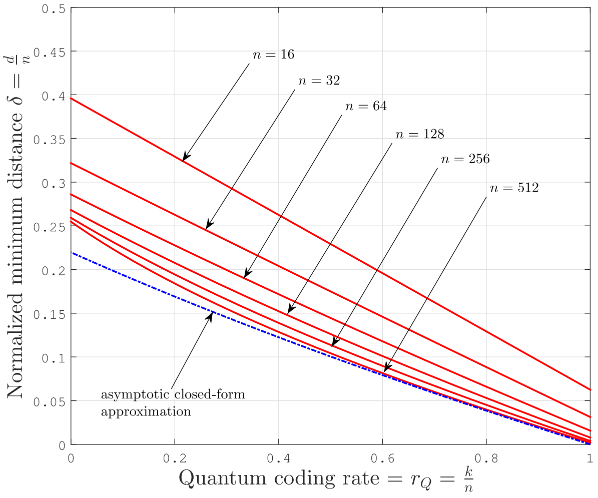


FIGURE 13. The evolution of our closed-form approximation for finite-length codewords for various values of codeword length *n*.

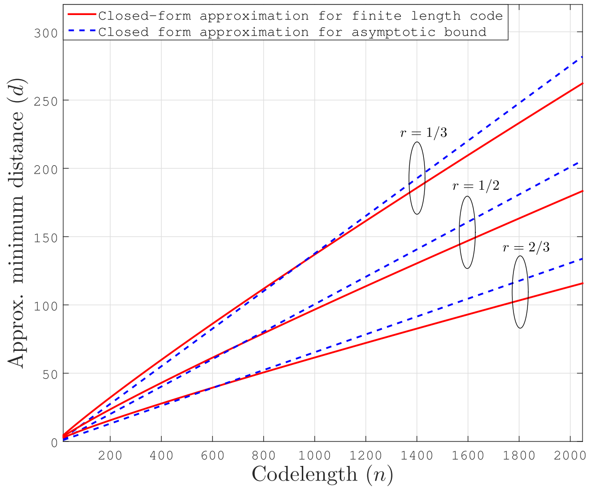


FIGURE 14. The growth of achievable minimum distance for short block QSCs as the codeword length increasing.

domain is the ability of creating entanglement. This unique property can be exploited for increasing the achievable minimum distance of quantum codes, hence increasing the error correction capability of QSCs. The EA-QSC constructions are denoted by $\mathcal{C}(n, k; c)$, where c denotes the number of preshared entangled qubits. It is important to note that even though the EA-QSCs expand the Pauli group operators from $\mathcal{G}^n$ into $\mathcal{G}^{n+c}$, we only consider the error operators in $\mathcal{G}^n$. This is because the paradigm of EA-QSCs assumes that the preshared entangled qubits are not subjected to transmission error. Hence, for EA-QSCs, the quantum Hamming bound of Eq. (66) can be modified to

$$2^k \le \frac{2^{n+c}}{\sum\limits_{j=0}^{t=\lfloor\frac{d_{ea}-1}{2}\rfloor} \binom{n}{j} 3^j}, \tag{91}$$

TABLE 12. The entanglement-assisted quantum coding bounds found in the literature.

Quantum Coding Bound	Finite-Length	Asymptotic	Notes
Singleton [49]	$\frac{k}{n} \leq 1 - 2\left(\frac{d_{ea}-1}{n}\right) + \left(\frac{c}{n}\right)$	$\frac{k}{n} \leq 1 - 2\left(\frac{d_{ea}}{n}\right) + \left(\frac{c}{n}\right)$	very loose upper bound
Hamming [48]	$\frac{k}{n} \leq 1 - \frac{1}{n}\log_2\left(\sum_{j=0}^{t=\lfloor\frac{d_{ea}-1}{2}\rfloor} \binom{n}{j}3^j\right) + \left(\frac{c}{n}\right)$	$\frac{k}{n} \leq 1 - \left(\frac{d_{ea}}{2n}\right)\log_2 3 - H\left(\frac{d_{ea}}{2n}\right) + \left(\frac{c}{n}\right)$	tight upper bound
Linear Programming [86]		$\frac{k}{n} \leq H(\tau) + \tau\log_2 3 - 1 + \left(\frac{c}{n}\right)$ $\tau = \frac{3}{4} - \frac{1}{2}\delta - \frac{1}{2}\sqrt{3\delta(1-\delta)}$	strengthen the upper bound
Plotkin [87], [88]	$\frac{d_{ea}}{n} \leq \frac{3(4^k)}{8(4^k-1)}\left(1 + \left(\frac{k}{n}\right) + \left(\frac{c}{n}\right)\right)$	$\frac{d_{ea}}{n} \leq \frac{3}{8}\left(1 + \left(\frac{k}{n}\right) + \left(\frac{c}{n}\right)\right)$	upper bound for minimum distance
GV [88]	$\frac{k}{n} \geq 1 - \frac{1}{n}\log_2\left(\sum_{j=0}^{d_{ea}-1} \binom{n}{j}3^j\right) + \left(\frac{c}{n}\right)$	$\frac{k}{n} \geq 1 - \left(\frac{d_{ea}}{n}\right)\log_2 3 - H\left(\frac{d_{ea}}{n}\right) + \left(\frac{c}{n}\right)$	tight lower bound

TABLE 13. The asymptotic quantum coding bounds for EA-QSCs given the arbitrary entanglement ratios of θ.

Quantum Coding Bound	Entanglement Ratio $= \theta$	Maximally Entangled $(\theta = 1)$
Singleton [49]	$\frac{k}{n} \leq 1 - \left(\frac{2}{1+\theta}\right)\left(\frac{d_{ea}}{n}\right)$	$\frac{k}{n} \leq 1 - \left(\frac{d_{ea}}{n}\right)$
Hamming [48]	$\frac{k}{n} \leq 1 - \frac{1}{1+\theta}\left(\left(\frac{d_{ea}}{2n}\right)\log_2 3 - H\left(\frac{d_{ea}}{2n}\right)\right)$	$\frac{k}{n} \leq 1 - \frac{1}{2}\left(\left(\frac{d_{ea}}{2n}\right)\log_2 3 - H\left(\frac{d_{ea}}{2n}\right)\right)$
Linear Programming [86]	$\frac{k}{n} \leq \frac{1}{1+\theta}\left(H(\tau) + \tau\log_2 3 - 1 + \theta\right)$	$\frac{k}{n} \leq \frac{1}{2}\left(H(\tau) + \tau\log_2 3\right)$
Plotkin [87], [88]	$\frac{d_{ea}}{n} \leq \frac{3}{8}\left(1 + \theta + \frac{k}{n}(1-\theta)\right)$	$\frac{d_{ea}}{n} \leq \frac{3}{4}$
GV [88]	$\frac{k}{n} \geq 1 - \frac{1}{1+\theta}\left(\left(\frac{d_{ea}}{n}\right)\log_2 3 - H\left(\frac{d_{ea}}{n}\right)\right)$	$\frac{k}{n} \geq 1 - \frac{1}{2}\left(\left(\frac{d_{ea}}{n}\right)\log_2 3 - H\left(\frac{d_{ea}}{n}\right)\right)$

where the notation d_{ea} denotes the minimum distance of EA-QSCs. Equation (91), can be rewritten to show explicitly the trade-off between quantum coding rate r_Q and minimum distance d_{ea} on EA-QSCs as follows:

$$\frac{k}{n} \leq 1 - \frac{1}{n}\log_2\left(\sum_{j=0}^{t=\lfloor\frac{d_{ea}-1}{2}\rfloor} \binom{n}{j}3^j\right) + \left(\frac{c}{n}\right). \tag{92}$$

When n tends to ∞, we yield

$$\frac{k}{n} \leq 1 - \left(\frac{d_{ea}}{2n}\right)\log_2 3 - H\left(\frac{d_{ea}}{2n}\right) + \left(\frac{c}{n}\right). \tag{93}$$

As encapsulated in Eq. (93), an additional conflicting parameter is involved in determining the quantum coding bounds, namely the entanglement consumption rate. The entanglement consumption rate E is the ratio between the number of preshared maximally entangled qubits c to the number of physical qubits n as encapsulated below:

$$E = \frac{c}{n}. \tag{94}$$

A maximally entangled[5] QSCs requires $c = n - k$ preshared qubit pairs. Hence, for a maximally entangled QSCs, the quantum Hamming bound of Eq. (93) can be reformulated as follows by substituting $c = n - k$ into Eq. (93), yielding:

$$\frac{k}{n} \leq 1 - \frac{1}{2}\left(\left(\frac{d_{ea}}{2n}\right)\log_2 3 - H\left(\frac{d_{ea}}{2n}\right)\right). \tag{95}$$

Let us how consider the more general cases, where we may have a range of different entanglement ratios $0 \leq \theta \leq 1$. The entanglement ratio is defined as the ratio of preshared qubits c to the maximally-entangled preshared qubits $(n - k)$, yielding:

$$\theta = \frac{c}{n-k}. \tag{96}$$

The quantum Hamming bound for EA-QSCs with arbitrary entanglement ratios of θ is given by

$$\frac{k}{n} \leq 1 - \frac{1}{1+\theta}\left(\left(\frac{d_{ea}}{2n}\right)\log_2 3 - H\left(\frac{d_{ea}}{2n}\right)\right). \tag{97}$$

The rest of the quantum coding bounds can readily be derived using the same analogy. The resultant entanglement-assisted quantum coding bounds are portrayed in Fig. 15 and 16. By substituting the entanglement ratio of $\theta = 0$, we arrive again at the quantum coding bounds derived for unassisted QSCs. By contrast, upon substituting into Eq. (97) the entanglement ratio $\theta = 1$, we have the quantum coding bounds for maximally-entangled QSCs. Figure 15 portrays the bounds on maximally-entangled QSCs. It is observed in Fig. 15 that at the point $(\delta = 0.75)$, the quantum

[5] For a maximally-entangled QSCs, all of the auxiliary qubits required to generate the encoded state are already preshared using maximally entangled pair qubits. Hence, the maximal number of entangled pair qubits that can be shared beforehand is equal to the total number of auxiliary qubits, which is equal to $(n - k)$.

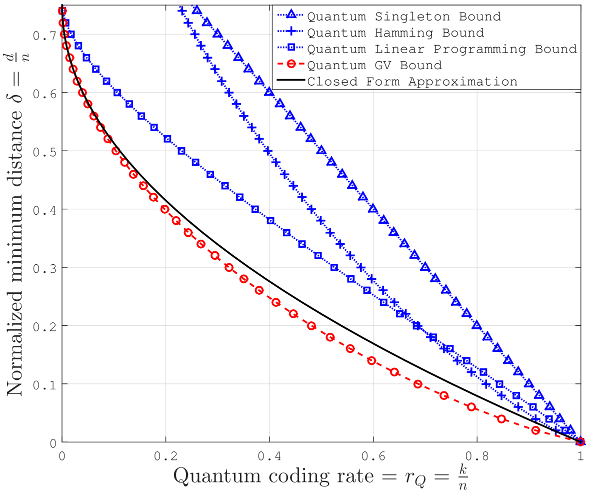


FIGURE 15. The asymptotic quantum coding bounds on EA-QSCs for maximally-entangled constructions. A simple quadratic function $r(\delta) = \frac{16}{9}\delta^2 - \frac{8}{3}\delta + 1$ satisfies all of the quantum coding bounds.

GV bound (lower bound) intersects the quantum linear programming bound (upper bound). Indeed, it is confirmed by the quantum Plotkin bound for the maximally-entangled QSC constructions shown in Table 13 that for asymptotical maximally-entangled QSCs the highest normalized minimum distance that can be achieved is $\delta = 0.75$. Hence, based on this observation, we propose a simple quadratic function as the closed-form approximation of entanglement-assisted quantum stabilizer codes that will satisfy all of the well-known bounds. A quadratic function associated with a symmetry line at ($\delta = 0.75$) and crossing the point of $(\delta, r) = (0, 1)$ is given by

$$r_Q(\delta) = \frac{16}{9}\delta^2 - \frac{8}{3}\delta + 1 \text{ for } 0 \le \delta \le 0.75. \tag{98}$$

The simple quadratic approximaton given in Eq. (98), can also be inverted, yielding

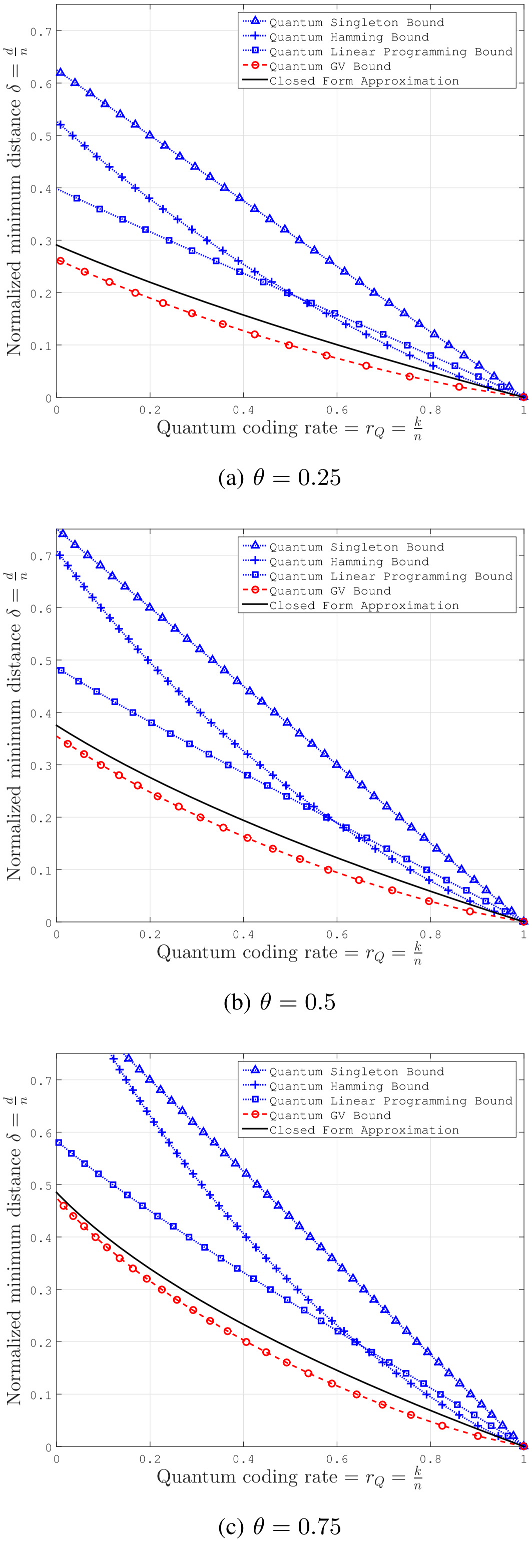
$$\delta(r_Q) = \frac{3}{4}(1 - \sqrt{r_Q}) \text{ for } 0 \le r_Q \le 1. \tag{99}$$

From the simple quadratic function in Eq. (98), we can also derive a simple closed-form approximation for a given arbitrary entanglement ratio of $0 \le \theta \le 1$, as shown below:

$$r_Q(\delta) = \frac{1}{1+\theta}\left(\frac{32}{9}\delta^2 - \frac{16}{3}\delta + 1 + \theta\right), \tag{100}$$

for $0 \le \delta \le \frac{3}{4}\left(1 - \sqrt{\frac{1-\theta}{2}}\right)$ and $0 \le \theta \le 1$. The expression given in Eq. (100) may be inverted to arrive at the following equation:

$$\delta(r_Q) = \frac{3(\sqrt{2} - \sqrt{r_Q(1+\theta) + (1-\theta)}}{4\sqrt{2}}, \tag{101}$$



(a) $\theta = 0.25$

(b) $\theta = 0.5$

(c) $\theta = 0.75$

FIGURE 16. The asymptotic quantum coding bounds on EA-QSCs for different entanglement ratios. (a) $\theta = 0.25$. (b) $\theta = 0.5$. (c) $\theta = 0.75$.

for $0 \le r_Q \le 1$ and $0 \le \theta \le 1$. The simple closed-form approximation given in Eq. (100) and (101) satisfies all entanglement-assisted quantum coding bounds for arbitrary entanglement ratios, as confirmed by Fig. 16. We should point out at this stage that as we substitute the value of $\theta = 0$ into Eq. (100) and (101), we comeback with the closed-form approximation presented in the Eq. (77) and (78) for unassisted asymptotic quantum coding bounds. Hence, we completed our closed-form approximations conceived for all of different constructions of quantum stabilizer codes.

IX. CONCLUSIONS

We have conducted a survey of quantum coding bounds, which describe the trade-off between the quantum coding rate and the error correction capability for a wide range of QSC constructions. Furthermore, we provided insights on their relationships with their classical counterparts. For the family of unassisted QSCs, we have provided both lower and upper bounds for both CSS and non-CSS code constructions. For the EA-QSCs, we have presented the quantum coding bounds for maximally-entangled constructions and also for arbitrary entanglement ratios.

We also have proposed a closed-form approximation as a beneficial tool for analyzing the performance of QSCs. The resultant closed-form approximation may be indeed used as a simple benchmark for developing QSCs, because the resultant minimum distance δ and quantum coding rate r_Q values from our approximations are unambiguous. For instance, for a half-rate quantum stabilizer code having a given codeword length of $n = 128$, the minimum distance is bounded by $11 < d < 22$. By using our approximation, we arrive at $d(n = 128, r_Q = 1/2) = 16$ from our finite-length approximation. Likewise, for a half-rate quantum stabilizer code having the codeword length of 1024, the minimum distance is bounded by $78 < d < 157$. By using our proposal, we have an approximate minimum distance of $d(n = 1024, r_Q = 1/2) = 103$ from our asymptotic bound approximation. Ultimately, the proposed method can be utilized as an efficient tool for the characterization of quantum stabilizer codes.

ACKNOWLEDGMENT

The authors acknowledge the use of the IRIDIS High Performance Computing Facility, and associated support services at the University of Southampton, in the completion of this work.

REFERENCES

[1] L. Hanzo, H. Haas, S. Imre, D. O'Brien, M. Rupp, and L. Gyongyosi, "Wireless myths, realities, and futures: From 3G/4G to optical and quantum wireless," *Proc. IEEE*, vol. 100, Special Centennial Issue, pp. 1853–1888, May 2012.

[2] M. M. Waldrop, "The chips are down for Moore's law," *Nature News*, vol. 530, pp. 144–147, Feb. 2016.

[3] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. 35th Annu. Symp. Found. Comput. Sci.*, 1994, pp. 124–134.

[4] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Rev.*, vol. 41, no. 2, pp. 303–332, 1999.

[5] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proc. 28th Annu. ACM Symp. Theory Comput.*, 1996, pp. 212–219.

[6] M. Boyer, G. Brassard, P. Høyer, and A. Tapp. (1996). "Tight bounds on quantum searching." [Online]. Available: https://arxiv.org/abs/quant-ph/9605034

[7] C. Durr and P. Høyer. (1996). "A quantum algorithm for finding the minimum." [Online]. Available: https://arxiv.org/abs/quant-ph/9607014

[8] L. K. Grover, "Quantum mechanics helps in searching for a needle in a haystack," *Phys. Rev. Lett.*, vol. 79, no. 2, p. 325, 1997.

[9] C. Zalka, "Grover's quantum searching algorithm is optimal," *Phys. Rev. A, Gen. Phys.*, vol. 60, no. 4, p. 2746, 1999.

[10] G. Brassard, F. Dupuis, S. Gambs, and A. Tapp. (2011). "An optimal quantum algorithm to approximate the mean and its application for approximating the median of a set of points over an arbitrary distance." [Online]. Available: https://arxiv.org/abs/1106.4267

[11] P. Botsinis, S. X. Ng, and L. Hanzo, "Quantum search algorithms, quantum wireless, and a low-complexity maximum likelihood iterative quantum multi-user detector design," *IEEE Access*, vol. 1, pp. 94–122, 2013.

[12] P. Botsinis, D. Alanis, S. X. Ng, and L. Hanzo, "Low-complexity soft-output quantum-assisted multiuser detection for direct-sequence spreading and slow subcarrier-hopping aided SDMA-OFDM systems," *IEEE Access*, vol. 2, pp. 451–472, 2014.

[13] D. Alanis, P. Botsinis, S. X. Ng, and L. Hanzo, "Quantum-assisted routing optimization for self-organizing networks," *IEEE Access*, vol. 2, pp. 614–632, 2014.

[14] D. Alanis, P. Botsinis, Z. Babar, S. X. Ng, and L. Hanzo, "Non-dominated quantum iterative routing optimization for wireless multihop networks," *IEEE Access*, vol. 3, pp. 1704–1728, 2015.

[15] D. P. DiVincenzo, "The physical implementation of quantum computation," *Fortschritte Phys.*, vol. 48, nos. 9–11, pp. 771–783, 2000.

[16] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," *Phys. Rev. A, Gen. Phys.*, vol. 52, no. 4, p. R2493(R), 1995.

[17] A. M. Steane, "Error correcting codes in quantum theory," *Phys. Rev. Lett.*, vol. 77, no. 5, p. 793, 1996.

[18] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, "Perfect quantum error correcting code," *Phys. Rev. Lett.*, vol. 77, no. 1, p. 198, 1996.

[19] D. Gottesman, "Class of quantum error-correcting codes saturating the quantum Hamming bound," *Phys. Rev. A, Gen. Phys.*, vol. 54, no. 3, p. 1862, 1996.

[20] A. Ekert and C. Macchiavello, "Quantum error correction for communication," *Phys. Rev. Lett.*, vol. 77, no. 12, p. 2585, 1996.

[21] D. Gottesman, "Stabilizer codes and quantum error correction," Ph.D. dissertation, California Inst. Technol., Pasadena, CA, USA, 1997.

[22] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction via codes over GF(4)," *IEEE Trans. Inf. Theory*, vol. 44, no. 4, pp. 1369–1387, Jul. 1998.

[23] M. Grassl and T. Beth, "Quantum BCH codes," in *Proc. Int. Symp. Theor. Elect. Eng.*, 1999, pp. 207–212.

[24] M. Grassl, T. Beth, and T. Pellizzari, "Codes for the quantum erasure channel," *Phys. Rev. A, Gen. Phys.*, vol. 56, no. 1, p. 33, 1997.

[25] M. Grassl, W. Geiselmann, and T. Beth, "Quantum Reed–Solomon codes," in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*. Berlin, Germany: Springer, 1999, pp. 231–244.

[26] A. M. Steane, "Quantum Reed–Muller codes," *IEEE Trans. Inf. Theory*, vol. 45, no. 5, pp. 1701–1703, Jul. 1999.

[27] H. F. Chau, "Quantum convolutional error-correcting codes," *Phys. Rev. A, Gen. Phys.*, vol. 58, no. 2, p. 905, 1998.

[28] H. Ollivier and J.-P. Tillich, "Description of a quantum convolutional code," *Phys. Rev. Lett.*, vol. 91, no. 17, p. 177902, 2003.

[29] D. MacKay, G. Mitchison, and P. McFadden, "Sparse-graph codes for quantum error correction," *IEEE Trans. Inf. Theory*, vol. 50, no. 10, pp. 2315–2330, Oct. 2004.

[30] D. Poulin, J. P. Tillich, and H. Ollivier, "Quantum serial turbo codes," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2776–2798, Jun. 2009.

[31] J. M. Renes, F. Dupuis, and R. Renner, "Efficient polar coding of quantum information," *Phys. Rev. Lett.*, vol. 109, no. 5, p. 050504, 2012.

[32] A. Y. Kitaev, "Quantum computations: Algorithms and error correction," *Russian Math. Surv.*, vol. 52, no. 6, pp. 1191–1249, 1997.

[33] A. Y. Kitaev, "Fault-tolerant quantum computation by anyons," *Ann. Phys.*, vol. 303, no. 1, pp. 2–30, Jan. 2003.

[34] M. H. Freedman, D. A. Meyer, and F. Luo, "Z2-systolic freedom and quantum codes," in *Mathematics of Quantum Computation*. London, U.K.: Chapman & Hall, 2002, pp. 287–320.

[35] S. B. Bravyi and A. Y. Kitaev. (1998). "Quantum codes on a lattice with boundary." [Online]. Available: https://arxiv.org/abs/quant-ph/9811052

[36] C. Horsman, A. G. Fowler, S. Devitt, and R. Van Meter, "Surface code quantum computing by lattice surgery," *New J. Phys.*, vol. 14, no. 12, p. 123011, 2012.

[37] H. Bombin and M. A. Martin-Delgado, "Topological quantum distillation," *Phys. Rev. Lett.*, vol. 97, no. 18, p. 180501, 2006.

[38] J. Haah, "Local stabilizer codes in three dimensions without string logical operators," *Phys. Rev. A, Gen. Phys.*, vol. 83, no. 4, p. 042330, 2011.

[39] G. Zémor, "On Cayley graphs, surface codes, and the limits of homological coding for quantum error correction," in *Proc. Int. Conf. Coding Cryptol.*, 2009, pp. 259–273.

[40] A. Couvreur, N. Delfosse, and G. Zemor, "A construction of quantum LDPC codes from Cayley graphs," *IEEE Trans. Inf. Theory*, vol. 59, no. 9, pp. 6087–6098, Sep. 2013.

[41] N. Delfosse, "Tradeoffs for reliable quantum information storage in surface codes and color codes," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2013, pp. 917–921.

[42] J.-P. Tillich and G. Zémor, "Quantum LDPC codes with positive rate and minimum distance proportional to $n^{\frac{1}{2}}$," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun./Jul. 2009, pp. 799–803.

[43] A. A. Kovalev and L. P. Pryadko, "Improved quantum hypergraph-product LDPC codes," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2012, pp. 348–352.

[44] J.-P. Tillich and G. Zémor, "Quantum LDPC codes with positive rate and minimum distance proportional to the square root of the blocklength," *IEEE Trans. Inf. Theory*, vol. 60, no. 2, pp. 1193–1202, Feb. 2014.

[45] S. Bravyi and M. B. Hastings, "Homological product codes," in *Proc. 46th Annu. ACM Symp. Theory Comput.*, 2014, pp. 273–282.

[46] D. A. Lidar and T. A. Brun, Eds., *Quantum Error Correction*. Cambridge, U.K.: Cambridge Univ. Press, 2013.

[47] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction and orthogonal geometry," *Phys. Rev. Lett.*, vol. 78, no. 3, p. 405, 1997.

[48] G. Bowen, "Entanglement required in achieving entanglement-assisted channel capacities," *Phys. Rev. A, Gen. Phys.*, vol. 66, no. 5, p. 052313, 2002.

[49] T. A. Brun, I. Devetak, and M.-H. Hsieh, "Correcting quantum errors with entanglement," *Science*, vol. 314, no. 5798, pp. 436–439, Oct. 2006.

[50] M. M. Wilde and T. A. Brun, "Entanglement-assisted quantum convolutional coding," *Phys. Rev. A, Gen. Phys.*, vol. 81, no. 4, p. 042333, 2010.

[51] M. S. Postol. (2001). "A proposed quantum low density parity check code." [Online]. Available: https://arxiv.org/abs/quant-ph/0108131

[52] T. Camara, H. Ollivier, and J.-P. Tillich. (2005). "Constructions and performance of classes of quantum LDPC codes." [Online]. Available: https://arxiv.org/abs/quant-ph/0502086

[53] T. Camara, H. Ollivier, and J.-P. Tillich, "A class of quantum LDPC codes: Construction and performances under iterative decoding," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2007, pp. 811–815.

[54] M.-H. Hsieh, T. A. Brun, and I. Devetak, "Entanglement-assisted quantum quasicyclic low-density parity-check codes," *Phys. Rev. A, Gen. Phys.*, vol. 79, no. 3, p. 032340, 2009.

[55] Z. Babar, P. Botsinis, D. Alanis, S. X. Ng, and L. Hanzo, "Fifteen years of quantum LDPC coding and improved decoding strategies," *IEEE Access*, vol. 3, pp. 2492–2519, 2015.

[56] M. M. Wilde and M.-H. Hsieh, "Entanglement boosts quantum turbo codes," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul./Aug. 2011, pp. 445–449.

[57] M. M. Wilde, M.-H. Hsieh, and Z. Babar, "Entanglement-assisted quantum turbo codes," *IEEE Trans. Inf. Theory*, vol. 60, no. 2, pp. 1203–1222, Feb. 2014.

[58] Z. Babar, P. Botsinis, D. Alanis, S. X. Ng, and L. Hanzo, "The road from classical to quantum codes: A hashing bound approaching design procedure," *IEEE Access*, vol. 3, pp. 146–176, 2015.

[59] M. M. Wilde and J. M. Renes, "Quantum polar codes for arbitrary channels," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2012, pp. 334–338.

[60] J. Preskill, "Reliable quantum computers," *Proc. R. Soc. Lond. A, Math., Phys. Eng. Sci.*, vol. 454, no. 1969, pp. 385–410, 1998.

[61] D. Gottesman, "Theory of fault-tolerant quantum computation," *Phys. Rev. A, Gen. Phys.*, vol. 57, no. 1, p. 127, 1998.

[62] E. Knill, R. Laflamme, and W. H. Zurek, "Resilient quantum computation," *Science*, vol. 279, no. 5349, pp. 342–345, 1998.

[63] E. Knill, R. Laflamme, and W. H. Zurek, "Resilient quantum computation: Error models and thresholds," *Proc. R. Soc. Lond. A, Math., Phys. Eng. Sci.*, vol. 454, no. 1969, pp. 365–384, 1998.

[64] D. Gottesman, "Fault-tolerant quantum computation with constant overhead," *Quantum Inf. Comput.*, vol. 14, nos. 15–16, pp. 1338–1372, 2014.

[65] J. Akhtman, R. Maunder, N. Bonello, and L. Hanzo, "Closed-form approximation of maximum free distance for binary block codes," in *Proc. IEEE 70th Veh. Technol. Conf. Fall (VTC-Fall)*, Sep. 2009, pp. 1–3.

[66] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Phys. Rev. A, Gen. Phys.*, vol. 54, no. 2, p. 1098, 1996.

[67] A. Steane, "Multiple-particle interference and quantum error correction," *Proc. R. Soc. Lond. A, Math., Phys. Eng. Sci.*, vol. 452, no. 1954, pp. 2551–2577, Nov. 1996.

[68] P. A. M. Dirac, "A new notation for quantum mechanics," *Math. Proc. Cambridge Philos. Soc.*, vol. 35, no. 3, pp. 416–418, 1939.

[69] A. Ashikhmin. (1997). "Remarks on bounds for quantum codes." [Online]. Available: https://arxiv.org/abs/quant-ph/9705037

[70] P. Sarvepalli and A. Klappenecker, "Degenerate quantum codes and the quantum Hamming bound," *Phys. Rev. A, Gen. Phys.*, vol. 81, no. 3, p. 032318, 2010.

[71] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge, U.K.: Cambridge Univ. Press, 2000.

[72] P. Botsinis *et al.*, "Quantum error correction protects quantum search algorithms against decoherence," *Sci. Rep.*, vol. 6, Dec. 2016, Art. no. 38095.

[73] R. Cleve and D. Gottesman, "Efficient computations of encodings for quantum error correction," *Phys. Rev. A, Gen. Phys.*, vol. 56, no. 1, p. 76, 1997.

[74] I. Djordjevic, *Quantum Information Processing and Quantum Error Correction: An Engineering Approach*. New York, NY, USA: Academic, 2012.

[75] R. C. Singleton, "Maximum distance q-nary codes," *IEEE Trans. Inf. Theory*, vol. 10, no. 2, pp. 116–118, Apr. 1964.

[76] R. W. Hamming, "Error detecting and error correcting codes," *Bell Syst. Tech. J.*, vol. 29, no. 2, pp. 147–160, Apr. 1950.

[77] E. N. Gilbert, "A comparison of signalling alphabets," *Bell Syst. Tech. J.*, vol. 31, no. 3, pp. 504–522, 1952.

[78] E. Knill and R. Laflamme, "Theory of quantum error-correcting codes," *Phys. Rev. A, Gen. Phys.*, vol. 55, no. 2, p. 900, 1997.

[79] R. J. McEliece, E. R. Rodemich, H. Rumsey, and L. Welch, "New upper bounds on the rate of a code via the Delsarte-MacWilliams inequalities," *IEEE Trans. Inf. Theory*, vol. 23, no. 2, pp. 157–166, Mar. 1977.

[80] M. Plotkin, "Binary codes with specified minimum distance," *IRE Trans. Inf. Theory*, vol. 6, no. 4, pp. 445–450, 1960.

[81] E. M. Rains, "Quantum shadow enumerators," *IEEE Trans. Inf. Theory*, vol. 45, no. 7, pp. 2361–2366, Nov. 1999.

[82] A. Ashikhmin and S. Litsyu, "Upper bounds on the size of quantum codes," *IEEE Trans. Inf. Theory*, vol. 45, no. 4, pp. 1206–1215, May 1999.

[83] C.-Y. Lai and C.-C. Lu, "A construction of quantum stabilizer codes based on syndrome assignment by classical parity-check matrices," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 7163–7179, Oct. 2011.

[84] Y. Xie, J. Yuan, and Q. Sun. (2014). "Design of quantum stabilizer codes from quadratic residues sets." [Online]. Available: https://arxiv.org/abs/1407.8249

[85] M. Grassl. (2007). *Bounds on the Minimum Distance of Linear Codes and Quantum Codes*, accessed on May 1, 2017. [Online]. Available: http://www.codetables.de

[86] C.-Y. Lai and A. Ashikhmin. (2016). "Linear programming bounds for entanglement-assisted quantum error-correcting codes by split weight enumerators." [Online]. Available: https://arxiv.org/abs/1602.00413

[87] L. Guo and R. Li, "Linear Plotkin bound for entanglement-assisted quantum codes," *Phys. Rev. A, Gen. Phys.*, vol. 87, no. 3, p. 032309, 2013.

[88] C.-Y. Lai, T. A. Brun, and M. M. Wilde, "Dualities and identities for entanglement-assisted quantum codes," *Quantum Inf. Process.*, vol. 13, no. 4, pp. 957–990, 2014.

DARYUS CHANDRA (S'15) received the M.Eng. degree in electrical engineering from Universitas Gadjah Mada, Indonesia, in 2014. He is currently pursuing the Ph.D. degree with the Southampton Wireless Group, School of Electronics and Computer Science, University of Southampton, U.K. He was a recipient of the Scholarship Award from the Indonesia Endowment Fund for Education, Lembaga Pengelola Dana Pendidikan.

His research interests include classical and quantum error correction codes, quantum information, and quantum communications.

ZUNAIRA BABAR received the B.Eng. degree in electrical engineering from the National University of Science and Technology, Islamabad, Pakistan, in 2008, and the M.Sc. degree (Hons.) and the Ph.D. degree in wireless communications from the University of Southampton, U.K., in 2011 and 2015, respectively.

Her research interests include quantum error correction codes, channel coding, coded modulation, iterative detection, and cooperative communications.

HUNG VIET NGUYEN received the B.Eng. degree in electronics and telecommunications from the Hanoi University of Science and Technology, Hanoi, Vietnam, in 1999, the M.Eng. degree in telecommunications from the Asian Institute of Technology, Bangkok, Thailand, in 2002, and the Ph.D. degree in wireless communications from the University of Southampton, Southampton, U.K., in 2013. Since 1999, he has been a Lecturer at the Post and Telecommunications Institute of Technology, Vietnam. He is currently a Post-Doctoral Researcher with the Southampton Wireless Group, University of Southampton, U.K. He is involved in the OPTIMIX and CONCERTO European projects.

His research interests include cooperative communications, channel coding, network coding, and quantum communications.

DIMITRIOS ALANIS (S'13) received the M.Eng. degree in electrical and computer engineering from the Aristotle University of Thessaloniki in 2011 and the M.Sc. and Ph.D. degrees in wireless communications from the University of Southampton in 2012 and 2017, respectively. He is currently a Research Fellow with the Southampton Wireless Group, School of Electronics and Computer Science, University of Southampton, U.K.

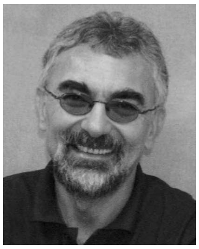
His research interests include quantum computation and quantum information theory, quantum search algorithms, cooperative communications, resource allocation for self-organizing networks, bio-inspired optimization algorithms, and classical and quantum game theory.

PANAGIOTIS BOTSINIS (S'12–M'16) received the M.Eng. degree from the School of Electrical and Computer Engineering, National Technical University of Athens, Greece, in 2010, the M.Sc. degree (Hons.) and the Ph.D. degree in wireless communications from the University of Southampton, U.K., in 2011 and 2015, respectively. He is currently a Research Fellow with the Southampton Wireless Group, School of Electronics and Computer Science, University of Southampton, U.K. Since 2010, he has been a member of the Technical Chamber of Greece.

His research interests include quantum-assisted communications, quantum computation, iterative detection, OFDM, MIMO, multiple access systems, coded modulation, channel coding, cooperative communications, and combinatorial optimization.

SOON XIN NG (S'99–M'03–SM'08) received the B.Eng. degree (Hons.) in electronic engineering and the Ph.D. degree in telecommunications from the University of Southampton, Southampton, U.K., in 1999 and 2002, respectively. From 2003 to 2006, he was a Post-Doctoral Research Fellow and involved in collaborative European research projects such as SCOUT, NEWCOM, and PHOENIX. Since 2006, he has been a member of the Academic Staff with the School of Electronics and Computer Science, University of Southampton, where he is currently an Associate Professor in telecommunications. He is involved in the OPTIMIX and CONCERTO European projects and the IU-ATC and UC4G projects.

His research interests include adaptive coded modulation, coded modulation, channel coding, space-time coding, joint source and channel coding, iterative detection, OFDM, MIMO, cooperative communications, distributed coding, quantum error correction codes, and joint wireless-and-optical-fiber communications. He has authored over 200 papers and co-authored two John Wiley/IEEE Press books in this field. He is a Chartered Engineer and a fellow of the Higher Education Academy in the U.K.



LAJOS HANZO (M'91–SM'92–F'04) received the degree in electronics in 1976 and the Ph.D. degree in 1983. In 2009, he received the honorary doctorate Doctor Honoris Causa degree from the Technical University of Budapest. During his 38-year career in telecommunications, he has held various research and academic posts in Hungary, Germany, and the U.K. Since 1986, he has been with the School of Electronics and Computer Science, University of Southampton, U.K., where he holds the chair in telecommunications. He has successfully supervised about 100 Ph.D. students, co-authored 20 John Wiley/IEEE Press books on mobile radio communications totalling in excess of 10 000 pages, and authored over 1,400 research entries in the IEEE Xplore. He has acted both as the TPC and the General Chair of the IEEE conferences, presented keynote lectures, and received a number of distinctions. He is currently directing a 100-strong academic research team, involved in a range of research projects in the field of wireless multimedia communications sponsored by industry, the Engineering and Physical Sciences Research Council U.K., the European Research Councils Advanced Fellow Grant, and the Royal Society's Wolfson Research Merit Award. He is an enthusiastic supporter of industrial and academic liaison and he offers a range of industrial courses.

Dr. Lajos is a fellow of the Royal Academy of Engineering, the Institution of Engineering and Technology, and the European Association for Signal Processing. He is also a Governor of the IEEE VTS. During 2008-2012, he was the Editor-in-Chief of the IEEE Press and a Chaired Professor at Tsinghua University, Beijing. He has over 30 000 citations.

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received October 6, 2017, accepted December 11, 2017, date of publication December 18, 2017, date of current version March 28, 2018.

Digital Object Identifier 10.1109/ACCESS.2017.2784417

Quantum Topological Error Correction Codes: The Classical-to-Quantum Isomorphism Perspective

DARYUS CHANDRA, (Student Member, IEEE), ZUNAIRA BABAR, HUNG VIET NGUYEN, DIMITRIOS ALANIS, (Student Member, IEEE), PANAGIOTIS BOTSINIS, (Member, IEEE), SOON XIN NG, (Senior Member, IEEE), AND LAJOS HANZO, (Fellow, IEEE)
School of Electronics and Computer Science, University of Southampton, Southampton SO17 1BJ, U.K.

Corresponding author: Lajos Hanzo (lh@ecs.soton.ac.uk)

This work was supported in part by the EPSRC under Grant EP/L018659/1, in part by the European Research Council's Advanced Fellow Grant, and in part by the Royal Society's Wolfson Research Merit Award.

ABSTRACT We conceive and investigate the family of classical topological error correction codes (TECCs), which have the bits of a codeword arranged in a lattice structure. We then present the classical-to-quantum isomorphism to pave the way for constructing their quantum dual pairs, namely, the quantum TECCs (QTECCs). Finally, we characterize the performance of QTECCs in the face of the quantum depolarizing channel in terms of both the quantum-bit error rate (QBER) and fidelity. Specifically, from our simulation results, the threshold probability of the QBER curves for the color codes, rotated-surface codes, surface codes, and toric codes are given by 1.8×10^{-2}, 1.3×10^{-2}, 6.3×10^{-2}, and 6.8×10^{-2}, respectively. Furthermore, we also demonstrate that we can achieve the benefit of fidelity improvement at the minimum fidelity of 0.94, 0.97, and 0.99 by employing the $1/7$-rate color code, the $1/9$-rate rotated-surface code, and $1/13$-rate surface code, respectively.

INDEX TERMS Quantum error correction codes, quantum stabilizer codes, quantum topological codes, lattice code, LDPC.

NOMENCLATURE

A. LIST OF ACRONYMS

BCH	Bose-Chaudhuri-Hocquenghem
CNOT	Controlled-NOT
CSS	Calderbank-Shor-Steane
GV	Gilbert-Varshamov
LDPC	Low Density Parity Check
ML	Maximum Likelihood
PCM	Parity Check Matrix
QBCH	Quantum Bose-Chaudhuri-Hocquenghem
QBER	QuBit Error Rate
QECC	Quantum Error Correction Code
QSC	Quantum Stabilizer Code
QTECC	Quantum Topological Error Correction Code
TECC	Topological Error Correction Code

B. LIST OF SYMBOLS

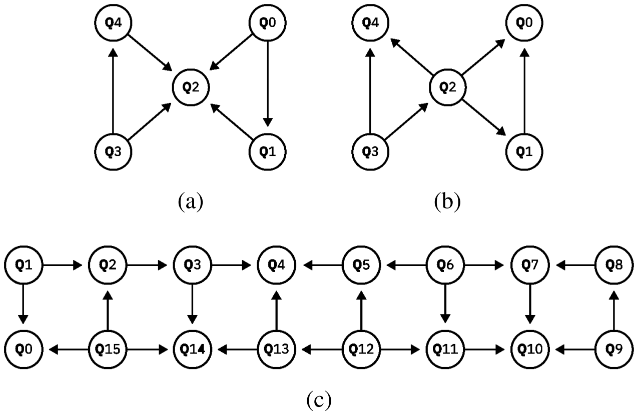
d	Minimum Distance
F	Fidelity
F_{th}	Threshold Fidelity
$H(x)$	Binary Entropy of x
$\mathbf{H}$	Parity Check Matrix, Hadamard Transformation
k	Information Bit Length, Number of Logical Qubits
n	Codeword Length, Number of Physical Qubits
p	Depolarizing Probability
p_{th}	Threshold Probability
r	Classical Coding Rate
r_Q	Quantum Coding Rate
S_i	Stabilizer Operator
$\mathcal{S}$	Stabilizer Group
t	Error Correction Capability
δ	Normalized Minimum Distance
$\otimes$	Kronecker Tensor Product
$\|\psi\rangle$	Quantum State ψ
$\mathcal{C}(n, k, d)$	Classical Error Correction Codes Having Parameter n, k and d
$\mathcal{C}[n, k, d]$	Quantum Stabilizer Codes Having Parameter n, k and d

I. INTRODUCTION

One of the essential prerequisites to build quantum computers is the employment of quantum error correction codes (QECCs) to ensure that the computers operate reliably by mitigating the deleterious effects of quantum decoherence [1]–[3]. However, the law of quantum mechanics prevent us from transplanting classical error correction codes directly into the quantum domain. In order to circumvent the constraints imposed by the nature of quantum physics, the notion of quantum stabilizer codes (QSCs) emerged [4]–[6]. The invention of QECCs and specifically the QSC formalism did not immediately eradicate all of the obstacles of developing reliable quantum computers. Employing the QSCs requires redundancy in the form of auxiliary quantum bits (qubits) to encode the logical qubits onto physical qubits. The redundant qubits are then utilized to invoke the error correction. Hence, additional components such as the quantum encoder and decoder circuits built from quantum gates are required. Therefore, the employment of a QSC itself has to be fault-tolerant to guarantee that the QSC circuit does not introduce additional decoherence into the quantum computers.

The notion of QSC trigerred numerous discoveries in the domain of QECCs, which are inspired by classical error corrrection codes. Essentially, QSCs represent the quantum version of the classical syndrome decoding-based error correction codes. Since the concept of utilizing the syndrome values for error correction is widely exploited in the classical domain, diverse classical error correction codes can be conveniently ‘‘quantumized’’. Consequently, we can find in the literature the quantum version of error correction codes based on algebraic formalisms such as those of the Bose-Chaudhuri-Hocquenghem (BCH) codes [7] and of Reed-Solomon (RS) codes [8], quantum codes based on a coventional trellis structure such as convolutional codes [9] and turbo codes [10], [11], as well as quantum codes based on bipartite graphs, such as low density parity check (LDPC) codes [12]–[16]. Another approach that can be exploited to develop both classical and quantum error correction codes hinges on code constructions based on lattice or topological structures. Unfortunately, this concept has not been widely explored in the classical domain. By contrast, in the quantum domain, having a code construction relying on the physical configuration of qubits is highly desirable for the low-complexity high-reliability quantum computers.

The development of QECCs was inspired by Shor [17], who proposed a 9-qubit code. The 9-qubit code, which is also referred to as Shor’s code, can protect 9 physical qubits from any type of quantum errors, namely bit-flips (**X**), phase-flips (**Z**), as well as from simultaneous bit and phase-flips (**Y**). Not long after the discovery of the first QECCs, Steane invented the 7-qubit code, which was followed by Laflamme’s perfect 5-qubit code [18], [19]. However, the construction of these codes does not naturally exhibit inherent fault-tolerance. The quantum circuit based implementation of these codes always involves a high number of qubit interactions within the codeword of physical qubits. As a consequence, an error caused by a faulty gate within either the encoder, or within the stabilizer measurement, and/or in the inverse encoder potentially propagates to other qubits and instead of being eliminated, the deleterious effects of quantum decoherence are actually further aggravated.

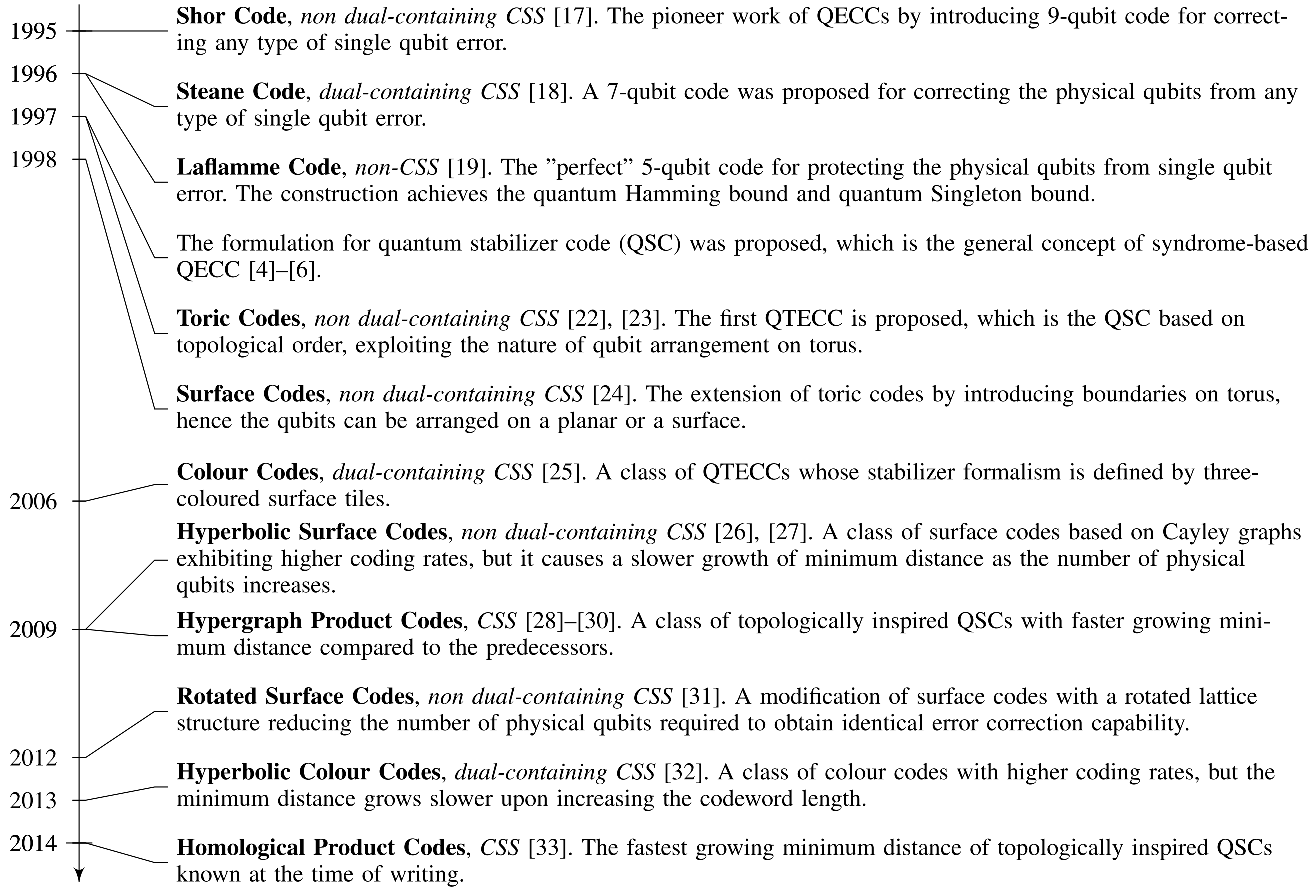


(a) (b)

(c)

FIGURE 1. The qubit arrangement of IBM’s superconducting quantum computers. The circles represent the qubits, while the arrows represent the possible qubit interactions within the computers [20]. (a) 5 qubits (ibmqx2). (b) 5 qubits (ibmqx4). (c) 16 qubits (ibmqx5).

The quantum version of the classical topological error correction codes (TECCs) [21], namely the quantum topological error correction codes (QTECCs), constitute beneficial fault-tolerant QSCs for improving quantum computer implementations. Firstly, they are capable of supporting the physical implementation of quantum memory. For instance, this strategy has been deployed for developing the IBM’s superconducting quantum computers, as shown in Fig. 1. From this figure, we can see the qubit arrangement of the three prototypes of IBM’s quantum computer - which can be viewed online - namely the ibmqx2, ibmqx4, and ibmqx5 configurations [20]. The first two of the quantum computers are the 5-qubit quantum computers, while the last one is a 16-qubit quantum computer. The circles in Fig. 1 represent the qubits, while the arrows represent all the possible two-qubit interactions. It can be clearly seen that the existing architectures impose a limitation, namely the two-qubit interactions can be only performed between the neighbouring qubits. Even though this particular limitation potentially imposes additional challenges, when it comes to QSCs deployment, the stabilizer effect can still be achieved by the corresponding qubit arrangement by invoking the QTECCs. Secondly, the locality of stabilizer measurements minimizes the requirements imposed on the corresponding quantum gates. The interdependence of the qubits within the codeword are inevitable. However, the interaction between the most distant qubits should be avoided, which imposes challenges on the realization. Another property that makes the QTECCs fault-tolerant is their growing minimum distance as a function of codeword length. More explicitly, the growing minimum



Shor Code, *non dual-containing CSS* [17]. The pioneer work of QECCs by introducing 9-qubit code for correcting any type of single qubit error.

Steane Code, *dual-containing CSS* [18]. A 7-qubit code was proposed for correcting the physical qubits from any type of single qubit error.

Laflamme Code, *non-CSS* [19]. The "perfect" 5-qubit code for protecting the physical qubits from single qubit error. The construction achieves the quantum Hamming bound and quantum Singleton bound.

The formulation for quantum stabilizer code (QSC) was proposed, which is the general concept of syndrome-based QECC [4]–[6].

Toric Codes, *non dual-containing CSS* [22], [23]. The first QTECC is proposed, which is the QSC based on topological order, exploiting the nature of qubit arrangement on torus.

Surface Codes, *non dual-containing CSS* [24]. The extension of toric codes by introducing boundaries on torus, hence the qubits can be arranged on a planar or a surface.

Colour Codes, *dual-containing CSS* [25]. A class of QTECCs whose stabilizer formalism is defined by three-coloured surface tiles.

Hyperbolic Surface Codes, *non dual-containing CSS* [26], [27]. A class of surface codes based on Cayley graphs exhibiting higher coding rates, but it causes a slower growth of minimum distance as the number of physical qubits increases.

Hypergraph Product Codes, *CSS* [28]–[30]. A class of topologically inspired QSCs with faster growing minimum distance compared to the predecessors.

Rotated Surface Codes, *non dual-containing CSS* [31]. A modification of surface codes with a rotated lattice structure reducing the number of physical qubits required to obtain identical error correction capability.

Hyperbolic Colour Codes, *dual-containing CSS* [32]. A class of colour codes with higher coding rates, but the minimum distance grows slower upon increasing the codeword length.

Homological Product Codes, *CSS* [33]. The fastest growing minimum distance of topologically inspired QSCs known at the time of writing.

FIGURE 2. Timeline of important milestones in the area of QTECCs. The code construction is highlighted with bold while the associated code type is marked in *italics*.

distance ensures having an increasing error correction capability per codeword for the QTECCs upon increasing the codeword length, albeit this does not necessarily increase the per-bit normalized error correction capability. To elaborate a little further, increasing the number of physical qubits[1] also increases the number of qubit interactions within the block. Thus, the per-codeword error correction capability of the code should grow fast enough to compensate for the potential error propagation, which may further aggravate the effect of quantum decoherence. The latter phenomenon is also related to the problem experienced in the classical coding theory field, associated with the trade-off between the coding rate and the error correction capability of the error correction code. The study of this particular trade-off in QSCs is a pivotal subject, because we can simply decrease the coding rate further and further to achieve a certain error correction capability without considering the sheer amount of redundant resources wasted, when aiming for achieving the target performance. Therefore, a comprehensive investigation related to this particular trade-off has to be conducted for characterizing the performances versus code parameters. A timeline portraying the important milestones of the QTECCs' development is depicted in Fig. 2.[2]

Based on the aforementioned background, our novel contributions are:

1) *We conceive the construction of classical error correction codes based on topological or lattice structures. Additionally, we demonstrate for a long codeword that the resultant codes have a resemblance to the classical LDPC codes exhibiting reasonable code parameters.*
2) *We present a tutorial on both classical and quantum topological error correction codes as well as the classical-to-quantum isomorphism along with the comparative study of code parameters.*
3) *We derive the upper bound QBER performance of the QTECCs in the face of quantum depolarizing channel and the formula to determine the threshold fidelity.*

The structure of the paper is described in Fig. 3 and the rest of this treatise is organized as follows. In Section II, we commence with design examples of classical TECCs to pave the

[1] The terms 'number of physical qubits' is usually used to refer the 'codeword length' in quantum codes.

[2] Shor's, Steane's and Laflamme's codes do not belong to the QTECCs family. However, we believe that it is still important to include the three pioneeering contributions on QECCs in the timeline for the sake of completeness.

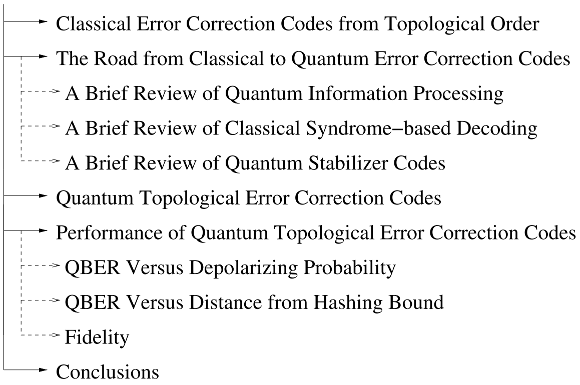

Classical Error Correction Codes from Topological Order
The Road from Classical to Quantum Error Correction Codes
A Brief Review of Quantum Information Processing
A Brief Review of Classical Syndrome–based Decoding
A Brief Review of Quantum Stabilizer Codes
Quantum Topological Error Correction Codes
Performance of Quantum Topological Error Correction Codes
QBER Versus Depolarizing Probability
QBER Versus Distance from Hashing Bound
Fidelity
Conclusions

FIGURE 3. The structure of the paper.

way for delving into the quantum domain. In Section III, we provide a tutorial on the fundamentals of QSCs by exploiting its isomorphism with the classical syndrome-based decoding, while in Section IV we detail our QSC design examples for QTECCs. We continue by characterizing the performance of QTECCs over the popular quantum depolarizing channel in terms of QBER and fidelity in Section V. Finally, we conclude our discussion in Section VI.

II. CLASSICAL ERROR CORRECTION CODES FROM TOPOLOGICAL ORDER: DESIGN EXAMPLES

As we mentioned earlier in Section I, the classical error correction codes can be developed relying on diverse approaches [34]. We can find in the literature various family of codes based on algebraic formalisms (such as BCH codes and RS codes), codes based on conventional trellis structures (such as convolutional codes and turbo codes) and also codes based on bipartite graphs (such as LDPC codes). Another approach that can be adopted to formulate a classical error correction code is by exploiting the topological or lattice structure. By assuming that we can arrange the bits of a codeword on a lattice structure, it can inherently provide us with an error correction scheme [21]. For instance, let us assume that a codeword of classical bits is arranged on the square lattice given in Fig. 4. The black circles laying on the edges of the lattice define the encoded information bits or the codeword. The red squares laying on the vertices of the lattice define the parity check matrix (PCM) of the codes, which also directly defines the syndrome values of the received codeword. The number of black circles is associated with the codeword length of n bits and the number of red squares is associated with the length of the syndrome vector or the number of rows of the PCM, which is equal to $(n-k)$ bits. For the particular square lattice seen in Fig. 4, the codeword length n is equal to 13 bits and the length $(n-k)$ of the syndrome vector is equal to 6 bits. Hence, the number of information bits k is equal to 7 bits. Therefore, this code has $2^7 = 128$ legitimate codewords out of the $2^{13} = 8192$ possible received words. Based on the above-mentioned construction, for example in classical BCH codes, we would be able to distinguish $2^{(13-7)} = 2^6 = 64$ distinct error patterns (including the error free scenario) and correct a single bit error based on sphere packing bound.

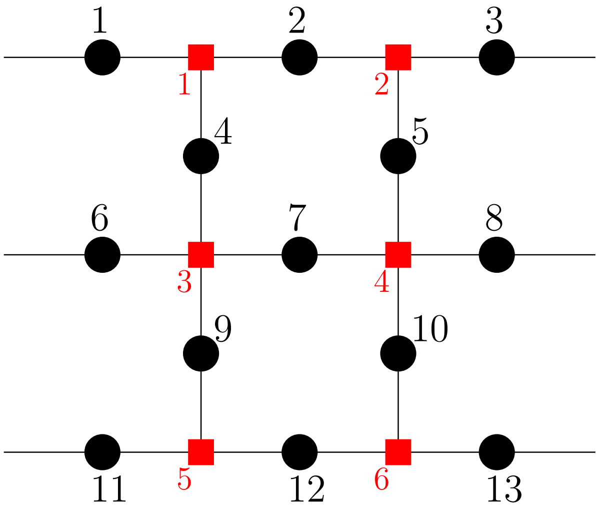


FIGURE 4. Example of a classical bit arrangement on a square lattice structure. The black circles laying on the edges of the lattice denote the bits of the codeword, while the vertices of the lattice denoted by red squares define the parity check matrix and also the syndrome values.

The coding rate r is defined by the ratio between the number of information bits k to the codeword length n, yielding:

$$r = \frac{k}{n} \tag{1}$$

Hence, the coding rate of the square lattice code of Fig. 4 is $r = 7/13$.

Now, let us delve deeper into how the error correction works. Let us revisit the square lattice of Fig. 4. The k information bits are encoded to n-bit codewords, where $n > k$. Noise or decoherence imposed by the channel corrupts the legitimate codeword. The syndrome computation is invoked to generate the $(n-k)$-bit syndrome vector, which tells us both the predicted number and the position of the errors. In Fig. 4, the i-th red square indicates a syndrome bit of s_i. Hence, the syndrome vector $\mathbf{s}$ is a 6-bit vector, which is given by

$$\mathbf{s} = [s_1 \quad s_2 \quad s_3 \quad s_4 \quad s_5 \quad s_6]. \tag{2}$$

In the case of an error-free received codeword, the resultant syndrome vector is $\mathbf{s} = [0\ 0\ 0\ 0\ 0\ 0]$. By contrast, if an error is imposed on the codeword, it triggers a syndrome bit value of 1 at the adjacent syndrome bit positions. For example, if an error occurs at the bit index 4 of Fig. 4, it triggers the syndrome values of $s_1 = 1$ and $s_3 = 1$. The rest of the syndrome values remain equal to 0. Therefore, an error corrupting the bit index 4 generates a syndrome vector of $\mathbf{s} = [1\ 0\ 1\ 0\ 0\ 0]$. Hence, the decoder flips the value of bit index 4. Similarly, if an error occurs at bit number 3, it only triggers the syndrome value of $s_2 = 1$. Hence, it generates the syndrome vector of $\mathbf{s} = [0\ 1\ 0\ 0\ 0\ 0]$ and the error recovery procedure proceeds accordingly.

Now let us consider the ocurrence of two bit errors in the codeword. For instance, let us assume that errors occur at bit indices of 6 and 7 of Fig. 4. Note that both these errors affect s_3, therefore they cancel each other effect on s_3 out, hence generating a syndrome bit value of $s_3 = 0$. However, we still do not receive an all-zero syndrome vector, because the bit index 7 results in a syndrome bit value of $s_4 = 1$ of Fig. 4. Therefore, the resultant syndrome vector due to a bit error in both bit 6 and 7 is $\mathbf{s} = [0\ 0\ 0\ 1\ 0\ 0]$. Since the syndrome vector of $\mathbf{s} = [0\,0\,0\,1\,0\,0]$ is also associated with the error incident upon bit index 8, the error recovery procedure decides to flip bit 8 instead, because a single error occurance is more likely to happen than a double-error when the error probability less than $1/2$. This example is an illustration that the occurence of two bit errors in the codeword is beyond the error correction capability of the code given in Fig. 4. We conclude that the code based on the square lattice illustrated in Fig. 4 is capable of correcting only a single bit error. The error correction capability of t bits for a given code construction is defined by the minimum distance d of the code as formulated by

$$t = \left\lfloor \frac{d-1}{2} \right\rfloor. \tag{3}$$

Hence, a code that is only capable of correcting a single error has a minimum distance of $d = 3$, as exemplified by the square lattice code given in Fig. 4. Moreover, the minimum distance of a square lattice code is defined by the dimension of the lattice. Therefore, to increase the error correction capability of the code, we can simply increase the dimension of the lattice, which directly translates into the increase of the minimum distance. The square lattice considered in our example can be generalized to a rectangular lattice structure having a dimension of $(l \times h)$, where l is the length of the lattice and h is the height of the lattice. In the case of a rectangular structure, the minimum distance is defined by

$$d = \min(l, h). \tag{4}$$

The codeword length is also uniquely defined by the dimension of the lattice. More explicitly, for a rectangular lattice of dimension $(l \times h)$, the codeword length is equal to the number of the lattice edges, which is given by

$$n\text{-edges} = n_{\text{square}} = 2lh - l - h + 1. \tag{5}$$

The number of rows in the PCM of a square lattice code is defined by the number of faces or plaquettes of the rectangular lattice, which is formulated as follows:

$$n\text{-vertices} = n_{\text{square}} - k_{\text{square}} = h(l-1). \tag{6}$$

Hence, from Eq. (5) and (6), the number of information bits k encoded by the rectangular lattice codes is

$$\begin{aligned} k_{\text{square}} &= n_{\text{square}} - (n_{\text{square}} - k_{\text{square}}) \\ &= lh - l + 1. \end{aligned} \tag{7}$$

The most efficient code can be constructed by a square lattice, where $d = l = h$. Therefore, the expression given in Eq. (5) and (7) can be simplified to

$$n_{\text{square}} = 2d^2 - 2d + 1 \tag{8}$$

$$k_{\text{square}} = d^2 - d + 1. \tag{9}$$

Hence, the coding rate of square lattice based codes can be formulated as follows:

$$r_{\text{square}} = \frac{k_{\text{square}}}{n_{\text{square}}} = \frac{d^2 - d + 1}{2d^2 - 2d + 1}. \tag{10}$$

TABLE 1. Constructing the PCM of the square lattice code of Fig. 4 with minimum distance of $d = 3$. Each row is associated with the syndrome operators denoted by red squares in Fig. 4.

	1	2	3	4	5	6	7	8	9	10	11	12	13
$\mathbf{h}_1$	1	1	0	1	0	0	0	0	0	0	0	0	0
$\mathbf{h}_2$	0	1	1	0	1	0	0	0	0	0	0	0	0
$\mathbf{h}_3$	0	0	0	1	0	1	1	0	1	0	0	0	0
$\mathbf{h}_4$	0	0	0	0	1	0	1	1	0	1	1	0	0
$\mathbf{h}_5$	0	0	0	0	0	0	0	0	1	0	1	1	0
$\mathbf{h}_6$	0	0	0	0	0	0	0	1	0	1	0	0	1

The PCM can be readily constructed in a similar fashion. Each red square of Fig. 4 represents the row of the PCM, where the adjacent black circles denote the index of the column containing a value of 1. For example, the first red square is adjacent to the black circles numbered 1, 2, and 4. Therefore, in the first row of the PCM, there are only three elements containing a value of 1 and those are marked by the index 1, 2, and 4. The remaining rows of the PCM are generated using the same principle. Explicitly, each row of the PCM of the square lattice code of Fig. 4 is portrayed in Table 1. Finally, the PCM $\mathbf{H}$ of the square lattice code of Fig. 4 is given by

$$\mathbf{H} = \begin{bmatrix} \mathbf{h}_1 \\ \mathbf{h}_2 \\ \mathbf{h}_3 \\ \mathbf{h}_4 \\ \mathbf{h}_5 \\ \mathbf{h}_6 \end{bmatrix}. \tag{11}$$

The code construction based on the general lattice structure is not limited to a rectangular lattice. Let us consider, for example the triangular lattice of Fig. 5. The black circles laying on the vertex of the lattice define the codeword and the red squares on the faces of the lattice define the syndrome vector. The error correction principle of the triangular lattice code is similar to that of its square counterpart. Hence, the PCM of the triangular lattice code is readily derived using the following equation:

$$\mathbf{H} = \begin{bmatrix} \mathbf{h}_1 \\ \mathbf{h}_2 \\ \mathbf{h}_3 \end{bmatrix}, \tag{12}$$

where $\mathbf{h}_1$, $\mathbf{h}_2$, and $\mathbf{h}_3$ correspond to the syndrome bits given in Table 2. It is important to point out that the resultant triangular lattice code is one of the possible construction for the classical $\mathcal{C}(7, 4, 3)$ Hamming code. Specifically, both codes have a codeword length of $n = 7$ and number of information bits of $k = 4$. Hence, the length of syndrome vector is 3 bits.

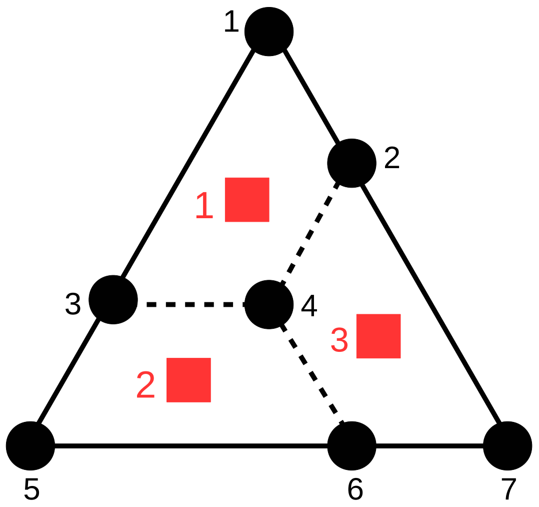


FIGURE 5. Example of a classical bit arrangement constructed over a triangular lattice structure. The black circles laying on the vertices of the lattice represent the codeword bits, while the faces or the plaquettes of the lattice denoted by red squares define the parity-check matrix and the syndrome bits of the error correction code. This configuration is an alternative representation for the $\mathcal{C}(7, 4, 3)$ classical Hamming code.

TABLE 2. Constructing the PCM of the triangular lattice code with minimum distance of $d = 3$. Each row is associated with the syndrome operators denoted by blue circles in Fig. 5.

	1	2	3	4	5	6	7
$\mathbf{h}_1$	1	1	1	1	0	0	0
$\mathbf{h}_2$	0	0	1	1	1	1	0
$\mathbf{h}_3$	0	1	0	1	0	1	1

Consequently, the codes have 2^4 legitimate codewords out of the possile 2^7 received words. Based on the sphere packing bound, the codes are capable of distinguishing $2^3 = 8$ distinct error patterns including the error-free scenario. Therefore, both constructions are capable of correcting exactly a single error with an identical coding rate of $r = 4/7$.

Similar to its rectangular counterpart, increasing the error correction capability of a triangular lattice code is achieved by expanding the underlying lattice configuration. However, increasing the number of vertices of the triangular lattice structure is not as straightforward as that of its rectangular counterpart because it can be carried out in several differennt ways. In this example, we use the construction proposed in [25] and Fig. 6 illustrates how to increase the number of encoded bits of the triangular lattice code of Fig. 5 by using hexagonal tiles.

Following the pattern of Fig. 6, the codeword length, which is also given by the number of vertices of the given lattices, is explicitly formulated as follows:

$$n\text{-vertices} = n_{\text{triangular}} = \frac{1}{4}(3d^2 + 1), \tag{13}$$

where d is the minimum distance of the code. The number of faces in the triangular lattice, which corresponds to the number of rows of the PCM and also to the syndrome vector length, can be encapsulated as

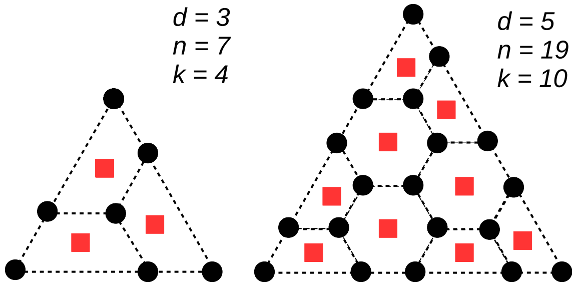


FIGURE 6. Extending the length of the triangular lattice code, which directly increases the numbers of error corrected.

$$n\text{-faces} = n_{\text{triangular}} - k_{\text{triangular}} = \frac{1}{8}(3d^2 - 3). \tag{14}$$

Hence, the number of information bits can be expressed as

$$\begin{aligned} k_{\text{triangular}} &= n_{\text{triangular}} - (n - k)_{\text{triangular}} \\ &= \frac{1}{8}(3d^2 + 5). \end{aligned} \tag{15}$$

Finally, the coding rate of the triangular lattice codes of Fig. 6 is formulated as follows:

$$r_{\text{triangular}} = \frac{k_{\text{triangular}}}{n_{\text{triangular}}} = \frac{3d^2 + 5}{2(3d^2 + 1)}. \tag{16}$$

Then, the normalized minimum distance, which directly corresponds to the error correction capability per-bit of a code may be defined as:

$$\delta = \frac{d}{n} \tag{17}$$

For square lattice and triangular lattice codes, the normalized minimum distances are given by

$$\begin{aligned} \delta_{\text{square}} &= \frac{d}{2d^2 - 2d + 1} \\ \delta_{\text{triangular}} &= \frac{4d}{3d^2 + 1}. \end{aligned} \tag{18}$$

In the rest of this treatise, we will consider the family of error correction codes based on lattice structures as a prominent representative of classical topological error correction codes (TECC). The lattice structures given in Fig. 4 and 5 can be transformed to Tanner graphs [35]. The dual representation of TECCs in the rectangular lattice domain and in the Tanner graph domain is given in Fig. 7 as exemplified by the square lattice code. We can observe that TECCs based on square lattices have a maximum row weight of $\rho_{\max} = 4$ and a maximum column weight of $\gamma_{\max} = 2$. By contrast, the codes based on triangular lattices have $\rho_{\max} = 6$ and $\gamma_{\max} = 3$. For a very long codeword, these properties lead to sparse PCMs. Hence, classical TECCs can be viewed as a specific family of LDPC codes. The asymptotical limit of the coding rate for LDPC codes based on TECCs can be directly derived from Eq. (10) and (16). As the codeword length tends to infinity

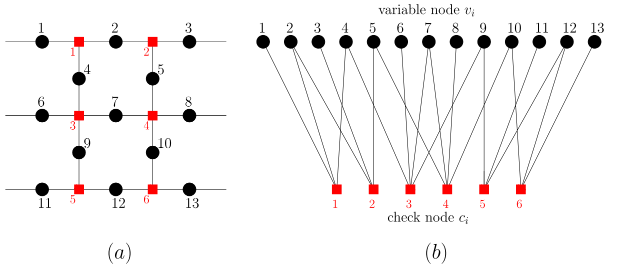


FIGURE 7. Example of how to represent the square lattice code. (a) The representation in lattice structure. (b) The representation in Tanner or bipartite graph.

$(n \to \infty)$, the minimum distance d is also expected to tend to infinity. Hence, at the asymptotical limit we have

$$r^{\infty}_{\text{square}} = \lim_{d\to\infty} \frac{d^2 - d + 1}{2d^2 - 2d + 1} = \frac{1}{2}, \tag{19}$$

$$r^{\infty}_{\text{triangular}} = \lim_{d\to\infty} \frac{3d^2 + 5}{2(3d^2 + 1)} = \frac{1}{2}. \tag{20}$$

TABLE 3. Code parameters of classical Hamming code having a single error correction capability, which is used in Fig. 8 and 9. The coding rate *r* and normalized minimum distance δ are calculated using Eq. (1) and (17), respectively.

n	k	d	n	k	d
3	1	3	127	120	3
7	4	3	255	247	3
15	11	3	511	502	3
31	26	3	1023	1013	3
63	57	3	...	...	...

Let us observe Fig. 8, where we plot the minimum distance (d) versus coding rate (r) of TECCs based on Eq. (10) and (16). We also include the classical codes based on the sphere packing concept, namely the Hamming codes and the BCH codes, whose parameters are portrayed in Table 3 and 4, respectively. We also include some labels for several codes in the figure, in order to show how to convert the code parameters into data points in the figure. More explicitly, let us consider the specific triangular codes T1 and T2, where T1 represents the triangular code having a minimum distance of 3, which we have already used in the example in Fig. 5. As it has been elaborated on earlier, the resultant code T1 is $\mathcal{C}(7, 4, 3)$. Hence, the coding rate is $r = 4/7 \approx 0.57$. Again, the triangular code T1 has identical code parameters to the Hamming code $\mathcal{C}(7, 4, 3)$, which is labeled H1. Hence, the same point in Fig. 8 represents both T1 and H1. Next, the code parameters of the triangular code T2 having a minimum distance of $d = 5$ are obtained using Eq. (13) and (15) for determining the codeword length n and the information length k, respectively. Explicitly, by substituting $d = 5$ into Eq. (13) and (15), we have $n = 19$ and $k = 10$. Finally, we arrive at the coding rate of $r = k/n = 10/19 \approx 0.53$ for the triangular code T2. The rest of the code parameters for square codes, triangular codes, Hamming codes and BCH codes are protrayed in the same way in Fig. 8.

TABLE 4. Code parameters of classical BCH codes having codeword length of $n = 255$, which is used in Fig. 8 and 9. The coding rate *r* and normalized minimum distance δ are calculated using Eq. (1) and (17), respectively.

n	k	d	n	k	d	n	k	d
255	1	255	255	87	53	255	171	23
255	9	127	255	91	51	255	179	21
255	13	119	255	99	47	255	187	19
255	21	111	255	107	45	255	191	17
255	29	95	255	115	43	255	199	15
255	37	91	255	123	39	255	207	13
255	45	87	255	131	37	255	215	11
255	47	85	255	139	31	255	223	9
255	55	63	255	147	29	255	231	7
255	63	61	255	155	27	255	239	5
255	71	59	255	163	25	255	247	3
255	79	55						

In general, increasing the minimum distance of the codes while mantaining the codeword length can be achieved at the expense of reducing the coding rate. This penomenon is perfectly reflected by the behaviour of classical BCH codes in Fig. 8. Explicitly, in Fig. 8 we portray BCH codes having a constant codeword length of $n = 255$, which are described in Table 4. As seen, upon increasing the minimum distance of BCH codes, the coding rate is gradually reduced. Next, increasing the coding rate while maintaining the minimum distance of the code can indeed be achieved by increasing the codeword length. In this case, the Hamming codes, whose code parameters are described in Table 3, reflect perfectly this phenomenon. Observe in Fig. 8, that for the Hamming codes exhibiting a constant minimum distance of $d = 3$, we can see the gradual increase of coding rate upon increasing the codeword length. However, the behaviour of the BCH and Hamming codes is not reflected by the TECCs. Let us elaborate on the TECCs behaviour in Fig. 8. The increase of minimum distance of TECCs upon increasing the codeword length looks very impressive, since they do not seem to require much sacrifice in terms of coding rate reduction. In fact, the coding rate is saturated at approximately $r = 1/2$ for long codewords. This is indeed a rather different behaviour compared to that of the classical BCH codes. However, it is of pivotal importance to mention again that the increasing error correction capability per codeword does not necessarily imply the improvement of error correction capability per bit. Therefore, we have to normalize the performance to the codeword length in order to portray a fair comparison.

Let us now observe Fig. 9, where we plot the normalized minimum distance (δ) versus the coding rate (r) of TECCs based on Eq. (18). We include both the BCH codes as well as the Hamming codes for the sake of comparison. We also plot the classical Hamming bound [36] and Gilbert-Varshamov (GV) [37] bound in this figure to portray

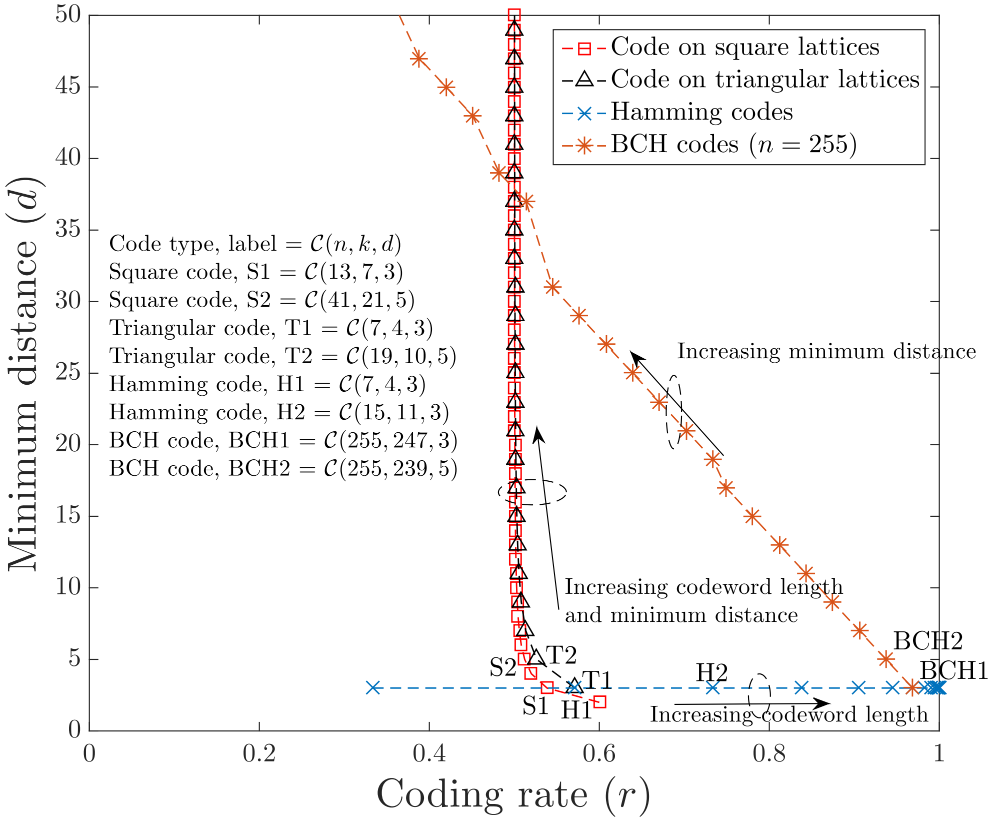


FIGURE 8. The coding rate versus minimum distance of TECCs. For asymptotical limit, the TECCs may be categorized into LPDC codes and the coding rates converge to $r = \frac{1}{2}$. We also include the BCH codes and Hamming codes for the sake of comparison. The coding rate for the square lattice based codes and the triangular lattice based codes are defined in Eq. (10) and (16), respectively. The code parameters for classical Hamming and BCH codes are described in Table 3 and 4, respectively. We put labels only for several codes as examples on how to convert the given code parameters into the figure.

the upper bound and lower bound of the normalized minimum distance, which correspond directly to the normalized error correction capability, given the coding rate. The classical Hamming bound is formulated as follows [36]:

$$\frac{k}{n} \leq 1 - H\left(\frac{d}{2n}\right), \tag{21}$$

where $H(x)$ is the binary entropy of x defined by $H(x) = -x \log_2 x - (1-x) \log_2(1-x)$, while the classical GV bound is expressed as [37]

$$\frac{k}{n} \geq 1 - H\left(\frac{d}{n}\right). \tag{22}$$

The classical Hamming bound and GV bound defined in Eq. (21) and (22) are valid for asymptotical limit where $n \to \infty$.

The classical Hamming codes constitute the so-called *perfect codes* for a finite-length, since they always achieve the Hamming bound for finite-length codes.[3] Therefore, the Hamming codes also mark the upper bound of normalized minimum distance, given the coding rate of finite-length codewords. Secondly, the classical BCH codes having a codeword length of $n = 255$ lay perfectly - as expected - between the Hamming and GV bound in the asymptotical limit, as shown in Fig. 9. However, we observe an unusual behaviour for the family of TECCs, since the normalized minimum distance drops to zero upon increasing the codeword length, while the coding rate saturates at $r = 1/2$. We hypothesize that since these codes were not designed using the sphere packing concept - which the Hamming and BCH codes are based on - the Hamming distance radius of the associated decoding sphere in the TECCs codespace is most likely to be non-identical for the different codewords. In addition, the minimum distance of TECCs is only on the order of $\mathcal{O}(\sqrt{n})$, which implies that the codeword length of TECCs is proportional to the factor of $\mathcal{O}(d^2)$. By contrast, for clasical BCH and Hamming codes the growth of the minimum distance is approximately linear, i.e. of order $\mathcal{O}(n)$. It is clearly seen that even though the growth of minimum distance per codeword of the TECCs appears to be impressive in Fig. 8, it is not fast enough to compensate for the undesired effect of the increasing codeword length. Hence, the TECC error correction capability per bit tends to zero in the asymptotical limit. Nevertheless, we leave the definitive answer for this peculiar phenomenon open for future research, since our

[3] The Hamming bound for finite length codes has a different formulation from that of asymptotical limit. Therefore, we refer to [38] for further explanations.

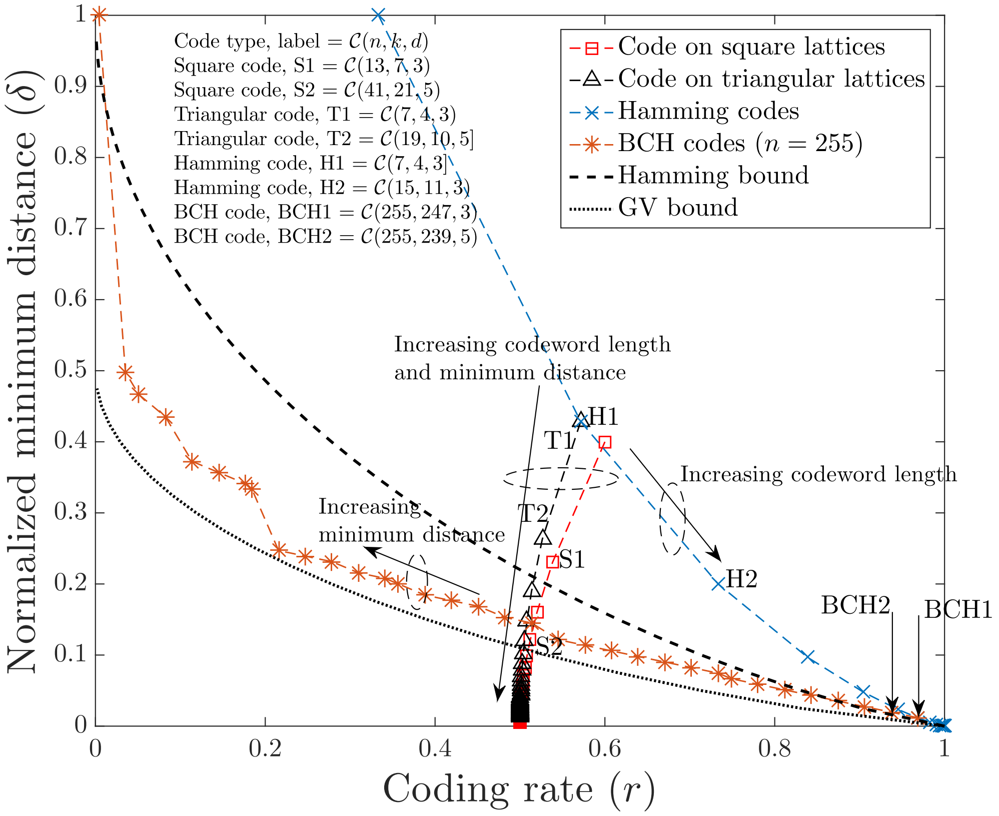


FIGURE 9. The coding rate versus normalized minimum distance of TECCs. For asymptotical limit, the TECCs may be categorized into LPDC codes and the coding rates converge to $r = \frac{1}{2}$, while the normalized minimum distances (δ) vanish to zero. In addition, we also include the classical Hamming and BCH codes, which constructed based on sphere packing bound, for the sake of comparison. The code parameters for classical Hamming and BCH codes are portrayed in Table 3 and 4, respectively. We put labels only for several codes as examples on how to convert the given code parameters into the figure.

focus in this treatise is on finding the classical-to-quantum isomorphism of TECCs.

Since the TECC associated with the asymptotical limit of $n \rightarrow \infty$ belongs to the family of LDPC codes, an efficient LDPC decoder such as the belief propagation (BP) technique [39] can be invoked for these code constructions. However, the normalized minimum distance of the LDPC codes based on topological order tends to zero, as the codeword length increases. Nevertheless, TECC-based LDPC codes exhibit several desirable code properties, such as an attractive coding rate ($r \approx 1/2$), structured construction and unbounded minimum distance. However, another aspect worth considering for TECC-based LDPC codes is the fact that we can find numerous cycles of length 4 in triangular constructions and cycles of length 6 in square constructions, which potentially degrades the performances of the codes. A brief summary of code parameters of TECC-based LDPC codes is given in Table 5.

III. THE ROAD FROM CLASSICAL TO QUANTUM ERROR CORRECTION CODES

In this section, we provide a brief review of quantum information processing. This will be followed by a rudimentary introduction of classical syndrome-based decoding and how we can demonstrate the isomorphism towards quantum stabilizer codes.

TABLE 5. The code parameters of TECC-based LDPC codes.

Parameter	Square lattice	Triangular lattice
r	$\approx \frac{1}{2}$	$\approx \frac{1}{2}$
d	$\mathcal{O}(\sqrt{n})$	$\mathcal{O}(\sqrt{n})$
δ	$\frac{d}{2d^2-2d+1}$	$\frac{4d}{3d^2+1}$
$\rho_{\max}$	4	6
$\gamma_{\max}$	2	3
Girth	6	4

A. A BRIEF REVIEW OF QUANTUM INFORMATION PROCESSING

In the classical domain the information is represented by a series of binary digits (bits), whilst in the quantum domain the information is conveyed by quantum bits (qubits). A classical bit can only hold a value of either ‘0’ or ‘1’ at a time, while the qubit can hold the value of ‘0’, ‘1’ and the superposition of both values. More specifically, the state of a single qubit can be expressed mathematically as follows:

$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle, \quad \alpha_0, \alpha_1 \in \mathbb{C}, \tag{23}$$

where $P_0 = |\alpha_0|^2$ and $P_1 = |\alpha_1|^2$ are the probability of obtaining the value of 0 and 1 upon measurement, respectively. Hence, the unitary constraint of having $|\alpha_0|^2 + |\alpha_1|^2 = 1$ is applied. Representing the pure states of '0' by the notation $|0\rangle$ and the pure state of '1' by the so-called *ket* notation $|1\rangle$,[4] as shown in Eq. (23), is referred to as the Dirac notation [40]. The pure state of $|0\rangle$ and $|1\rangle$ can also be represented as a 2-element vector in the Hilbert space $\mathcal{H}$ as follows:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{24}$$

Hence, substituting the vectors given in Eq. (24) into Eq. (23) yields:

$$|\psi\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}, \quad \alpha_0, \alpha_1 \in \mathbb{C}. \tag{25}$$

The state of a single qubit can be manipulated by using the quantum unitary transformations. A unitary transformation of U may be realized by a quantum gate, which is the elementary building block of quantum computers. All of the quantum domain unitary transformations are represented by unitary matrices to ensure that the final probability of quantum states remains 1, which can be explicitly formulated as

$$U^\dagger U = \mathbf{I}, \tag{26}$$

where $\mathbf{I}$ is an identity matrix. The Pauli gates or Pauli operators constitute a collection of unitary transformations representing the discrete set of errors that may be imposed on a single qubit. The Pauli operators are defined using the Pauli matrices, as follows:

$$\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$
$$\mathbf{Y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \mathbf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{27}$$

The Pauli matrices can be physically interpreted as a bit-flip error, phase-flip error as well as both bit-flip and phase-flip error for the Pauli matrix **X**, **Z** and **Y**, respectively. The Pauli-**I** matrix is an identity matrix corresponding to the absence of errors.

The error imposed on multi-qubit systems can be described using the Kronecker tensor product. Explicitly, for the matrices **P** and **Q** having $(a \times b)$ elements and $(x \times y)$ elements, respectively, the resultant Kronecker product is a matrix having $(ax \times by)$ elements formulated by

$$\mathbf{P} \otimes \mathbf{Q} = \begin{pmatrix} p_{11}\mathbf{Q} & \cdots & p_{1(b-1)}\mathbf{Q} & p_{1b}\mathbf{Q} \\ p_{21}\mathbf{Q} & \cdots & p_{2(b-1)}\mathbf{Q} & p_{2b}\mathbf{Q} \\ \vdots & \ddots & \vdots & \vdots \\ p_{(a-1)1}\mathbf{Q} & \cdots & p_{(a-1)(b-1)}\mathbf{Q} & p_{(a-1)b}\mathbf{Q} \\ p_{a1}\mathbf{Q} & \cdots & p_{a(b-1)}\mathbf{Q} & p_{ab}\mathbf{Q} \end{pmatrix}. \tag{28}$$

For instance, a two-qubit system is represented by the Kronecker product between a pair of two-element vectors given in Eq. (24). More explicitly, let us consider the qubit having the state of $|\psi_1\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ and another one in the state of $|\psi_2\rangle = \beta_0|0\rangle + \beta_1|1\rangle$. The superimposed state can be described as follows:

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} \otimes \begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix} = \begin{pmatrix} \alpha_0\beta_0 \\ \alpha_0\beta_1 \\ \alpha_1\beta_0 \\ \alpha_1\beta_1 \end{pmatrix}$$
$$\equiv \alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle, \tag{29}$$

where $\alpha_0, \alpha_1, \beta_0, \beta_1 \in \mathbb{C}$. It can be observed that a two-qubit state is a superposition of all four possible states that can be generated by two bits i.e. 00, 01, 10 and 11. Moreover, the unitary condition of $|\alpha_0\beta_0|^2 + |\alpha_0\beta_1|^2 + |\alpha_1\beta_0|^2 + |\alpha_1\beta_1|^2 = 1$ still holds. The Kronecker product of a pair of two-element vectors yields a vector consisting of 2^2 elements. Hence, the N-qubit systems yield all of the 2^N possible states that can be generated by an N-bit sequence. If i is the decimal representation of an N-bit sequence, the N-qubit superposition state can be expressed by the Dirac notation as follows:

$$|\psi\rangle = \sum_{i=0}^{2^N-1} \alpha_i|i\rangle \quad \text{where } \alpha_i \in \mathbb{C} \text{ and } \sum_{i=0}^{2^N-1} |\alpha_i|^2 = 1. \tag{30}$$

Since the N-qubit state is represented by a 2^N-element column vector, the unitary transformation of the N-qubit system is defined by a $(2^N \times 2^N)$ elements unitary matrix. In quantum communication, the quantum decoherence may impose a bit-flip error, phase-flip error, as well as both bit-flip and phase-flip error. For the sake of modeling the behaviour of quantum information in the presence of quantum impairments, the Pauli channel model is widely used [41]. To elaborate a little further, the Pauli channel inflicts an error $\mathcal{P} \in \mathcal{G}_n$ on the state of an N-qubit system, where each qubit may independently experience either a bit-flip error (**X**), a phase-flip error (**Z**), or both bit-flip and phase-flip error ($i\mathbf{XZ} = \mathbf{Y}$). For an N-qubit system, the general Pauli group $\mathcal{G}_n$ is represented by an N-fold tensor product of $\mathcal{G}_1$, as described below:

$$\mathcal{G}_n = \{P_1 \otimes P_2 \cdots \otimes P_n | P_j \in \mathcal{G}_1\}, \tag{31}$$

where the Pauli group $\mathcal{G}_1$ is constituted by the unitary transformations applied to a single qubit state, which is closed under multiplication and is explicitly defined as follows:

$$\mathcal{G}_1 = \{eP : P \in \{\mathbf{I}, \mathbf{X}, \mathbf{Y}, \mathbf{Z}\}, e \in \{\pm 1, \pm i\}\}. \tag{32}$$

The laws of quantum mechanics prevent us from directly transplanting the classical error correction codes into the quantum domain owing to the following obstacles:

1) **No Cloning Theorem**. In the classical domain, the basic technique of protecting the information bits in repetition coding is that of copying the same information several times. By contrast, in the quantum domain, this simple approach cannot be implemented, since no

[4] The terminology *ket* comes from the *bra-ket* notation. The *bra* notation refers to the $\langle\psi|$ notation, while *ket* notation is used for $|\psi\rangle$ notation.

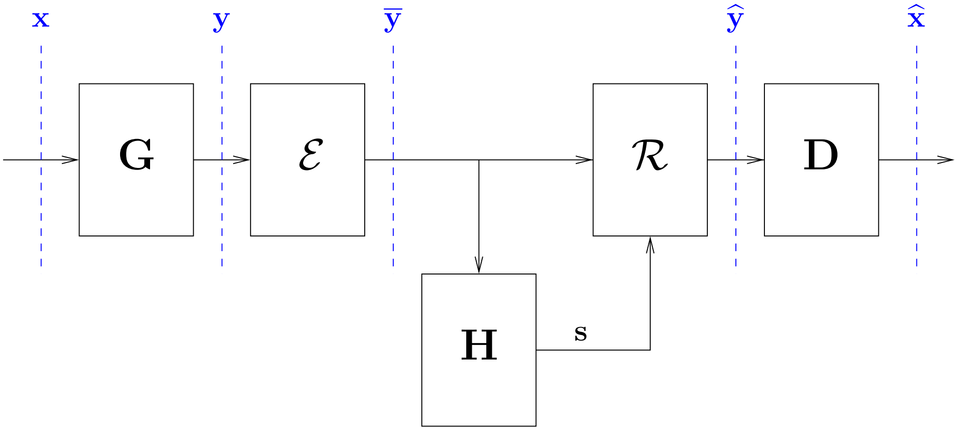


FIGURE 10. The basic model of classical error correction codes invoking syndrome-based decoding. The operation **G** denotes the generator matrix, which maps the k information bits **x** to the n coded bits **y**. The channel $\mathcal{E}$ inflicts an error vector $\mathbf{e} \in \{0,1\}^n$ upon the codeword **y**, resulting in the corrupted received bits $\bar{\mathbf{y}}$. The receiver calculates the syndrome vector **s** based on the PCM **H** and the received bits $\bar{\mathbf{y}}$ to predict the number and the position of errors contained in the received bits $\bar{\mathbf{y}}$. The error recovery $\mathcal{R}$ generates the error recovery vector **r**, which is applied to the received bits $\bar{\mathbf{y}}$. This operation collapses the received bits $\bar{\mathbf{y}}$ to one of the legitimate codedword **y**, yielding the predicted codeword $\hat{\mathbf{y}}$. Finally, we can readily determine the predicted information bits $\hat{\mathbf{x}}$ from the predicted codeword $\hat{\mathbf{y}}$.

unitary quantum transformation is capable of performing this specific task.

2) **The quantum bit collapses into the corresponding classical bit upon measurement**. In the classical domain, the error correction schemes are typically fed by measuring the bits received at the output of the demodulator. In the quantum domain, measuring the qubits represented by the superposition of the classical states will collapse the superposition into a single classical post-measurement state and consequently we lose the original quantum information.

3) **QECCs have to handle not only bit-flip errors, but also phase-flip errors, as well as the simultaneous bit-flip and phase-flip errors**. By contrast, in the classical domain, we deal with a single type of error, which is the bit-flip error. In quantum domain, the nature of quantum decoherence is continuous and it can be modeled as a linear combination of bit-flip errors ($\mathbf{X}$), phase-flip errors ($\mathbf{Z}$), or both bit-flip and phase-flip errors ($i\mathbf{XZ} = \mathbf{Y}$). However, thanks to the beneficial effect of the stabilizer measurement, the continuous nature of quantum decoherence can be treated as a discrete set of independent errors imposed on the physical qubits.

Albeit all of the aforementioned obstacles hindering the development of QECC schemes, the invention of QSC formulation succeeded in circumventing these problems.

B. A BRIEF REVIEW OF CLASSICAL SYNDROME-BASED DECODING

As mentioned earlier, the problems revolving around the QECCs are effectively circumvented by QSCs, which essentially constitute the syndrome-based decoding version of QECCs. Hence, for the sake of sheding some light onto the parallelism between the classical and quantum regime, we proceed with the classical syndrome-based decoding first.

In the classical domain a $\mathcal{C}(n,k)$ code maps k information bits into n coded bits, where $k < n$. The purpose of attaching $(n-k)$ redundant bits is to facilitate error detection or even error correction. Let us refer to Fig. 10 and consider the classical $\mathcal{C}(7,4)$ Hamming code, which maps 4 information bits into 7 coded bits and hence becomes capable of correcting a single error. In general, the mapping of the k information bits is performed by multiplying the information row vector $\mathbf{x}$ consisting of k elements by the generator matrix $\mathbf{G}$ having $(k \times n)$ elements. Explicitly, the mapping can be formulated as

$$\mathbf{y} = \mathbf{x} * \mathbf{G}, \tag{33}$$

where the resultant codeword $\mathbf{y}$ is a row vector having n elements, while the notation of $*$ represents the matrix multiplication over modulo-2. For instance, the generator matrix of the $\mathcal{C}(7,4)$ Hamming code is defined by

$$\mathbf{G}_{\text{Hamming}} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}. \tag{34}$$

From Eq. (33) and (34) we can generate the code space mapping shown in Table 6, where $\mathbf{x}_i$ denotes all the possible combination of information bits and $\mathbf{y}_i$ represents the associated legitimate codeword bits.

The generator matrix $\mathbf{G}$ can be arranged into a systematic form as

$$\mathbf{G} = (\mathbf{I}_k|\mathbf{P}), \tag{35}$$

where $\mathbf{I}_k$ is a $(k \times k)$ identity matrix and $\mathbf{P}$ is a matrix having $k \times (n-k)$ elements. The form given in Eq. (35) generates a systematic codeword $\mathbf{y}$ consisting of the k-bit information word $\mathbf{x}$ followed by $(n-k)$ parity bits. A generator matrix $\mathbf{G}$ is associated with an $(n-k) \times n$-element PCM $\mathbf{H}$, which is defined as

$$\mathbf{H} = \left(\mathbf{P}^T | \mathbf{I}_{n-k}\right). \tag{36}$$

As an example, the generator matrix of the classical $\mathcal{C}(7,4)$ Hamming code of Eq. (34) is associated with the following PCM:

$$\mathbf{H}_{\text{Hamming}} = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}. \tag{37}$$

The PCM of $\mathbf{H}$ is constructed for ensuring that a valid codeword $\mathbf{y}$ satisfies the following requirement:

$$\mathbf{y} * \mathbf{H}^T = \mathbf{0}. \tag{38}$$

A received word $\bar{\mathbf{y}}$ may be contaminated by an error vector $\mathbf{e} \in \{0,1\}^n$ due to channel impairments, which is denoted by $\mathcal{E}$ in Fig. 10. More explicitly, the resultant received words corrupted by the additive noise $\mathcal{E}$ can be formulated as

$$\bar{\mathbf{y}} = \mathbf{y} + \mathbf{e}. \tag{39}$$

The error syndrome $\mathbf{s}$ is a row vector having $(n-k)$ elements obtained by the following calculation:

$$\begin{aligned} \mathbf{s} = \bar{\mathbf{y}} * \mathbf{H}^T &= (\mathbf{y} + \mathbf{e}) * \mathbf{H}^T \\ &= \mathbf{y} * \mathbf{H}^T + \mathbf{e} * \mathbf{H}^T \\ &= \mathbf{0} + \mathbf{e} * \mathbf{H}^T \\ &= \mathbf{e} * \mathbf{H}^T. \end{aligned} \tag{40}$$

The syndrome vector $\mathbf{s}$ contains the information related to the error pattern imposed by the channel. To elaborate, we have 2^k legitimate codewords generated by the all possible combination of the k information bits, 2^n possible received bit patterns of $\widehat{\mathbf{y}}$ and $2^{(n-k)}$ possible syndromes $\mathbf{s}$, each unambiguously identifying one of the $2^{(n-k)}$ error patterns, including the error-free scenario. Hence, for the classical $\mathcal{C}(7,4)$ Hamming code, the syndrome vector $\mathbf{s}_i$ can detect and correct a single error pattern as specified in Table 7. The error recovery $\mathbf{r}_i$ is determined based on the most likely error pattern. After obtaining the syndrome vector, the recovery vector $\mathbf{r}_i$ is applied to the received words to obtain the predicted codeword $\widehat{\mathbf{y}} = \bar{\mathbf{y}} + \mathbf{r}$, as depicted in Fig. 10. The application of the recovery operator $\mathbf{r}_i$ to the received word always collapses it into one of the legitimate codewords $\mathbf{y}$, hence the predicted codeword $\widehat{\mathbf{y}}$ can be finally demapped in order to obtain the predicted information bits $\widehat{\mathbf{x}}$ using Table 6, as illustrated in Fig. 10. For linear systematic codes, this process can be simply performed by chopping the last $(n-k)$ bits, namely the redundant bits.

TABLE 6. The code space mapping of the $\mathcal{C}(7,4)$ classical Hamming code.

i	$\mathbf{x}_i$	$\mathbf{y}_i$
1	0 0 0 0	0 0 0 0 0 0 0
2	0 0 0 1	0 0 0 1 1 1 1
3	0 0 1 0	0 0 1 0 0 1 1
4	0 0 1 1	0 0 1 1 1 0 0
5	0 1 0 0	0 1 0 0 1 0 1
6	0 1 0 1	0 1 0 1 0 1 0
7	0 1 1 0	0 1 1 0 1 1 0
8	0 1 1 1	0 1 1 1 0 0 1
9	1 0 0 0	1 0 0 0 1 1 0
10	1 0 0 1	1 0 0 1 0 0 1
11	1 0 1 0	1 0 1 0 1 0 1
12	1 0 1 1	1 0 1 1 0 1 0
13	1 1 0 0	1 1 0 0 0 1 1
14	1 1 0 1	1 1 0 1 1 0 0
15	1 1 1 0	1 1 1 0 0 0 0
16	1 1 1 1	1 1 1 1 1 1 1

TABLE 7. The look-up table to determine the most likely error pattern $\mathbf{e}_i \in \mathcal{E}$ that corresponds to the syndrome value $\mathbf{s}_i$, which is created based on Eq. (37) and (40).

i	$\mathbf{s}_i$	$\mathbf{e}_i$
1	0 0 0	0 0 0 0 0 0 0
2	0 0 1	0 0 0 0 0 0 1
3	0 1 0	0 0 0 0 0 1 0
4	0 1 1	0 0 1 0 0 0 0
5	1 0 0	0 0 0 0 1 0 0
6	1 0 1	0 1 0 0 0 0 0
7	1 1 0	1 0 0 0 0 0 0
8	1 1 1	0 0 0 1 0 0 0

For more a detailed example, let us consider k information bits of $\mathbf{x} = (1\ 1\ 0\ 1)$. The information bits are encoded using the classical $\mathcal{C}(7,4)$ Hamming code employing the generator matrix of Eq. (33), yielding the coded bits of $\mathbf{y} = (1\ 1\ 0\ 1\ 1\ 0\ 0)$. Let us assume that the channel corrupts the legitimate codeword $\mathbf{y}$ by imposing an error pattern of $\mathbf{e} = (1\ 0\ 0\ 0\ 0\ 0\ 0)$ yielding the received word of $\bar{\mathbf{y}} = (0\ 1\ 0\ 1\ 1\ 0\ 0)$. Next, the received word is fed to the syndrome calculation block, which contains the PCM of Eq. (37). Based on Eq. (40), the received word $\bar{\mathbf{y}} = (0\ 1\ 0\ 1\ 1\ 0\ 0)$ generates the syndrome vector of $\mathbf{s} = (1\ 1\ 0)$. Utilizing the look-up table of Table 7, the error recovery vector becomes $\mathbf{r} = (1\ 0\ 0\ 0\ 0\ 0\ 0)$. Upon applying the error recovery vector, the received word $\bar{\mathbf{y}}$ is collapsed to one of the legitimate codewords $\mathbf{y}$ in Table 6, which is $\widehat{\mathbf{y}} = (1\ 1\ 0\ 1\ 1\ 0\ 0)$. Assuming that the predicted codeword $\widehat{\mathbf{y}}$ is valid, the demapper decides to translate the predicted codeword $\widehat{\mathbf{y}} = (1\ 1\ 0\ 1\ 1\ 0\ 0)$ to the predicted information bits as $\widehat{\mathbf{x}} = (1\ 1\ 0\ 1)$. Hence, the original information is successfully recovered. The whole process of syndrome calculation, error recovery and demapping jointly form the *decoding* process. It is important to note that in practice, the syndrome calculation, recovery operator and demapper are amalgamated into a single *decoder* block.

Let us now assume that the channel imposes an error pattern beyond the error correction capability of the classical

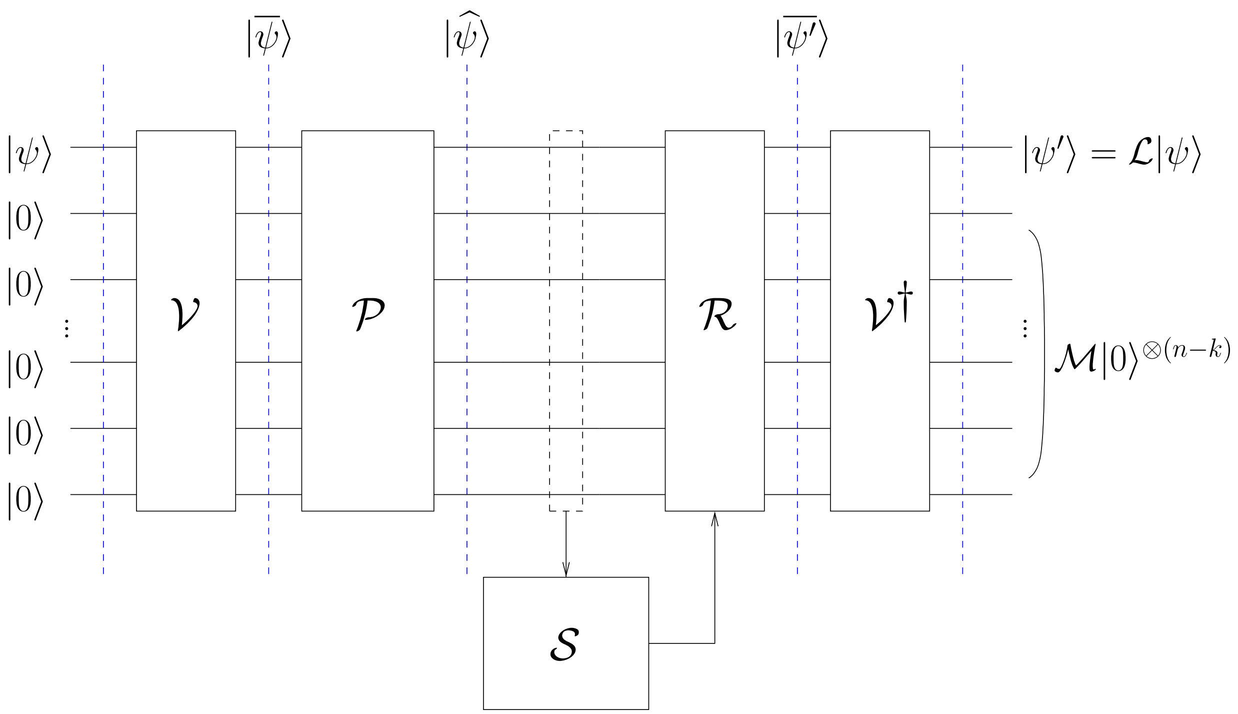


FIGURE 11. The basic model of QSCs implementation over the quantum depolarizing channel. The k logical qubits are mapped into n physical qubits with the aid of $(n-k)$ redundant/auxilliarry qubits (*ancillas*) to provide protection from the quantum decoherence. This schematic is similar to the classical error correction model where $(n-k)$ redundant bits are added to k information bits in order to provide error correction. The quantum encoder $\mathcal{V}$ serves the same purpose as G of the classical error correction codes in Fig. 10. The quantum encoder $\mathcal{V}$ transforms the state of k logical qubits $|\psi\rangle$ into the state of n physical qubits $|\overline{\psi}\rangle$ with the aid of $(n-k)$ ancillas. The quantum depolarizing channel imposes the error vector represented by the n-tupple Pauli operator $\mathcal{P} \in \mathcal{G}_n$. The syndrome operators $S_i \in \mathcal{S}$ generate the eigenvalues of ±1, which are analogous to the value 0 and 1 of the classical syndrome vector, which is provided by the PCM H in Fig. 10. The error recovery $\mathcal{R}$ applies the correction according to the syndrome values provided by the syndrome measurements. Finally, the quantum-domain inverse encoder $\mathcal{V}^{\dagger}$ transforms the predicted state of physical qubits $|\overline{\psi'}\rangle$ back to the predicted state of logical qubits $|\psi'\rangle$, which carries out the same function as the demapper D in the classical syndrome-based decoding of Fig. 10.

$\mathcal{C}(7,4)$ Hamming code. For example, assume that we send k information bits of $\mathbf{x} = (1\ 1\ 0\ 1)$, similar to that of in the previous example, while the channel inflicts an error pattern of $\mathbf{e} = (1\ 1\ 0\ 0\ 0\ 0\ 0)$. As a result, we have the received codeword bits of $\overline{\mathbf{y}} = (0\ 0\ 0\ 1\ 1\ 0\ 0)$. Based on the received codeword, we have the syndrome vector of $\mathbf{s} = (0\ 1\ 1)$. Based on the syndrome vector, the error recovery of $\mathbf{r} = (0\ 0\ 1\ 0\ 0\ 0\ 0)$ is chosen. Consequently, the error recovery vector collapses the received word to the incorrect legitimate codeword, which is $\widehat{\mathbf{y}} = (0\ 0\ 1\ 1\ 1\ 0\ 0)$, instead of the correct codeword of $\mathbf{y} = (1\ 1\ 0\ 1\ 1\ 0\ 0)$. Since the demapper assumes that the error recovery completes the task perfectly, the demapper decides that the predicted information bits are $\mathbf{x} = (0\ 0\ 1\ 1)$. Compared to the original information bits, the predicted information bits are considered as an error. This example demonstrates that the classical $\mathcal{C}(7,4)$ Hamming code is unable to operate flawlessly beyond its error correction capability.

C. A BRIEF REVIEW OF QUANTUM STABILIZER CODES

The formulation of QSCs is capable of detecting both the number and the position of errors without actually observing the state of physical qubits, which is vitally important since otherwise the quantum state will collapse to classical bits upon measurement. This was achieved by amalgamating the classical syndrome-based decoding with the QECCs. Similar to classical error correction codes, QSCs also rely on attaching redundant qubits to the information qubits for invoking error correction. The basic model of QSCs is depicted in Fig. 11, which will be contrasted to its classical pair in Fig. 10. In order to generate the codespace $\mathcal{C}$, the redundancy is constituted by $(n-k)$ auxiliary qubits. Next, a unitary transformation $\mathcal{V}$ transforms the k qubits in the state of $|\psi\rangle$ and the $(n-k)$ auxiliary qubits into an n qubits in the state of $|\overline{\psi}\rangle$. The unitary transformation of $\mathcal{V}$ represents the action of the *quantum encoder*. Explicitly, the mapping of the *logical qubits* constituting the state of $|\psi\rangle \in \mathbb{C}^{2^k}$ to the *physical qubits* forming the state of $|\overline{\psi}\rangle \in \mathbb{C}^{2^n}$ by the encoder $\mathcal{V}$ of Fig. 11 can be mathematically formulated as follows:

$$\mathcal{C} = \{|\overline{\psi}\rangle = \mathcal{V}(|\psi\rangle \otimes |0\rangle^{\otimes(n-k)})\}. \qquad (41)$$

The QSCs rely on the stabilizer operators $S_i \in \mathcal{S}$ for identifying the type, the number and also the position of the qubit errors. A stabilizer operator S_i is an n-tuple Pauli operator, which preserves the state of physical qubits as defined below:

$$S_i|\overline{\psi}\rangle = |\overline{\psi}\rangle. \qquad (42)$$

The quantum channel inflicts errors represented by n-tuple Pauli operators $\mathcal{P} \in \mathcal{G}_n$, as given in Eq. (31), which transforms the encoded physical qubits that were originally in the state of $|\overline{\psi}\rangle$ to the potentially corrupted physical qubits in the state of $|\widehat{\psi}\rangle$, as seen in Fig. 11. More explicitly, this process can be described as follows:

$$|\widehat{\psi}\rangle = \mathcal{P}|\overline{\psi}\rangle. \tag{43}$$

The stabilizer operators act similarly to the syndrome calculations routinely used in classical error correction codes. To elaborate a little further, a stabilizer operator will return an eigenvalue of $+1$, when an error operator $\mathcal{P}$ commutes with the stabilizer operator, while we arrive at the eigenvalue of -1, if it anti-commutes. The eigenvalues of $+1$ and -1 are analogous to the classic syndrome bit of 0 and 1, respectively, which can be defined as follows:

$$S_i|\widehat{\psi}\rangle = \begin{cases} |\widehat{\psi}\rangle, & S_i\mathcal{P} = \mathcal{P}S_i \\ -|\widehat{\psi}\rangle, & S_i\mathcal{P} = -\mathcal{P}S_i. \end{cases} \tag{44}$$

Therefore, the stabilizer operators naturally have to inherit the commutative property. Consequently, the product between the stabilizer operators S_i yields another legitimate stabilizer operator. Furthermore, the commutativity property implies that

$$S_i|\overline{\psi}\rangle = S_j|\overline{\psi}\rangle = S_iS_j|\overline{\psi}\rangle = |\overline{\psi}\rangle, \quad \forall S_{i,j} \in \mathcal{S}, \tag{45}$$

suggesting that the stabilizer group $\mathcal{S}$ is closed under multiplication.

Based on the syndrome measurement by the stabilizer operators S_i, a recovery operator constituted by the n-tupple Pauli operator of $\mathcal{R} \in \mathcal{G}_n$ seen in Fig. 11 is applied to the corrupted physical qubit state $|\widehat{\psi}\rangle$, yielding the predicted state of the original encoded logical qubit $|\overline{\psi'}\rangle$, which is formulated as

$$|\overline{\psi'}\rangle = \mathcal{R}|\widehat{\psi}\rangle. \tag{46}$$

Finally, the inverse encoder $\mathcal{V}^\dagger$ of Fig. 11 performs the following transformation[5]:

$$\begin{aligned} \mathcal{V}^\dagger|\overline{\psi'}\rangle &= \mathcal{V}^\dagger\mathcal{R}|\widehat{\psi}\rangle \\ &= \mathcal{V}^\dagger\mathcal{R}\mathcal{P}|\overline{\psi}\rangle \\ &= \mathcal{V}^\dagger\mathcal{R}\mathcal{P}\mathcal{V}(|\psi\rangle \otimes |0\rangle^{\otimes(n-k)}) \\ &= (\mathcal{L}|\psi\rangle) \otimes (\mathcal{M}|0\rangle^{\otimes(n-k)}), \end{aligned} \tag{47}$$

where we have $\mathcal{V}^\dagger\mathcal{R}\mathcal{P}\mathcal{V} \equiv \mathcal{L}\otimes\mathcal{M}$ and $\mathcal{L} \in \mathcal{G}_k$ represents the error inflicted on the logical qubits according to $|\psi'\rangle = \mathcal{L}|\psi\rangle$, while $\mathcal{M} \in \mathcal{G}_{n-k}$ represents the residual error remained in the $(n-k)$ auxiliary qubits after the error correction procedure. In the case of $\mathcal{R} = \mathcal{P}$, we arrive at $\mathcal{R}\mathcal{P} = \mathbf{I}^{\otimes n}$, where $\mathbf{I}^{\otimes n}$ denotes an n-fold tensor product Pauli-$\mathbf{I}$ matrix. Another possibility is to arrive at $\mathcal{R}\mathcal{P} = S_i$. In either of these cases, the state of the physical qubits is not altered, since we have $\mathcal{R}\mathcal{P}|\overline{\psi}\rangle = |\overline{\psi}\rangle$. Therefore, the decoding procedure of Fig. 11 successfully recovers the original quantum state constituted by the logical qubits, yielding $|\psi'\rangle = |\psi\rangle$.

The stabilizer operators can be translated into the classical PCM $\mathbf{H}$ by mapping the Pauli matrices $\mathbf{I}$, $\mathbf{X}$, $\mathbf{Y}$ and $\mathbf{Z}$ onto $(\mathbb{F}_2)^2$ as follows:

$$\begin{aligned} \mathbf{I} &\rightarrow (0 \mid 0), \\ \mathbf{X} &\rightarrow (0 \mid 1), \\ \mathbf{Y} &\rightarrow (1 \mid 1), \\ \mathbf{Z} &\rightarrow (1 \mid 0). \end{aligned} \tag{48}$$

This concept is also known as the *Pauli-to-binary isomorphism*. By exploiting the Pauli-to-binary isomorphism, the stabilizer operators of any QSC can be represented as a pair of PCMs $\mathbf{H}_z$ and $\mathbf{H}_z$, where $\mathbf{H}_z$ is invoked for handling the phase-flip ($\mathbf{Z}$) errors and $\mathbf{H}_x$ for handling the bit-flip ($\mathbf{X}$) errors. Explicitly, the classical PCM representation of the QSC stabilizer operators may be written as follows:

$$\mathbf{H} = (\mathbf{H}_z|\mathbf{H}_x). \tag{49}$$

The classical representation of the stabilizer operators gives the advantage of predicting and evaluating the performances of QSCs by treating them similarly to classical error correction codes. Additionally, it allows us to transform a pair of classical PCMs into the correponding quantum counterpart. However, to ensure that the commutative property is preserved in the quantum domain, a pair of classical PCMs have to satisfy the so-called *symplectic criterion* [6] given by

$$\mathbf{H}_z \cdot \mathbf{H}_x^T + \mathbf{H}_x \cdot \mathbf{H}_z^T = 0. \tag{50}$$

A special class of QSCs, namely the family of Calderbank-Shor-Steane (CSS) codes, treats the phase-flip ($\mathbf{Z}$) and bit-flip ($\mathbf{X}$) errors as two separate entities. More specifically, this can be interpreted as having the PCMs of $\mathbf{H}_z$ and $\mathbf{H}_x$ in Eq. (49) formulated as $\mathbf{H}_z = \begin{pmatrix} \mathbf{H}'_z \\ 0 \end{pmatrix}$ and $\mathbf{H}_x = \begin{pmatrix} 0 \\ \mathbf{H}'_x \end{pmatrix}$, respectively. Therefore, the binary PCM $\mathbf{H}$ can be expressed as follows:

$$\mathbf{H} = \left(\begin{array}{c|c} \mathbf{H}'_z & \mathbf{0} \\ \mathbf{0} & \mathbf{H}'_x \end{array}\right). \tag{51}$$

Consequently, the symplectic criterion given in Eq. (50) can be reduced to the following criterion:

$$\mathbf{H}'_z \cdot \mathbf{H}'^{\,T}_x = 0. \tag{52}$$

Furthermore, we can formulate a CSS code by using a PCM of $\mathbf{H}'_z = \mathbf{H}'_x$ and the resultant quantum code may be referred to as a dual-containing quantum CSS code or self-orthogonal quantum CSS code. For dual-containing CSS codes, the symplectic criterion can be further simplified to $\mathbf{H}'_z\mathbf{H}'^{\,T}_z = 0$. For a more detailed example, please refer to [38].

[5] The inverse encoder $\mathcal{V}^\dagger$ is the Hermitian transpose of encoder $\mathcal{V}$. It is referred to as the *inverse*, since it satisfies the unitary requirement of $\mathcal{V}^\dagger\mathcal{V} = \mathbf{I}$, as the inverse of the matrix does.

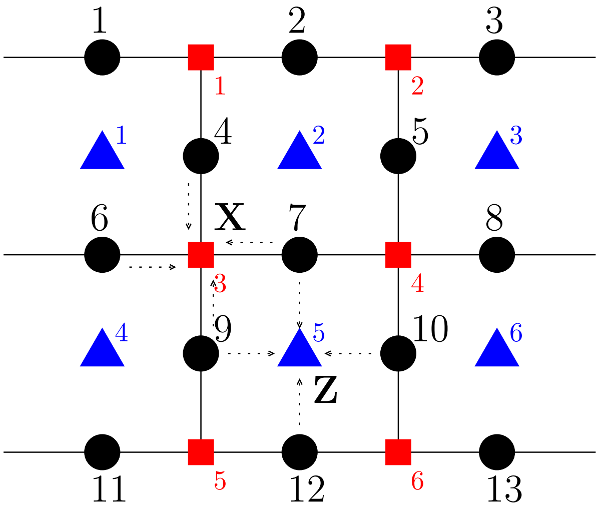


FIGURE 12. Example of qubit arrangement on a rectangular lattice structure. The black circle-based qubits on the edges of the lattice represent the physical qubits or the encoded state, the red square-based qubits lying on the vertices of the lattice act as the **X** stabilizer operators, while the blue triangle-based qubits lying on the plaquettes (faces) of the lattice constitute the **Z** stabilizer operators.

IV. QUANTUM TOPOLOGICAL ERROR CORRECTION CODES: DESIGN EXAMPLES

Let us now delve deeper into the TECC concept in the quantum domain. The quantum version of TECCs, namely the QTECCs, constitute a member of the QSC family, whose stabilizer operators are defined by the underlying lattice structure. This formalism offers several benefits for the implementation of quantum computers. Firstly, it explicitly accommodates the physical implementation of quantum memory by mapping the qubits to the lattice arrangement exemplified by Fig. 4 and 5. Secondly, the localized nature of the stabilizer measurements confines the interaction amongst qubits and also eliminates the interaction of qubits associated with a specific quantum gate that physically far from each other. Thirdly, the number of errors corrected can be increased simply by extending the size of the lattice. For now, let us assume having a square lattice structure similiar to Fig. 4 for defining the stabilizer operators of a surface code illustrated in Fig. 12 [24]. Explicitly, surface codes represent the quantum equivalent of classical TECCs on rectangular lattice structures. The physical qubits are portrayed by the black circles laying on the edge of the lattice, the **X** stabilizer operators are defined by the red squares on the lattice vertices, while the **Z** stabilizers are defined by the blue triangles on the lattice plaquettes (faces). The stabilizer operators of QTECCs are defined as follows:

$$A_v = \prod_{i \in \text{vertex}(v)} \mathbf{X}_i, \quad B_p = \prod_{i \in \text{plaquette}(p)} \mathbf{Z}_i, \tag{53}$$

where i indicates the index of stabilizer operators containing the Pauli matrix **X** as well as **Z** and the rest of the stabilizer operators are given by the Pauli identity matrix **I**. Hence, the encoded state of the physical qubits of QTECCs is constrained within a code space $\mathcal{C}$ satisfying

$$\mathcal{C} = \{|\overline{\psi}\rangle \in \mathcal{H} | A_v|\overline{\psi}\rangle = |\overline{\psi}\rangle, B_p|\overline{\psi}\rangle = |\overline{\psi}\rangle; \forall v, p\}. \tag{54}$$

More specifically, let us revisit Fig. 12 for exemplifying the construction of the stabilizer operators of a QTECC, namely of the surface codes, which is one of the QTECC constructions whose stabilizer operators are defined by a rectangular lattice structure [24]. For instance, the red square on the vertex number 3 of Fig. 12 represents the **X** stabilizer operator of $A_3 = \mathbf{X}_4\mathbf{X}_6\mathbf{X}_7\mathbf{X}_9$[6] as seen in the row S_3 of Table 8. Similarly, the blue triangle on the plaquette number 5 of Fig. 12 defines the **Z** stabilizer operator of $B_5 = \mathbf{Z}_7\mathbf{Z}_9\mathbf{Z}_{10}\mathbf{Z}_{12}$ as seen in the line B_5 of Table 8. By performing the same evaluation for all of the red squares and blue triangles, we arrive at the stabilizer operators for the quantum surface codes, as listed in Table 8.

TABLE 8. The stabilizer operators (S_i) of the quantum surface code having the lattice construction of Fig. 12. The code has a minimum distance of 3 ($d = 3$), which means that it is only capable of correcting a single qubit error.

S_i	A_v	S_i	B_p
S_1	$\mathbf{X}_1\mathbf{X}_2\mathbf{X}_4$	S_7	$\mathbf{Z}_1\mathbf{Z}_4\mathbf{Z}_6$
S_2	$\mathbf{X}_2\mathbf{X}_3\mathbf{X}_5$	S_8	$\mathbf{Z}_2\mathbf{Z}_4\mathbf{Z}_5\mathbf{Z}_7$
S_3	$\mathbf{X}_4\mathbf{X}_6\mathbf{X}_7\mathbf{X}_9$	S_9	$\mathbf{Z}_3\mathbf{Z}_5\mathbf{Z}_8$
S_4	$\mathbf{X}_5\mathbf{X}_7\mathbf{X}_8\mathbf{X}_{10}$	S_{10}	$\mathbf{Z}_6\mathbf{Z}_9\mathbf{Z}_{11}$
S_5	$\mathbf{X}_9\mathbf{X}_{11}\mathbf{X}_{12}$	S_{11}	$\mathbf{Z}_7\mathbf{Z}_9\mathbf{Z}_{10}\mathbf{Z}_{12}$
S_6	$\mathbf{X}_{10}\mathbf{X}_{12}\mathbf{X}_{13}$	S_{12}	$\mathbf{Z}_8\mathbf{Z}_{10}\mathbf{Z}_{13}$

Let us now consider an example of how the error correction procedure works using the QTECCs, which is similar to the classical TECCs, by revisiting Fig. 12. For instance, let assume that the quantum decoherence imposes a bit-flip (**X**) error on the physical qubit index 7. Since, the **X**-type error commutes with the **Z** stabilizer operators, which are represented by the blue triangles, the adjacent **Z** stabilizer operators return the eigenstate values of -1 upon measurement. Consequently, the **Z** stabilizer measurements yield a syndrome vector of $\mathbf{s}_z = [0\ 1\ 0\ 0\ 1\ 0]$, where only the vector elements of $i = 2, 5$ have the value of 1. For the short block code considered in Fig. 12, the error recovery operators $\mathcal{R}$ of Fig. 11 are determined based on hard-decision maximum-likelihood (ML) decoding, which is translated into a simple look-up table (LUT) decoder. Therefore, based on the syndrome vector of $\mathbf{s}_z$, the error recovery operator $\mathcal{R}$ of Fig. 11 is given by $\mathcal{R} = \mathbf{X}_7$. Likewise, let us now assume that the qubit on index 7 also suffers from a **Z**-type error imposed by the quantum channel. The associated syndrome vector gleaned from the **X** stabilizer operators is $\mathbf{s}_x = [0\ 0\ 1\ 1\ 0\ 0]$, where only the vector elements of $i = 3, 4$ have the value of 1. Thus, based on the syndrome vector of $\mathbf{s}_x$, the decoder applies the error recovery operator of $\mathcal{R} = \mathbf{Z}_7$.

[6] This representation is used for simplifying the original stabilizer operator of $A_3 = \mathbf{I}_1 \otimes \mathbf{I}_2 \otimes \mathbf{I}_3 \otimes \mathbf{X}_4 \otimes \mathbf{I}_5 \otimes \mathbf{X}_6 \otimes \mathbf{X}_7 \otimes \mathbf{I}_8 \otimes \mathbf{X}_9 \otimes \mathbf{I}_{10} \otimes \mathbf{I}_{11} \otimes \mathbf{I}_{12} \otimes \mathbf{I}_{13}$. For the rest of this paper, the simplified notation is used.

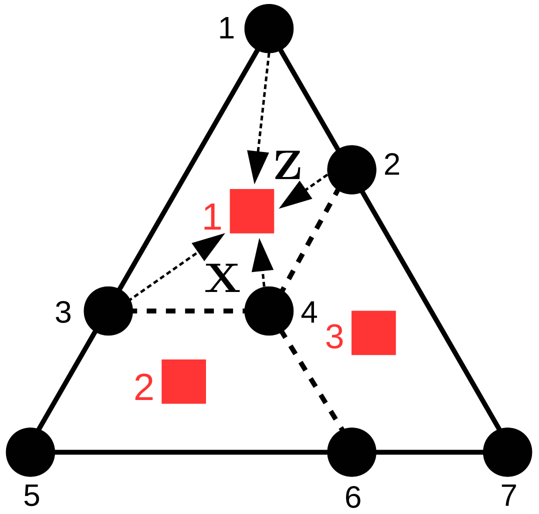


FIGURE 13. Example of a qubit arrangement for colour code, which is a type of QTECCs whose stabilizer operators are defined by a triangular lattice structure. The black circles-based qubits on the vertices of the lattice represent the physical qubits, while the faces or the plaquettes of the lattice denoted by red squares define stabilizer operators of the colour code. The resultant code has a minimum distance of $d = 3$ and hence becomes capable of correcting a single qubit error. This specific configuration bears a resemblance to the $\mathcal{C}[7, 1, 3]$ Steane's 7 qubit code.

Again, similar to the classical TECCs, the construction of QTECCs is indeed not limited to the square lattice structure. Let us now elaborate on another construction inspired by the construction proposed in [25] using the triangular lattice based on the classic example of Fig. 5. In the proposal of [25], this specific code construction is often referred to as the (triangular) colour code, since the underlying triangular lattice is composed by the tri-coloured hexagonal tiles. However, constructing the stabilizer operators of colour codes slightly differs from that of the surface codes. The colour codes use the lattice plaquettes to define both the $\mathbf{Z}$ and $\mathbf{X}$ stabilizer operators. Consequently, the resultant colour codes belong to the family of dual-containing CSS codes, which is in contrast to the surface codes that belong to the class of non-dual-containing CSS codes. For colour codes, defining both the $\mathbf{Z}$ and $\mathbf{X}$ stabilizer operators using the same plaquette always guarantees satisfying the symplectic criterion of Eq. (50). However, for surface codes, we cannot always satisfy the symplectic criterion by using the same procedure. Therefore, the dual of the lattice is used for defining half of the stabilizer operators of the surface codes in order to satisfy the symplectic criterion.[7]

Let us consider Fig. 13 for constructing the stabilizer operators of distance-3 colour codes, which are only capable of correcting a single qubit error. The plaquette denoted by red square at index 3 is used to define both the $\mathbf{Z}$ and $\mathbf{X}$ stabilizer operators. Thus, the resultant $\mathbf{X}$ stabilizer operator is $A_3 = \mathbf{X}_2\mathbf{X}_4\mathbf{X}_6\mathbf{X}_7$ and the resultant of $\mathbf{Z}$ stabilizer operator is $B_3 = \mathbf{Z}_2\mathbf{Z}_4\mathbf{Z}_6\mathbf{Z}_7$. The stabilizer operators for the colour code having the minimum distance 3 in Fig. 13 are listed in Table 9. We can observe that the colour code of Fig. 13 exhibits a strong resemblance to Steane's 7-qubit code.

TABLE 9. The stabilizer operators (S_i) of the colour code seen in Fig. 13. The code has a minimum distance of 3 ($d = 3$), which means that it is only capable of correcting a single qubit error.

S_i	A_p	S_i	B_p
S_1	$\mathbf{X}_1\mathbf{X}_2\mathbf{X}_3\mathbf{X}_4$	S_4	$\mathbf{Z}_1\mathbf{Z}_2\mathbf{Z}_3\mathbf{Z}_4$
S_2	$\mathbf{X}_3\mathbf{X}_4\mathbf{X}_5\mathbf{X}_6$	S_5	$\mathbf{Z}_3\mathbf{Z}_4\mathbf{Z}_5\mathbf{Z}_6$
S_3	$\mathbf{X}_2\mathbf{X}_4\mathbf{X}_6\mathbf{X}_7$	S_6	$\mathbf{Z}_2\mathbf{Z}_4\mathbf{Z}_6\mathbf{Z}_7$

To draw on the parallelism between classical TECCs and QTECCs, let us consider the stabilizer operators of the colour code having a minimum distance of $d = 3$, as seen in Table 9. Since the distance-3 colour code belongs to the family of quantum CSS codes, the PCM $\mathbf{H}$ obtained by using Eq. (48) and (51) is encapsulted as follows:

A CSS stabilizer code $\mathcal{C}[n, k, d]$ having $(n - k)$ stabilizer operators can be portrayed as a classical code having a PCM $\mathbf{H}$ containing $(n-k) \times 2n$ elements. Therefore, the coding rate of the classical dual of a quantum CSS code can be expressed as follows [11]:

$$\begin{aligned} r_C &= \frac{2n - (n-k)}{2n}, \\ &= \frac{n+k}{2n}, \\ &= \frac{1}{2}\left(1 + \frac{k}{n}\right), \\ &= \frac{1}{2}\left(1 + r_Q\right), \end{aligned} \tag{56}$$

where r_C is the coding rate of the classical dual of the stabilizer code $C[n, k, d]$ exhibiting a quantum coding rate of r_Q. The relationship between the classical and quantum coding rate in Eq. (56) can be rewritten as

$$r_Q = 2r_C - 1. \tag{57}$$

For instance, let us consider the distance-3 colour codes $\mathcal{C}[n, k, d] = \mathcal{C}[7, 1, 3]$, as exemplified in Fig. 13, and its classsical dual $\mathcal{C}(n, k, d) = \mathcal{C}(7, 4, 3)$,[8] as seen in Fig. 5. Explicitly, we have the classical coding rate of $r_C = 4/7$ for the $\mathcal{C}(7, 4, 3)$ code. By substituting $r_C = 4/7$ into Eq. (57), we obtain the quantum coding rate for its quantum counterpart as $r_Q = 1/7$, which is the quantum coding rate of distance-3 colour code $\mathcal{C}[7, 1, 3]$. The same goes for the classical square codes and their quantum counterpart, namely for the surface codes. Let us consider the distance-5 classical square code, which is labeled by S2 in Fig. 8 and its quantum pair, which is labeled by S2 in Fig. 14. We can readily determine the quantum coding rate of the surface code S2 $\mathcal{C}[41, 1, 5]$, which is $r_Q = 1/41$. Therefore, by substituting $r_Q = 1/41$ into Eq. (56), we arrive at the coding rate of its classical dual given by $r_C = 21/41$, which is indeed the coding rate of the classical square code S2 $\mathcal{C}(41, 21, 5)$.

[7] The dual of a lattice or a graph G is the graph that has a vertex for each plaquette of the graph.

[8] To avoid ambiguity, we use the notation $\mathcal{C}(n, k, d)$ for classical error correction codes and $\mathcal{C}[n, k, d]$ for quantum stabilizer codes.

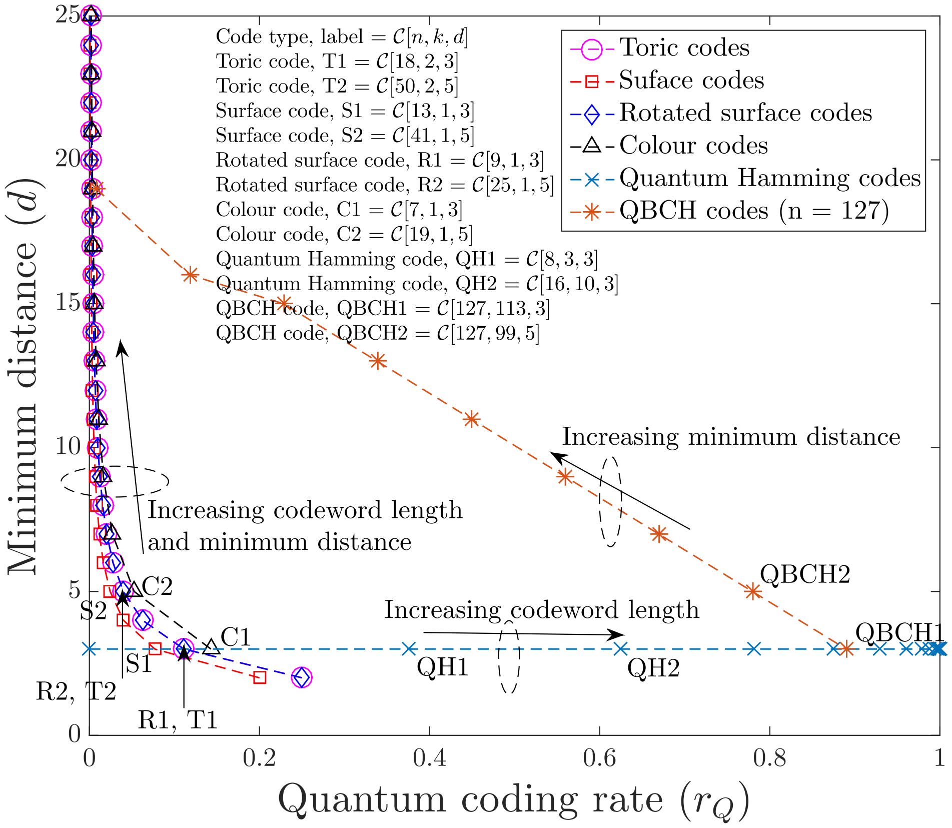


FIGURE 14. The minimum distance (d) versus quantum coding rate (r_Q) of QTECCs based on the code parameter given in Table 10. For QTECCs, the quantum coding rate tends to zero as we increase the minimum distance. We also include quantum Hamming codes and the QBCH codes having $n = 127$ physical qubits for the sake of comparing the QTECCs with the non-topological QSCs. The parameters of quantum Hamming codes and QBCH codes are listed in Table 11 and 12, respectively.

TABLE 10. The code parameters for various QTECCs based on the minimum distance d of the code.

Codes type	Dimension	Number of physical qubits	Number of stabilizers	Number of logical qubits
Colour	d^*	$\frac{1}{4}\left(3d^2+1\right)$	$\frac{1}{4}\left(3d^2-3\right)$	1
Rotated-surface	$d \times d$	d^2	d^2-1	1
Surface	$d \times d$	$2d^2-2d+1$	$2d^2-2d$	1
Toric	$d \times d$	$2d^2$	$2d^2-2$	2

* for triangular colour codes the dimension is defined by the side length of the equilateral triangle

Similar to their classical counterparts, the code parameters of QTECCs, such as the number of logical qubits k, the number of physical qubits n, the minimum distance of the code d, as well as the quantum coding rate r_Q, depend on the size of the lattices. Following the same line of investigation as for the classical TECCs, we derive the complete formulation for the number of logical qubits k and the number of physical qubits n as a function of the minimum distance of the codes, which is given in Table 10. We plot the minimum distance (d) versus quantum coding rate (r_Q) of QTECCs in Fig. 14 for colour codes [25], for rotated surface codes [31], for surface codes [24] and for toric codes [22]. We also include the non-topological QSCs, namely the QBCH codes [7] having $n = 127$ physical qubits and the quantum Hamming codes, which constitute the quantum analogue of Hamming bound-achieving code constructions [42]. Similarly to the

$$\mathbf{H} = \left(\begin{array}{ccccccc|ccccccc}
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1
\end{array}\right). \tag{55}$$

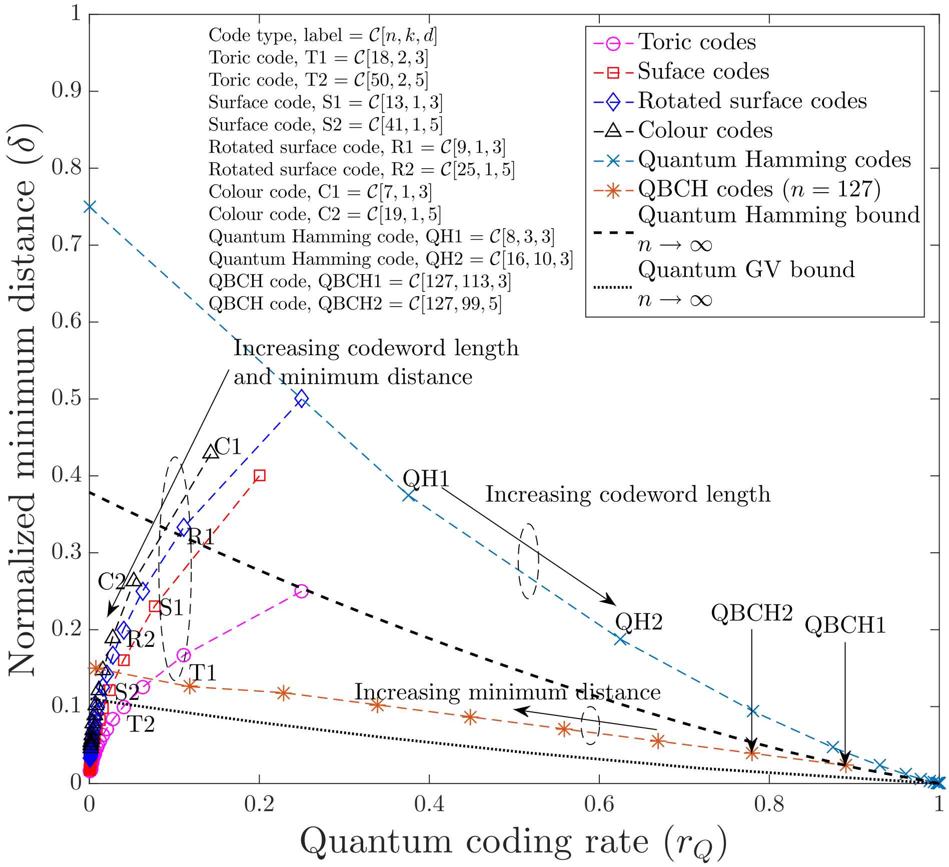


FIGURE 15. The normalized minimum distance versus quantum coding rate of QTECCs based on parameter given in Table 10. For QTECCs, the normalized minimum distance and quantum coding rate tend to zero as we increase the minimum distance. We also include the QBCH codes having the physical qubits of $n = 127$, quantum Hamming codes, quantum Hamming bound and also quantum GV bound for CSS codes for the sake of comparing the QTECCs with the non-topological QSCs.

TABLE 11. Code parameters of quantum Hamming codes having a single error correction capability, which is used in Fig. 14 and 15. The quantum coding rate r_Q and normalized minimum distance δ are calculated using Eq. (1) and (17), respectively.

n	k	d	n	k	d
8	3	3	256	246	3
16	10	3	512	501	3
32	25	3	1024	1012	3
64	56	3	2048	2035	3
128	119	3	...	...	...

classical domain, the behaviour of both the QBCH codes and the quantum Hamming codes is as expected, exhibiting the behaviour inherited from their classical analogues. However, it is interesting to observe that the quantum coding rate of QTECCs tends to zero for long codewords. Nevertheless, this phenomenon is expected, if we consider the classical to quantum isomorphism in the context of the coding rate given in Eq. (56) and (57). For the classical TECCs, the coding rate r_C approaches the value of $r_C = 1/2$ for long codewords. Hence, by substituting $r_C = 1/2$ into Eq. (57), we arrive at $r_Q = 0$, which is the phenomenon we observe in Fig. 14.

TABLE 12. Code parameters of QBCH codes having codeword length of $n = 127$, which is used in Fig. 14 and 15. The quantum coding rate r_Q and normalized minimum distance δ are calculated using Eq. (1) and (17), respectively.

n	k	d	n	k	d
127	1	19	127	71	9
127	15	16	127	85	7
127	29	15	127	99	5
127	43	13	127	113	3
127	57	11			

Next, we plot the normalized minimum distance (δ) versus the quantum coding rate (r_Q) in Fig. 15. Once again, for the sake of comparison, we also include the quantum Hamming bound [43] and the quantum GV bound derived for CSS codes [44] in addition to the QBCH codes and the quantum Hamming codes. The quantum Hamming bound is defined by [43]

$$\frac{k}{n} \leq 1 - \left(\frac{d}{2n}\right) \log_2 3 - H\left(\frac{d}{2n}\right), \tag{58}$$

while the quantum GV bound for CSS codes is given by [44]

$$\frac{k}{n} \geq 1 - 2H\left(\frac{d}{n}\right). \tag{59}$$

Both the quantum Hamming bound and the quantum GV bound of Fig. 15 serve the same purpose as the classical Hamming bound and the GV bound seen in Fig. 9. Explicitly, they portray the upper bound and the lower bound of normalized minimum distance versus quantum coding rate trade-off. Once again, the puzzling behaviour of classical TECCs resurfaces for the QTECCs, as observed in Fig. 15. Since all the QBCH codes, quantum Hamming codes and QTECCs inherit the properties of their classical counterparts, their behaviour is reminiscent of that of their classical counterparts. As for the QTECCs, the definitive interpretation of this unusual behaviour is left for future exploration in our research. Nonetheless, for a relatively long codeword, the QTECCs are reminiscent of QLDPC codes. Observe from Fig. 15 that both the normalized minimum distance and the quantum coding rate of QTECCs tend to zero upon increasing the minimum distance by increasing the codeword length. Therefore, the QTECCs are deemed to be more favourable for short to medium codeword lengths.

V. PERFORMANCE OF QUANTUM TOPOLOGICAL ERROR CORRECTION CODES

In this treatise, we consider the performance of QTECCs under the popular quantum depolarizing channel. Explicitly, the quantum depolarizing channel is characterized by the quantum depolarizing probability p inflicting an error pattern constituted by the Pauli operators $\mathcal{P} \in \mathcal{G}_n$ upon the state of physical qubits, where each qubit may independently experience a bit-flip error (**X**), a phase-flip error (**Z**), or both bit-flip and phase-flip error (**Y**) with an equal probability of $p/3$. In order to get a more precise insight into the performance trends of QTECCs, we have to distinguish how the different error patterns affect the state representing the physical qubits. Explicitly, the n-tupple Pauli error pattern may be classified as follows, which will be exemplified in Fig. 16 and 17 after their definitions:

1) **Harmful detected error pattern**. This specific type of error pattern has a similarity to the conventional bit error in the classical domain. The error pattern of $\mathcal{P}$ anti-commutes with the stabilizer operators $S_i \in \mathcal{S}$, hence triggers non-trivial syndrome values.
2) **Harmful undetected error pattern**. The error pattern commutes with all of the stabilizer operators, except that it does not belong to the stabilizer group $\mathcal{S}$. In the classical domain, this is similar to the error pattern that returns the all-zero syndrome. The error pattern is harmful, since it does not trigger a non-trivial syndrome value, yet it corrupts the legitimate state of the physical qubits.
3) **Harmless undetected error pattern**. This particular error pattern does not have any classical analogue. The error pattern is harmless, because it belongs to the stabilizer group $\mathcal{S}$. This is also referred to as a degenerate error pattern. Consequently, the error patttern does not alter the legitimate state of the physical qubits. By considering the degeneracy, the actual performances of QTECCs are potentially improved.

In order to illustrate both the harmless and harmful undetected error patterns, we refer to Fig. 16 and 17. First, we commence with the harmless undetected error pattern, which is illustrated in Fig. 16. In this example, we consider a surface code having a minimum distance of 5, which implies that it is only capable of correcting two qubit errors. Following the stabilizer formulation of QTECCs discussed in Section IV, the physical qubits are arranged along the edges of the square lattice, while the **X** stabilizer operators are located in the vertices. Therefore, the **X** stabilizer operators on the vertices are used for indicating the **Z** errors, which will trigger eigenvalues of -1 if they anticommute with the **X** stabilizer operators. Let us assume that the quantum depolarizing channel inflicts three **Z** errors on the physical qubits, which are denoted by the filled black circles in Fig 16, while the hollow black circles represent the error free physical qubits. All of the error patterns given in Fig 16 (a), (b), and (c) trigger the eigenvalues of -1 for the stabilizer operators denoted by filled red squares, while the rest of the stabilizer operators are represented by hollow red squares, which return eigenvalues of $+1$. Since the decoder relies on hard-decision ML decoding, all of the error patterns given in Fig. 16 (a), (b), and (c) have the same probability of occurence. Let us assume that the decoder always decides to apply the error recovery pattern of Fig. 16 (a) for the specified values of stabilizer measurement. When the actual error pattern is the one given in Fig. 16 (a), the states of the physical qubits are fully recovered. By contrast, if the actual error pattern is the one seen in Fig. 16 (b), but it is corrected using the error recovery operator of Fig. 16 (a), we arrive at the accumulated error pattern shown in Fig. 16 (d). Lastly, when the actual error pattern is the one given by Fig. 16 (c), but we attempt to correct it using the error recovery of Fig. 16 (a), we obtain the error pattern seen Fig. 16 (e). However, if we observe closely the error pattern illustrated in Fig. 16 (d), it is reminiscent of a plaquette **Z** stabilizer operator denoted by the filled blue triangle. Therefore, based on the definition of stabilizer operators, the error pattern given in Fig. 16 (d) does not alter the legitimate state of physical qubits. Similarly, the error pattern of Fig. 16 (e) resembles the product of two adjacent plaquette stabilizer operators. Since the product between a pair of stabilizer operators return another valid stabilizer operator, the error pattern given in Fig. 16 (e) belongs to the stabilizer group $\mathcal{S}$. Once again, by definition, the error pattern given in Fig. 16 (e) does not corrupt the legitimate state of physical qubits. This is an example of *harmless undetectable error patterns*.

To elaborate a little further, a harmless undetected error can be directly generated by the quantum decoherence, where the Pauli operator $\mathcal{P} \in \mathcal{G}_n$ imposed by the quantum depolarizing channel is identical to the stabilizer operator S_i. Another possibility is that it is generated by the associated error recovery procedure, when trying to recover an ambiguous error pattern, where there are more than one possible error patterns associated with a specific syndrome value, as illustrated in

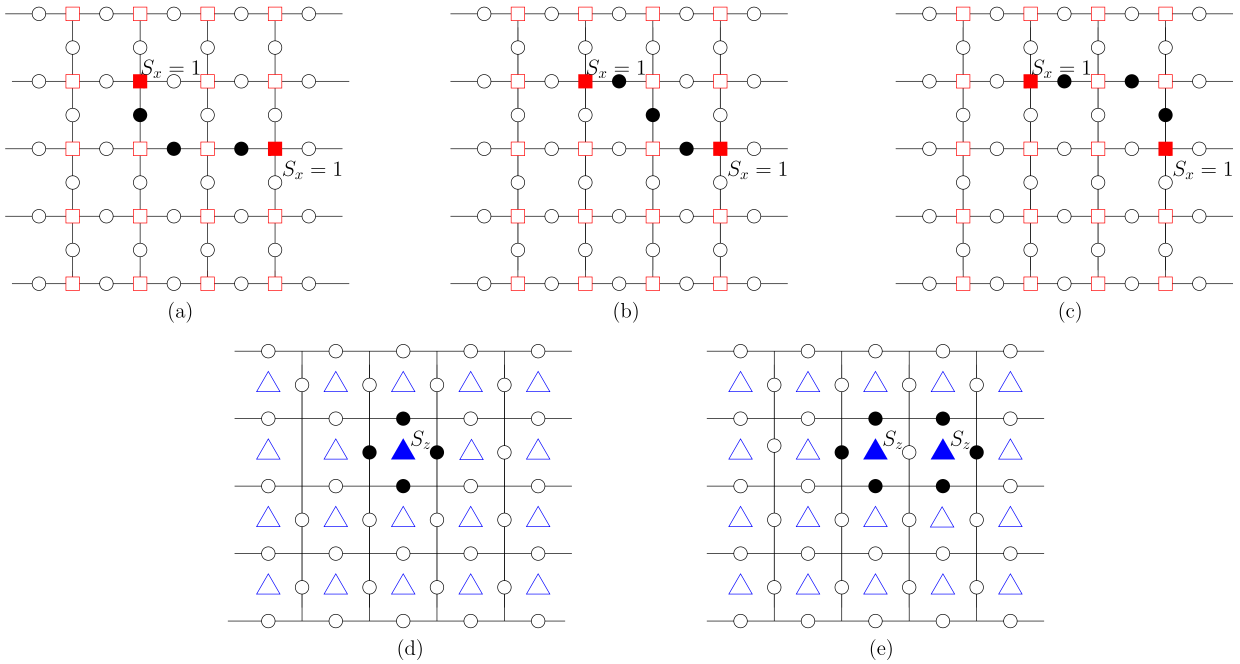


FIGURE 16. **Illustration of how the error recovery operator $\mathcal{R}$ creates the degenerate error patterns and how the degeneracy nature of QECCs may improve the performance of QTECCs. All of error patterns given in (a), (b) and (c) represent error patterns generating an identical syndrome value. Without lose of generality, let us assume that based on the generated syndrome value, the decoder always decides to perform error recovery operator $\mathcal{R}$ of (a) on the corrupted state of physical qubits. If the actual error pattern is (a), the corrupted state of physical qubits will be fully recovered. By contrast, figure (d) shows the resultant error pattern if the actual error pattern is (b), but it is corrected using the error pattern given in (a). Moreover, figure (e) represents the resultant error pattern if the actual error pattern is (c) and it is corrected using the error recovery pattern of (a). As the result, the error pattern (d) represents a stabilizer operator of a plaquette, while the error pattern (e) resembles the product of two adjacent stabilizer operators. Both error patterns of (d) and (e) constitute the *harmless undetecteable error patterns*, since they belong to the stabilizer group $\mathcal{S}$. Therefore, the state of physical qubits is not altered after the recovery operator $\mathcal{R}$ of (a) is applied to all error patterns of (a), (b) and (c). In classical set up, both error patterns (d) and (e) are considered as error events. However, in quantum domain, both error patterns (d) and (e) are considered as error-free cases. This specific error-type has no similarity in quantum domain and hence potentially improves the performance of QTECCs.**

Fig. 16. The degeneracy property, which is associated with the harmless undetectable error patterns, does not have a classical analogue, because in the classical setup, the resultant error patterns illustrated in Fig. 16 (d) and (e) will always be considered as an error. Ultimately, considering the degeneracy potentially improves the performance of QECCs.

Let us consider a range of different scenario for illustrating the presence of harmful undetected error patterns, which is portrayed in Fig. 17. Similar to the previous example of Fig. 16, three $\mathbf{Z}$ errors are imposed on the state of logical qubits by the quantum depolarizing channel. The error patterns given in Fig. 17 (a) and (b) trigger the eigenvalues of -1 for the stabilizer operators denoted by filled red squares in Fig. 17, while the rest of the stabilizer operators represented by hollow red squares return eigenvalues of $+1$. Given the associated syndrome value, the decoder always decides to apply the error recovery operator of Fig. 17 (a). In the specific scenario, where the actual error pattern is the one given by Fig. 17 (b), the resultant error pattern is given in Fig. 17 (c). We can observe that the resultant error pattern of Fig. 17 (c) commutes with all of the stabilizer operators in Fig. 17. However, this specific error pattern does not belong to the stabilizer operator $\mathcal{S}$, since we cannot represent a chain of errors by the product of stabilizer operators. Consequently, this undetectable error pattern inevitably corrupts the legitimate state representing the physical qubits. This is an example of the *harmful undetectable error patterns*. This error pattern is similar to that of its counterpart in the classical domain, where the error pattern returns the all-zero syndrome.

Therefore, based on these conditions, by modifying the probabilty of correct decoding in the classical domain [45], we can readily formulate the worst-case upper-bound QBER performance of QTECCs as

$$\text{QBER}_{\text{upper}}(n, d, p) = 1 - \sum_{i=0}^{t=\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i} p^i (1-p)^{n-i} - \sum_{i=1, \forall S_i \in \mathcal{S}}^{|\mathcal{S}|} p^{w(S_i)} (1-p)^{n-w(S_i)}, \tag{60}$$

where $w(S_i)$ is the weight of the stabilizer operator S_i, which is defined by the number of non-identity Pauli operators within the stabilizer operators. The second term of Eq. (60) represents all the correctable error patterns of QTECCs, while the last term of Eq. (60) represents the degenerate error patterns

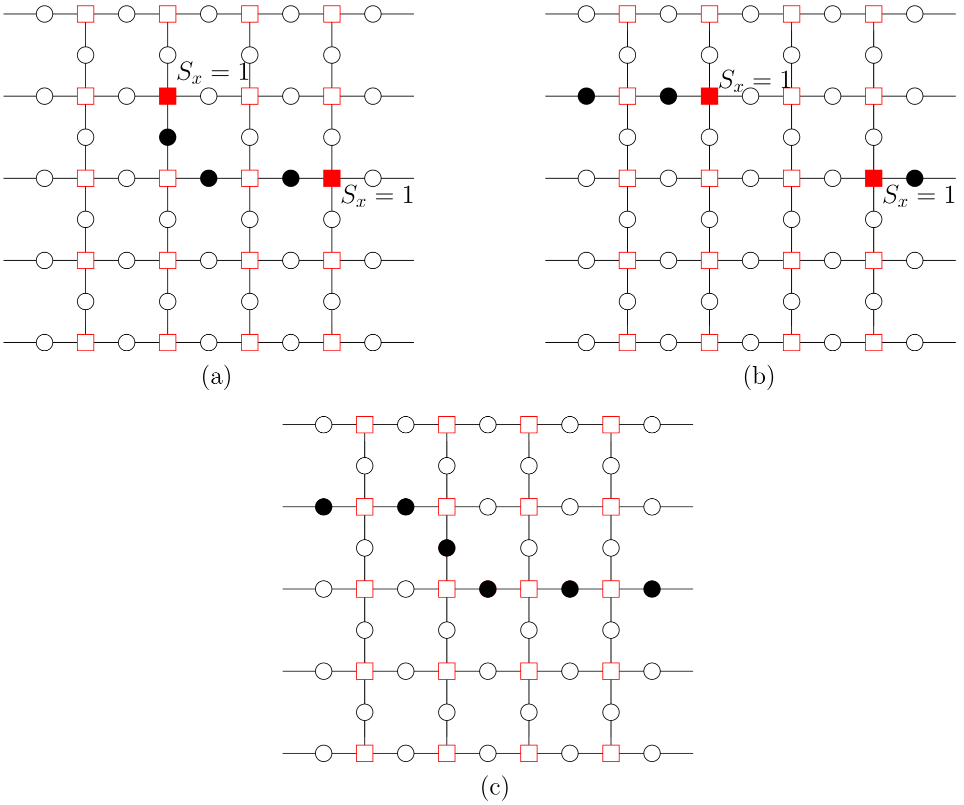
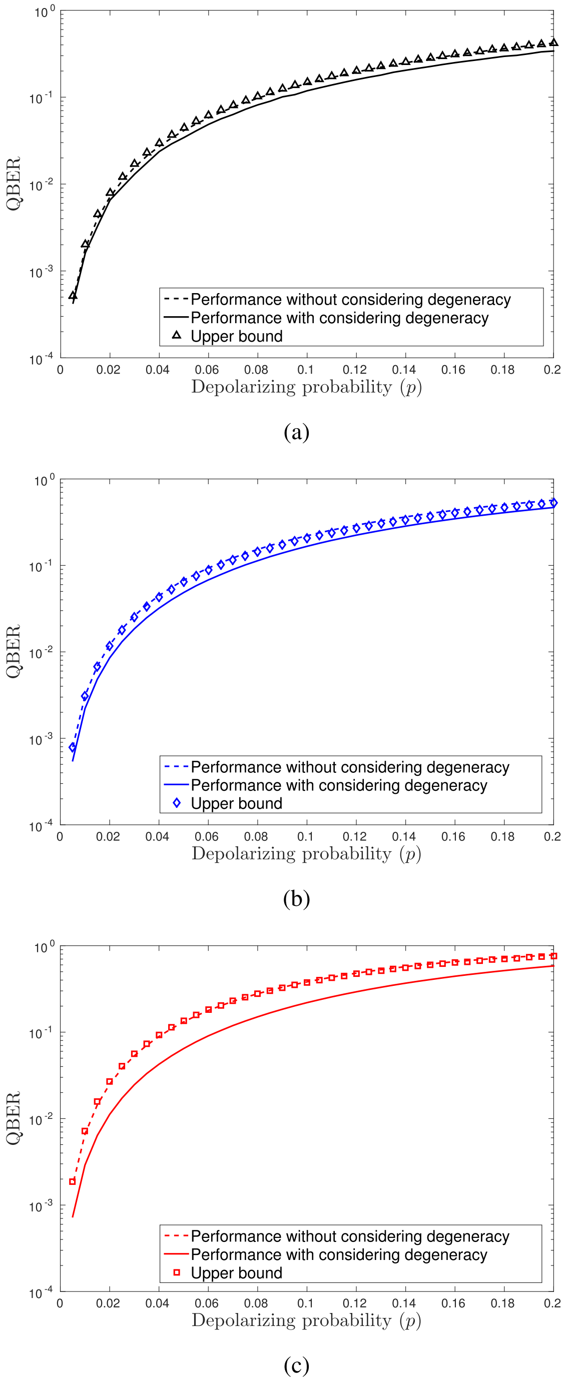


FIGURE 17. Illustration of the harmful undetectable error pattern in quantum domain. The actual error pattern inflicts the state of physical qubits is given in (b), while the decoder always decides to perform a recovery operator given in (a). Instead of recovering the legitimate state of the physical qubits, the specified error recovery procedure generates a chain of error that commutes with all of the stabilizer operators, as shown in (c). In quantum domain, it constitutes the ***harmful undetectable error patterns***. In classical domain, it resembles the error pattern that generates all-zero syndrome values.

that belong to the stabilizer operators. For example, let us revisit the construction of the surface codes of Fig. 12. There are 12 stabilizer generators for a distance-3 surface code, as seen in Table 8. Hence, we can potentially generate in total 2^{12} unique stabilizer operators, since the product of the stabilizer operators returns another valid stabilizer operator. However, in order to further simplify the expression given in Eq. (60), we only consider the error patterns resembling the specified stabilizer operators given in Table 8, since they exhibit a lower weight of non-identity Pauli matrices and hence have a higher probability of occurance. Therefore, for surface codes, the last term of Eq. (60) can be approximated as $(2d^2 - 2d)p^4(1-p)^{n-4}$. The term $(2d^2 - 2d)$ represents the number of stabilizer operators, which is given in Table 10, and we assume that all the weight of the stabilizer operators $w(S_i)$ are equal to 4.

A. QBER VERSUS DEPOLARIZING PROBABILITY

In order to characterize the performance of QTECCs by simulations, we exploit the fact that the QTECCs belong to the family of quantum CSS codes, which handle the bit-flips ($\mathbf{X}$) and phase-flips ($\mathbf{Z}$) separately. Hence, we invoke two independent binary symmetric channels (BSC), one for the $\mathbf{X}$ channel and one for the $\mathbf{Z}$ channel, where each channel is characterized by the flip probability of $2p/3$, where p is the associated depolarizing probability of the quantum depolarizing channel [13], [16]. The decoder utilizes hard-decision ML decoding relying on a simple LUT decoder, as exemplified in Section III. However, this classical-domain simulation only represents the performance of QTECCs without considering the degenerate error patterns. To elaborate a little further, we generate all-zero information bits at the input and send them through the two independent BSC channels. Therefore, we always consider all of non all-zero decoded bits at the decoder output as an error. However, in order to additionally consider several cases of degenerate error patterns, which is exemplified in Fig. 16, we performed an additional evaluation step. We evaluate the non all-zero corrected received words and check for the degenerate error patterns. If it satisfies the degenerate error pattern criterion that we have defined above, we conclude that this is an error free case. However, we are not capable of providing a complete list of all possible degenerate error patterns and in this treatise we only consider the error pattern resembling the stabilizer generators of S_i, which is exemplified in Table 8 and 9 for surface codes and



(a)

(b)

(c)

FIGURE 18. QBER performance of the distance-3 surface code, rotated-surface code and colour code over the quantum depolarizing channel, which is capable of correcting a single qubit error. The code parameters are given in Table 13. For this scenario, the decoder using hard-input ML decoding approach for predicting the error pattern. (a) Colour code. (b) Rotated surface code. (c) Surface code.

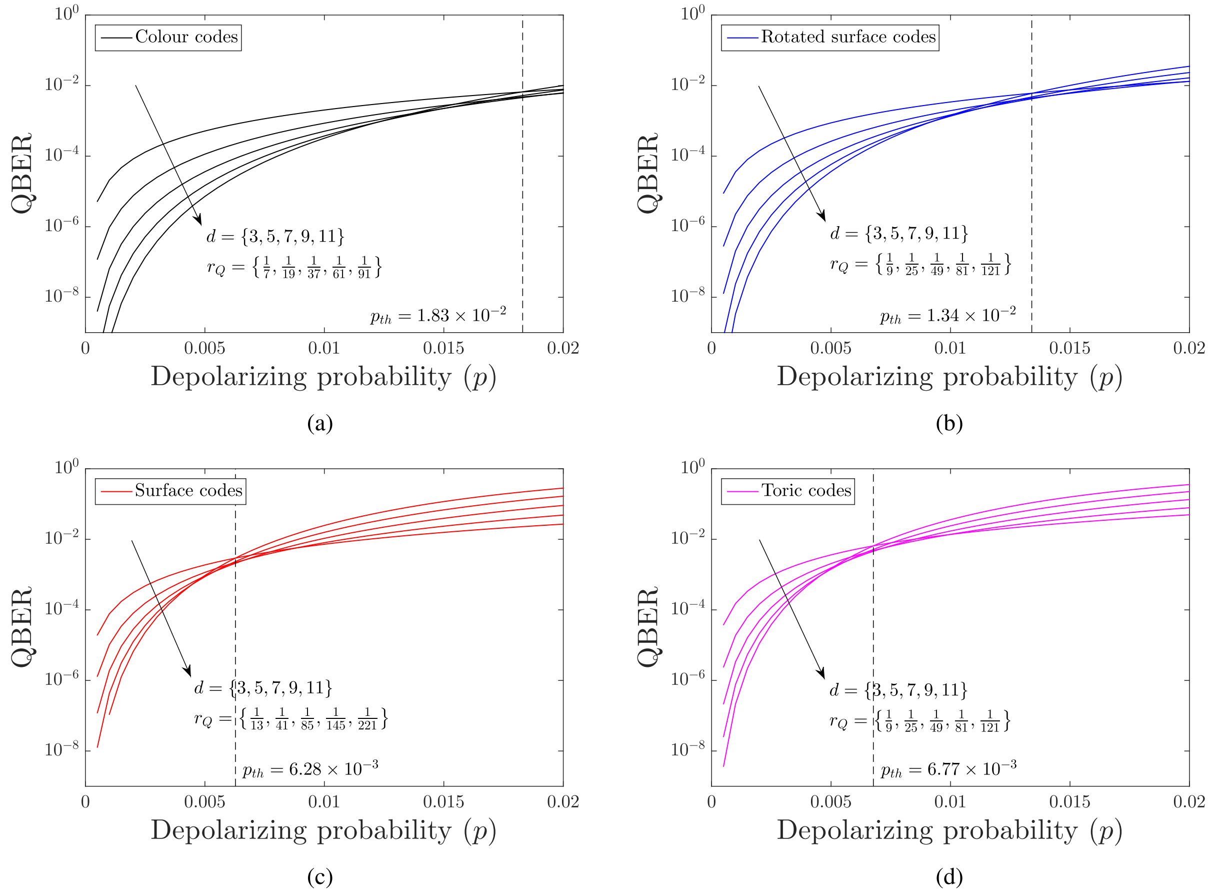
TABLE 13. Code parameters for distance-3 colour code, rotated surface code and surface code.

Code type	n	k	d	r_Q
Colour code	7	1	3	1/7
Rotated surface code	9	1	3	1/9
Surface code	13	1	3	1/13

triangular codes, respectively. The QBER performance of distance-3 QTECCs versus the quantum depolarizing probability is portrayed in Fig. 18, where the code parameters are given in Table 13. We also include the upper bound of the QTECCs performance of Eq. (60) in Fig. 18. It can be clearly observed that the upper bounds match with the QTECCs performance without considering the degenerate error patterns.

As we mentioned earlier, there are two sources of the degenerate error pattern at the output of the decoder. First, the degenerate error patterns that imposed ubiquitous directly by the quantum channel, where the error exhibits an identical pattern to the stabilizer operator S_i. Second, the degenerate error pattern generated by the recovery operator $\mathcal{R}$, when it tries to recover the legitimate physical qubits, as illustrated in Fig. 16. The second case is more dominant than the first one. The reason can be explained as follows. Let us assume the $\mathbf{Z}$ stabilizer operators of distance-3 surface code given in Table 8. There are six $\mathbf{Z}$ stabilizer operators correspond to the $2^6 = 64$ possible syndrome vector, including the error-free scenario. Remember that the distance-3 surface code can only flawlessly correct a single error qubit within the block of 13 physical qubits, where each of the single qubit error pattern is associated with only one syndrome vector. In other words, amongst all of 64 possible syndrome vectors, there are only 13 syndrome vectors used to uniquely distinguish the correctable error patterns, while the rest of the syndrome vectors are associated with the error pattern ambiguity, as exemplified in Fig. 16 and 17. Due to this reason, the QTECCs are considered as the highly degenerate QSCs. Hence, the upper bound of the QBER performance matches the simulation-based performance recorded without considering the degeneracy, since it considers only the first source of the degeneracy, where only a portion of all valid stabilizer operators $S_i \in \mathcal{S}$ in Eq. (60) is included in calculation. However, by accommodating both of the degeneracy cases, the QBER performance of QTECCs is indeed improved, as displayed in Fig. 18.

Increasing the minimum distance of a given QSC construction, which directly improves its per-codeword error corrrection capability (t), is achieved by increasing the number of physical qubits (n) or by decreasing the quantum coding rate. Specifically for QTECCs, increasing the minimum distance means simultaneously increasing the number of physical qubits (n) and decreasing the quantum coding rate (r_Q). Naturally, the goal of increasing the minimum distance of the QSCs is to achieve a better QBER performance. However, the improvement of QBER the performance can only be observed below a certain value of depolarizing probability (p), which may be referred to as the threshold probability (p_{th}). Using the upper bound QBER performance of Eq. (60), we plot the QBER curves for colour, rotated-surface, surface and



(a)

(b)

(c)

(d)

FIGURE 19. Upper bound QBER performance of QTECCs for the minimum distance of $d = \{3, 5, 7, 9, 11\}$ based on Eq. (60) and the code parameters given in Table 10. The crossover amongst the QBER curves represents the threshold probability (p_{th}), which are portrayed in dashed line. (a) Upper bound QBER performance of colour codes. (b) Upper bound QBER performance of rotated-surface codes. (c) Upper bound QBER performance of surface codes. (d) Upper bound QBER performance of toric codes.

toric codes in Fig. 19. For each of the QTECC constructions, we portray the upper bound QBER performance for the minimum distances of $d = \{3, 5, 7, 9, 11\}$. The threshold probability of each code is denoted by the crossover QBER curves, which we portray in dashed line. The threshold probability of colour, rotated-surface, surface and toric codes are 1.83×10^{-2}, 1.34×10^{-2}, 6.28×10^{-3} and 6.77×10^{-3}, respectively.

B. QBER VERSUS DISTANCE FROM HASHING BOUND

Presenting the performance of QTECCs over quantum depolarizing channel by portraying the QBER curves versus the depolarizing probability (p) does not take the quantum coding rate (r_Q) into consideration. As we mentioned earlier, we can simply decrease the quantum coding rate further and further in order to increase the error correction capability of the QTECCs. Nonetheless, for the sake of depicting a fair comparison upon reducing the quantum coding rate, we have to scrutinize how much performance improvement we obtain upon decreasing the quantum coding rate. Therefore, in order to demonstrate how much performance improvement we attain compared to the how much we decrease the quantum coding rate, we normalize the QBER performance by incorporating the quantum hashing bound. More explicitly, the quantum hashing bound can be expressed as follows [46]:

$$C_Q(p) = 1 - H(p) - p.\log_2(3), \tag{61}$$

where $H(p)$ is the binary entropy of p. More specifically, the quantum hashing bound of Eq. (61) dictates that a random quantum code $\mathcal{C}$ having a sufficiently long codeword and a quantum coding rate $r_Q \leq C_Q(p)$ may yield an infinitesimally low QBER for a given depolarizing probability p. Alternatively, we can refer to $C_Q(p)$ as the hashing limit for the quantum coding rate r_Q associated with a given depolarizing probability p. In terms of its classical dual pair, the value of C_Q is similar to the capacity limit. Similarly, for a given coding rate r_Q, we can find a value of p^* satisfying $r_Q = C_Q(p^*)$, where p^* denotes the maximum value of depolarizing probability p so that a quantum code $\mathcal{C}$ having quantum coding rate of r_Q can operate at an infinitesimally low QBER. The value of p^* may be referred to as the hashing limit for depolarizing probability of p associated with a given quantum coding rate r_Q. In classical domain the value of p^* is similar to the noise limit. Therefore, in general, the aim is that of finding

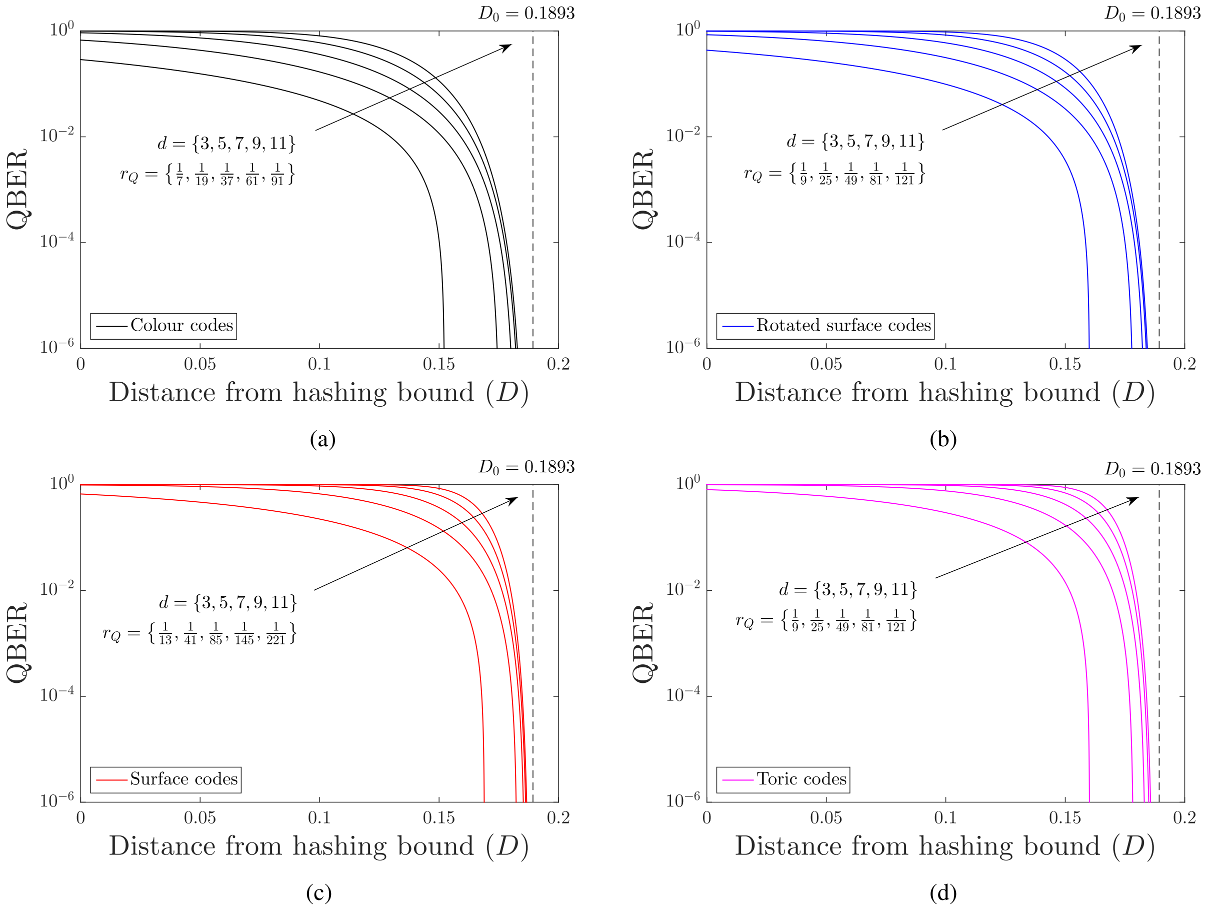


FIGURE 20. **Upper bound performance of QTECCs in term of the QBER versus the distance *D* from the hashing bound. The code parameters are given in Table 10. The dashed lines portray the ultimate distance to the quantum hashing bound of $D_0 = 0.1893$. (a) Upper bound performance of colour codes. (b) Upper bound performance of rotated surface codes. (c) Upper bound performance of surface codes. (d) Upper bound performance of toric codes.**

a QSC that is capable of performing as close as possible to the quantum hashing bound.

For example, let us consider the distance-3 and distance-5 rotated surface codes having quantum coding rate of $r_Q = 1/9$ and $r_Q = 1/25$, respectively. By substituting $C_Q = 1/9$ and $C_Q = 1/25$ into the Eq. (61), we obtain the noise limit of $p^* = 0.160$ and $p^* = 0.179$, respectively. It is clearly seen that the noise limit is higher for the quantum code exhibiting a lower quantum coding rate. To incorporate the quantum hashing bound into the QBER performances of QTECC, we define the distance from hashing bound as follows:

$$D \triangleq p(r_Q) - p, \tag{62}$$

where $p(r_Q)$ is the hashing limit for depolarizing probability of p associated with a given quantum coding rate r_Q. In other words, by changing the horizontal axis from the depolarizing probability p to the distance D from hashing bound, we shift all the QBER curves according to their hashing bounds, so that all the hashing bounds are at the reference point of $D = 0$.

Several pertinent questions arise from the quantum hashing bound formulation. Firstly, is there a noise limit, where no QSC constructions are capable of achieving a satisfactorily low QBER? Indeed, the answer is yes. By substituting the $C_Q = 0$ into Eq. (61), which is the lowest possible value of achievable quantum coding rate, we arrive at the ultimate hashing bound of $p(0) \approx 0.1893$. Secondly, what is the farthest possible distance from the quantum hashing bound for any QSC construction. To answer this question, we have to consider the worst-case scenario, where a QSC exhibiting a near zero quantum coding rate ($r_Q \approx 0$) achieves an infinitesimally low QBER at near zero quantum depolarizing probability ($p \approx 0$). By substituting the value of $r_Q = 0$ and $p = 0$ into Eq. (62), we define the ultimate distance of hashing bound D_0 as

$$\begin{aligned} D_0 &= p(0) - p \\ &= 0.1893 - 0 \\ &= 0.1893. \end{aligned} \tag{63}$$

Therefore, the desirable performance of any QSCs quantified in terms of the QBER versus distance from the quantum hashing bound is represented by the curves exhibiting a reasonably low QBER as close as possible to the reference point of $D = 0$. Naturally, this implies having a low QBER as

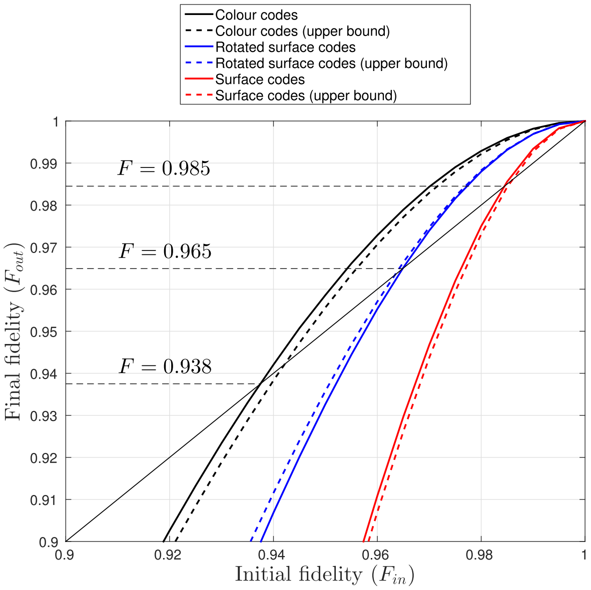


FIGURE 21. The performance of QTECCs having a minimum distance of 3 in terms of fidelity of Eq. (64). The colour code reaches the fidelity threshold earlier than the rotated-surface and surface code, since the colour code has the lowest number of physical qubits compared to the rotated surface code and the surface code. The code parameters are given in Table 13.

far as possible from the ultimate distance from the hashing bound of $D_0 = 0.1893$. In simpler terms, any QSCs can only operate at a reasonably low QBER within the hashing bound range of $0 \leq D \leq D_0$. Consequently, we should consider the reduction of the quantum coding rate r_Q as beneficial only if the associated QBER performance curve moves closer to the reference point of $D = 0$. Otherwise, it is more advisable to find a better code construction exhibiting an identical quantum coding rate, to increase the number of physical qubits, while maintaining the quantum coding rate, or to invoke more powerful decoding scheme, for example by utilizing a soft-decision-aided decoder. The QBER performance of QTECCs versus their distances from the quantum hashing bound are portrayed in Fig. 20. It can be observed that even though increasing the minimum distance of the QTECCs yields a performance improvement in terms of their QBER versus depolarizing probability p shown in Fig. 19, in terms of their distance from the hasing bound D, at low QBER, the curves are crowded in the vicinity of the ultimate hashing bound distance of D_0. Moreover, the results show an agreement with the quantum coding rate versus minimum distance evolution of QTECCs seen in Fig. 15. The improvement of the minimum distance, which is directly linked to the error correction capability, upon reducing the quantum coding rate is not fast enough to compensate the increasing number of physical qubits. Therefore, we believe that QTECCs are most suitable for short to moderate codeword lengths.

C. FIDELITY

From an implementational perspective, a quantum gate or quantum channel is often characterized by the so-called fidelity, which represents the closeness of a pure quantum state of $|\overline{\psi}\rangle$ compared to the mixed states having the quantum density operator of ρ. More explicitly, since the quantum channel imposes the quantum decoherence on our legitimate quantum state representing the physical qubits $|\overline{\psi}\rangle$, there is a probability that decoder does not successfully recover the legitimate state. Therefore, the ensemble of all the possible predicted legitimate state of physical qubits $|\widehat{\overline{\psi}}\rangle$ can be represented using the state of $|\psi_i\rangle$ having a probability of p_i. The fidelity can be formulated as follows [47]–[49]:

$$F = \langle\overline{\psi}|\rho|\overline{\psi}\rangle. \tag{64}$$

while ρ, which portrays the statistical characteristics of a the mixed states, is defined by

$$\rho = \sum_{i=1}^{N} p_i|\psi_i\rangle\langle\psi_i|, \tag{65}$$

where the $|\psi_i\rangle$ represents all of the possible state in the ensemble and p_i is the probability of having state $|\psi_i\rangle$ in the ensemble, which is subject to unity constraint of $\sum_{i=1}^{N} p_i = 1$.

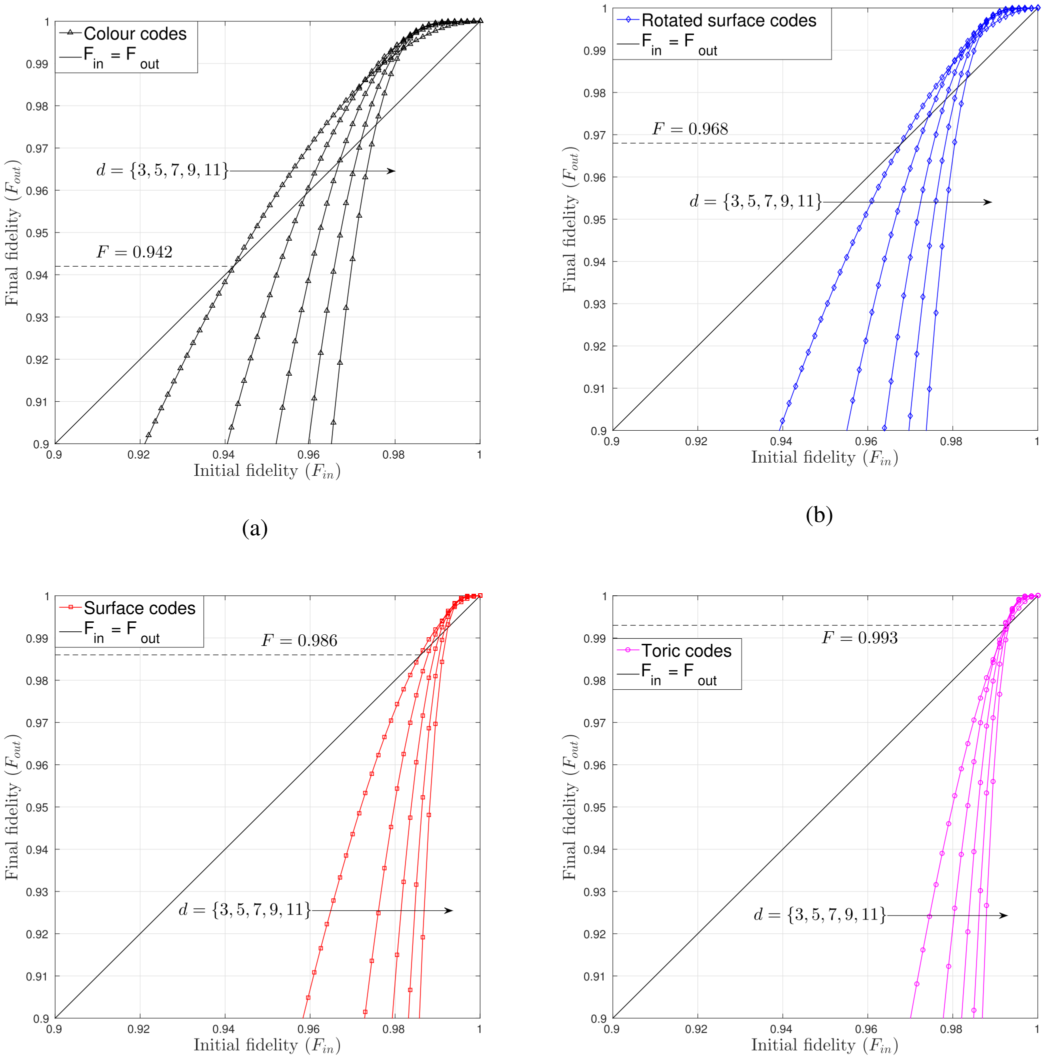
In order to demonstrate the benefit of QTECCs in the context of quantum depolarizing channel, we compare the so-called initial fidelity F_{in} and final fidelity F_{out}. The initial fidelity is the fidelity of the pure quantum state of $|\psi\rangle$ over the quantum depolarizing channel $\mathcal{P}$ unprotected by any QSCs scheme. Therefore, the initial fidelity F_{in} can be expressed as follows:

$$F_{\text{in}} = 1 - p. \tag{66}$$

The final fidelity is that of the pure state of the desired output $|\psi'\rangle$ protected by the a QSC scheme after the recovery procedure $\mathcal{R}$ and inverse encoder $\mathcal{V}^\dagger$ of Fig. 11. Therefore, the final fidelity F_{out} of the quantum system can be readily formulated as

$$F_{\text{out}} = 1 - \text{QBER}. \tag{67}$$

The fidelity performance for the distance-3 QTECCs are depicted in Fig. 21. The black solid line represents the condition of $F_{\text{in}} = F_{\text{out}}$. The crossover point between the line of $F_{\text{in}} = F_{\text{out}}$ and fidelity performance curve of QTECCs is the break-even point, which we may referred to as the *threshold fidelity* F_{th}. The break-even point denotes the minimal initial fidelity required to ensure that we do acquire a fidelity improvement upon the applicaton of the QSC scheme, which is invoked for protecting the state of the physical qubits. The upper bound of threshold fidelity F_{th} for the different types of QTECCs having code parameters listed in Table 10 is depicted in Fig. 22. It can be observed that different code families having various minimum distances d result in different threshold fidelity F_{th}. For the QSCs utilizing hard-decision syndrome decoding, we derive the upper-bound approximation formula for determining the value of F_{th}. First, from



(a)

(b)

(c)

(d)

FIGURE 22. Upper bound fidelity performance of QTECCs. (a) Upper bound fidelity performance of colour codes. (b) Upper bound fidelity performance of rotated surface codes. (c) Upper bound fidelity performance of surface codes. (d) Upper bound fidelity performance of toric codes.

Eq. (60) and Eq. (67), we arrive at

$$\begin{aligned} F_{\text{out}} &= 1 - \text{QBER}_{\text{upper}} \\ &= 1 - \left(1 - \sum_{i=0}^{t=\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i} p^i (1-p)^{n-i}\right) \\ &= 1 - \sum_{\lfloor \frac{d-1}{2} \rfloor + 1}^{n} \binom{n}{i} p^i (1-p)^{n-i}. \end{aligned} \tag{68}$$

For a low depolarizing probability p, the expression given in Eq. (68) can be approximated in order to determine the upper bound of the output fidelity as follows:

$$F_{\text{out}} \approx 1 - \binom{n}{\lfloor \frac{d-1}{2} \rfloor + 1} p^{\lfloor \frac{d-1}{2} \rfloor + 1}. \tag{69}$$

Since the threshold fidelity satisfies the relationship of $F_{\text{th}} = F_{\text{in}} = F_{\text{out}}$, we can substitute $F_{\text{out}} = F_{\text{th}}$ and $p = 1 - F_{\text{th}}$ into Eq. (69). Finally, the upper bound for the threshold probability can be encapsulated as

$$F_{\text{th}}(n, d) = 1 - \binom{n}{\lfloor \frac{d-1}{2} \rfloor + 1}^{-1/\lfloor \frac{d-1}{2} \rfloor}. \tag{70}$$

For example, the threshold for a distance-3 colour code having a quantum coding rate $r_Q = 1/7$ based on Fig. 22 is $F_{\text{th}} = 0.942$, while using the upper bound approximation of the fidelity threshold in Eq. (70) we have $F_{\text{th}} = 0.952$. For the distance-3 of rotated surface code, surface code and toric code, the threshold fidelity values based on Fig. 22 are $F_{\text{th}} = 0.968$, $F_{\text{th}} = 0.986$ and $F_{\text{th}} = 0.993$, respectively. By using the approximation of Eq. (70), the upper bound fidelity thresholds are given by $F_{\text{th}} = 0.972$, $F_{\text{th}} = 0.987$

and $F_{\text{th}} = 0.994$, respectively for the distance-3 rotated surface code, surface code and toric code. Here, we use the family of QTECCs as our representative examples, while the threshold fidelity of Eq. (70) is generically applicable for any QSCs using hard-decision syndrome decoding. Ultimately, the implementation of QTECCs are capable of reducing the effect of quantum decoherence, which is demonstrated by the QBER reduction and also improving the reliability of quantum channel, which is demonstrated by the fidelity improvement.

VI. CONCLUSIONS

We portrayed the evolution of the topological error correction codes designed in the classical domain to their quantum-domain dual pairs. We showed that by arranging the bits of the codeword on a lattice structure in classical domain provides a benificial inherent error correction capability. Furthermore, for a long codeword, the classical topological error correction codes (TECCs) correspond to the family of LDPC codes exhibiting attractive properties, such as unbounded minimum distance as a function of the codeword length, structured construction and a coding rate of $r = 1/2$. By contrast, the quantum topological error correction codes (QTECCs) are more suitable for applications requiring short to moderate codeword lengths, since the quantum coding rate of QTECCs tends to zero for a long codeword. We characterized the performance of QTECCs in the face of the quantum depolarizing channel in terms of the QBER attained. First, we showed that QTECCs are highly degenerate quantum codes, therefore the classical simulation is only capable of portraying the performance of QTECCs without considering the degeneracy property. Secondly, we demonstrated that increasing the minimum distance of the QTECCs improves the QBER performance. Additionally, we normalized the performance by taking the coding rate into consideration by introducing the *distance from the hashing bound*. Explicitly, we have shown that the growth of minimum distance of QTECCs upon increasing the codeword length is not fast enough to compensate for the increased codeword length. Consequently, the QBER performance of QTECCs gradually tends to the *ultimate distance from the hashing bound*. Finally, we determined the fidelity threshold for QSCs based on hard-decision syndrome decoding, which represents the minimum fidelity value required for a quantum system in order to glean benefits from QSCs. Ultimately, the employment of QSCs will improve the reliability of quantum computers.

ACKNOWLEDGMENT

The authors acknowledge the use of the IRIDIS High Performance Computing Facility, and associated support services at the University of Southampton. The research data of this paper can be found at http://doi.org/10.5258/SOTON/D0349.

REFERENCES

[1] P. W. Shor, "Fault-tolerant quantum computation," in *Proc. 37th Annu. Symp. Found. Comput. Sci.*, 1996, pp. 56–65, 1996.

[2] J. Preskill, "Reliable quantum computers," *Proc. Roy. Soc. London A, Math., Phys. Eng. Sci.*, vol. 454, no. 1969, pp. 385–410, 1998.

[3] D. P. DiVincenzo, "The physical implementation of quantum computation," *Fortschritte Phys.*, vol. 48, nos. 9–11, pp. 771–783, 2000.

[4] D. Gottesman, "Stabilizer codes and quantum error correction," Ph.D. dissertation, California Inst. Technol., Pasadena, CA, USA, 1997.

[5] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction and orthogonal geometry," *Phys. Rev. Lett.*, vol. 78, no. 3, p. 405, 1997.

[6] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction via codes over GF(4)," *IEEE Trans. Inf. Theory*, vol. 44, no. 4, pp. 1369–1387, Jul. 1998.

[7] M. Grassl and T. Beth, "Quantum BCH codes," in *Proc. Int. Symp. Theor. Elect. Eng.*, 1999, pp. 207–212.

[8] M. Grassl, W. Geiselmann, and T. Beth, "Quantum Reed–Solomon codes," in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*. Berlin, Germany: Springer, 1999, pp. 231–244.

[9] H. Ollivier and J.-P. Tillich, "Description of a quantum convolutional code," *Phys. Rev. Lett.*, vol. 91, no. 17, p. 177902, 2003.

[10] D. Poulin, J. P. Tillich, and H. Ollivier, "Quantum serial turbo codes," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2776–2798, Jun. 2009.

[11] Z. Babar, P. Botsinis, D. Alanis, S. X. Ng, and L. Hanzo, "The road from classical to quantum codes: A hashing bound approaching design procedure," *IEEE Access*, vol. 3, pp. 146–176, Mar. 2015.

[12] M. S. Postol. (2001). "A proposed quantum low density parity check code." [Online]. Available: https://arxiv.org/abs/quant-ph/0108131

[13] D. MacKay, G. Mitchison, and P. McFadden, "Sparse-graph codes for quantum error correction," *IEEE Trans. Inf. Theory*, vol. 50, no. 10, pp. 2315–2330, Oct. 2004.

[14] T. Camara, H. Ollivier, and J.-P. Tillich. (2005). "Constructions and performance of classes of quantum LDPC codes." [Online]. Available: https://arxiv.org/abs/quant-ph/0502086

[15] T. Camara, H. Ollivier, and J.-P. Tillich, "A class of quantum LDPC codes: Construction and performances under iterative decoding," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2007, pp. 811–815, 2007.

[16] Z. Babar, P. Botsinis, D. Alanis, S. X. Ng, and L. Hanzo, "Fifteen years of quantum LDPC coding and improved decoding strategies," *IEEE Access*, vol. 3, pp. 2492–2519, Nov. 2015.

[17] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," *Phys. Rev. A, Gen. Phys.*, vol. 52, no. 4, p. R2493(R), 1995.

[18] A. M. Steane, "Error correcting codes in quantum theory," *Phys. Rev. Lett.*, vol. 77, no. 5, p. 793, 1996.

[19] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, "Perfect quantum error correcting code," *Phys. Rev. Lett.*, vol. 77, no. 1, p. 198, 1996.

[20] *IBM Quantum Experience*. Accessed: Oct. 1, 2017. [Online]. Available: https://www.research.ibm.com/ibm-q/

[21] H. Bombin and M. A. Martin-Delgado, "Homological error correction: Classical and quantum codes," *J. Math. Phys.*, vol. 48, no. 5, p. 052105, 2007.

[22] A. Y. Kitaev, "Quantum computations: Algorithms and error correction," *Russian Math. Surv.*, vol. 52, no. 6, pp. 1191–1249, 1997.

[23] A. Y. Kitaev, "Fault-tolerant quantum computation by anyons," *Ann. Phys.*, vol. 303, no. 1, pp. 2–30, Jan. 2003.

[24] S. B. Bravyi and A. Y. Kitaev. (1998). "Quantum codes on a lattice with boundary." [Online]. Available: https://arxiv.org/abs/quant-ph/9811052

[25] H. Bombin and M. A. Martin-Delgado, "Topological quantum distillation," *Phys. Rev. Lett.*, vol. 97, no. 18, p. 180501, 2006.

[26] G. Zémor, "On Cayley graphs, surface codes, and the limits of homological coding for quantum error correction," in *Coding and Cryptology*. Berlin, Germany: Springer, 2009, pp. 259–273.

[27] A. Couvreur, N. Delfosse, and G. Zémor, "A construction of quantum LDPC codes from Cayley graphs," *IEEE Trans. Inf. Theory*, vol. 59, no. 9, pp. 6087–6098, Sep. 2013.

[28] J.-P. Tillich and G. Zémor, "Quantum LDPC codes with positive rate and minimum distance proportional to $n^{1/2}$," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun./Jul. 2009, pp. 799–803.

[29] A. A. Kovalev and L. P. Pryadko, "Improved quantum hypergraph-product LDPC codes," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2012, pp. 348–352.

[30] J.-P. Tillich and G. Zémor, "Quantum LDPC codes with positive rate and minimum distance proportional to the square root of the blocklength," *IEEE Trans. Inf. Theory*, vol. 60, no. 2, pp. 1193–1202, Feb. 2014.

[31] C. Horsman, A. G. Fowler, S. Devitt, and R. Van Meter, "Surface code quantum computing by lattice surgery," *New J. Phys.*, vol. 14, no. 12, 2012.

[32] N. Delfosse, "Tradeoffs for reliable quantum information storage in surface codes and color codes," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2013, pp. 917–921.

[33] S. Bravyi and M. B. Hastings, "Homological product codes," in *Proc. 46th Annu. ACM Symp. Theory Comput.*, 2014, pp. 273–282.

[34] L. Hanzo, T. H. Liew, B. L. Yeap, R. Y. S. Tee, and S. X. Ng, *Turbo Coding, Turbo Equalisation and Space-Time Coding: EXIT-Chart-Aided Near-Capacity Designs for Wireless Channels*. Hoboken, NJ, USA: Wiley, 2011.

[35] R. M. Tanner, "A recursive approach to low complexity codes," *IEEE Trans. Inf. Theory*, vol. 27, no. 5, pp. 533–547, Sep. 1981.

[36] R. W. Hamming, "Error detecting and error correcting codes," *Bell Syst. Tech. J.*, vol. 29, no. 2, pp. 147–160, Apr. 1950.

[37] E. N. Gilbert, "A comparison of signalling alphabets," *Bell Syst. Tech. J.*, vol. 31, no. 3, pp. 504–522, 1952.

[38] D. Chandra *et al.*, "Quantum coding bounds and a closed-form approximation of the minimum distance versus quantum coding rate," *IEEE Access*, vol. 5, pp. 11557–11581, 2017.

[39] F. R. Kschischang, B. J. Frey, and H.-A. Loeliger, "Factor graphs and the sum-product algorithm," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 498–519, Feb. 2001.

[40] P. A. M. Dirac, "A new notation for quantum mechanics," *Math. Proc. Cambridge Philos. Soc.*, vol. 35, no. 3, pp. 416–418, 1939.

[41] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge, U.K.: Cambridge Univ. Press, 2000.

[42] D. Gottesman, "Class of quantum error-correcting codes saturating the quantum Hamming bound," *Phys. Rev. A, Gen. Phys.*, vol. 54, no. 3, p. 1862, 1996.

[43] A. Ekert and C. Macchiavello, "Quantum error correction for communication," *Phys. Rev. Lett.*, vol. 77, no. 12, p. 2585, 1996.

[44] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Phys. Rev. A, Gen. Phys.*, vol. 54, no. 2, p. 1098, 1996.

[45] R. Steele and L. Hanzo, *Mobile Radio Communications: Second and Third Generation Cellular and WATM Systems*. Hoboken, NJ, USA: Wiley, 1999.

[46] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, "Mixed-state entanglement and quantum error correction," *Phys. Rev. A, Gen. Phys.*, vol. 54, no. 5, p. 3824, 1996.

[47] R. Jozsa, "Fidelity for mixed quantum states," *J. Mod. Opt.*, vol. 41, no. 12, pp. 2315–2323, 1994.

[48] B. Schumacher, "Quantum coding," *Phys. Rev. A, Gen. Phys.*, vol. 51, no. 4, p. 2738, 1995.

[49] E. Knill and R. Laflamme, "Theory of quantum error-correcting codes," *Phys. Rev. A, Gen. Phys.*, vol. 55, no. 2, p. 900, 1997.

DARYUS CHANDRA (S'15) received the M.Eng. degree in electrical engineering from Universitas Gadjah Mada, Indonesia, in 2014. He is currently pursuing the Ph.D. degree with the Southampton Wireless Group, School of Electronics and Computer Science, University of Southampton, U.K. He received the Scholarship Award from the Indonesia Endowment Fund for Education (Lembaga Pengelola Dana Pendidikan).

His research interests include classical and quantum error correction codes, quantum information, and quantum communications.

ZUNAIRA BABAR received the B.Eng. degree in electrical engineering from the National University of Sciences and Technology, Islamabad, Pakistan, in 2008, and the M.Sc. degree (Hons.) and the Ph.D. degree in wireless communications from the University of Southampton, U.K., in 2011 and 2015, respectively.

Her research interests include quantum error correction codes, channel coding, coded modulation, iterative detection, and cooperative communications.

HUNG VIET NGUYEN received the B.Eng. degree in electronics and telecommunications from the Hanoi University of Science and Technology, Hanoi, Vietnam, in 1999, the M.Eng. degree in telecommunications from the Asian Institute of Technology, Bangkok, Thailand, in 2002, and the Ph.D. degree in wireless communications from the University of Southampton, Southampton, U.K., in 2013. Since 1999, he has been a Lecturer with the Post and Telecommunications Institute of Technology, Vietnam. He is involved in the OPTIMIX and CONCERTO European projects. He is currently a Post-Doctoral Researcher with the Southampton Wireless Group, University of Southampton.

His research interests include cooperative communications, channel coding, network coding, and quantum communications.

DIMITRIOS ALANIS (S'13) received the M.Eng. degree in electrical and computer engineering from the Aristotle University of Thessaloniki in 2011 and the M.Sc. and Ph.D. degrees in wireless communications from the University of Southampton, U.K., in 2012 and 2017, respectively. He is currently a Research Fellow with the Southampton Wireless Group, School of Electronics and Computer Science, University of Southampton.

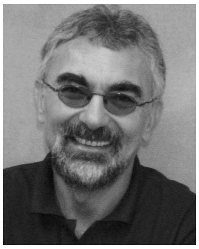
His research interests include quantum computation and quantum information theories, quantum search algorithms, cooperative communications, resource allocation for self-organizing networks, bio-inspired optimization algorithms, and classical and quantum game theories.

PANAGIOTIS BOTSINIS (S'12–M'16) received the M.Eng. degree from the School of Electrical and Computer Engineering, National Technical University of Athens, Greece, in 2010, and the M.Sc. degree (Hons.) and the Ph.D. degree in wireless communications from the University of Southampton, U.K., in 2011 and 2015, respectively. He is currently a Research Fellow with the Southampton Wireless Group, School of Electronics and Computer Science, University of Southampton. Since 2010, he has been a member of the Technical Chamber of Greece.

His research interests include quantum-assisted communications, quantum computation, iterative detection, orthogonal frequency-division multiplexing, multi-in multi-out, multiple access systems, coded modulation, channel coding, cooperative communications, as well as combinatorial optimization.

SOON XIN NG (S'99–M'03–SM'08) received the B.Eng. degree (Hons.) in electronic engineering and the Ph.D. degree in telecommunications from the University of Southampton, Southampton, U.K., in 1999 and 2002, respectively. From 2003 to 2006, he was a Post-Doctoral Research Fellow focusing on collaborative European research projects known as SCOUT, NEWCOM, and PHOENIX. Since 2006, he has been an Academic Staff Member with the School of Electronics and Computer Science, University of Southampton. He is involved in the OPTIMIX and CONCERTO European projects as well as the IU-ATC and UC4G projects. He is currently an Associate Professor of telecommunications with the University of Southampton.

His research interests include adaptive coded modulation, coded modulation, channel coding, space-time coding, joint source and channel coding, iterative detection, orthogonal frequency-division multiplexing, multi-in multi-out, cooperative communications, distributed coding, quantum error correction codes, and joint wireless-and-optical-fibre communications. He has authored over 200 papers and co-authored two books (John Wiley/IEEE Press) in this field. He is a Chartered Engineer and a fellow of the Higher Education Academy, U.K.



LAJOS HANZO (M'91–SM'92–F'04) received the master's degree in electronics in 1976 and the Ph.D. degree in 1983 from the Technical University of Budapest. During his 42-year career in telecommunications, he has held various research and academic posts in Hungary, Germany, and U.K. Since 1986, he has been with the School of Electronics and Computer Science, University of Southampton, U.K., where he is currently the Chair of telecommunications. He has successfully supervised 112 Ph.D. students. He has co-authored 18 books (John Wiley/IEEE Press) on mobile radio communications totaling in excess of 10 000 pages and published 1692 research contributions at IEEE Xplore. In 2009, he received the honorary doctorate "Doctor Honoris Causa" by the Technical University of Budapest. He was a TPC and General Chair of the IEEE conferences, presented keynote lectures and has been awarded a number of distinctions. He is directing a 100-strong academic research team, focusing on a range of research projects in the field of wireless multimedia communications sponsored by industry, the Engineering and Physical Sciences Research Council U.K., the European Research Council's Advanced Fellow Grant, and the Royal Society's Wolfson Research Merit Award. He is an enthusiastic supporter of industrial and academic liaison, and he offers a range of industrial courses.

Dr. Hanzo is a Chaired Professor with Tsinghua University, Beijing. He is a fellow of the Royal Academy of Engineering, Institution of Engineering and Technology, and the European Association for Signal Processing. He is also a Governor of the IEEE VTS. During 2008–2012, he was the Editor-in-Chief of the IEEE Press. He has 30 000+ citations. For further information on research in progress and associated publications please refer to http://www.wireless.ecs.soton.ac.uk.

The Evolution of Quantum Key Distribution Networks: On the Road to the Qinternet

Yuan Cao, Yongli Zhao, *Senior Member, IEEE,* Qin Wang, Jie Zhang, Soon Xin Ng, *Senior Member, IEEE*, and Lajos Hanzo, *Fellow, IEEE*

***Abstract*—Quantum key distribution (QKD) constitutes a symmetric secret key negotiation protocol capable of maintaining information-theoretic security. Given the recent advances in QKD networks, they have evolved from academic research to some preliminary applications. A QKD network consists of two or more QKD nodes interconnected by optical fiber or free space links. The secret keys are negotiated between any pair of QKD nodes, and then they can be delivered to multiple users in various areas for ensuring long-term protection and forward secrecy. We commence by introducing the QKD basics, followed by reviewing the development of QKD networks and their implementation in practice. Subsequently, we describe the general QKD network architecture, its elements, as well as its interfaces and protocols. Next, we provide an in-depth overview of the associated physical layer and network layer solutions, followed by the standardization efforts as well as the application scenarios associated with QKD networks. Finally, we discuss the potential future research directions and provide design guidelines for QKD networks.**

***Index Terms*—Quantum key distribution networks, quantum cryptography, quantum communication, security, communication networks, next generation networking.**

NOMENCLATURE

5G	Fifth Generation
AES	Advanced Encryption Standard
API	Application Programming Interface
ASE	Amplified Spontaneous Emission
BB84	Bennett-Brassard-1984
BBM92	Bennett-Brassard-Mermin-1992
BER	Bit Error Rate
CORBA	Common Object Request Broker Architecture
COW	Coherent-One-Way
CSA	Cloud Security Alliance
CV	Continuous-Variable
DI	Device-Independent
DPS	Differential-Phase-Shift
DV	Discrete-Variable
DWDM	Dense Wavelength-Division Multiplexing
E91	Ekert-91
ECC	Elliptic Curve Cryptography
ECP	Encryption Control Protocol
EDFA	Erbium Doped Fiber Amplifier
ETSI	European Telecommunications Standards Institute
FEC	Forward Error Correction
FMF	Few-Mode Fiber
FWM	Four-Wave Mixing
GG02	Grosshans-Grangier-2002
GPON	Gigabit Passive Optical Network
HTTPS	HyperText Transfer Protocol Secure
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
ILP	Integer Linear Programming
IoT	Internet of Things
IP	Internet Protocol
IPsec	Internet Protocol Security
ISO	International Organization for Standardization
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
JSON	JavaScript Object Notation
KoD	Key on Demand
KP	Key Pool
LEO	Low Earth Orbit
MACsec	Media Access Control Security
MCF	Multi-Core Fiber
MDI	Measurement-Device-Independent
NFV	Network Function Virtualization
NIST	National Institute of Standards and Technology
OFDM	Orthogonal Frequency-Division Multiplexing
ONU	Optical Network Unit

Manuscript received XXXX. This work was supported in part by National Natural Science Foundation of China (62150032), National Key Research and Development Program of China (2020YFE0200600), the Funds for Creative Research Groups of China (62021005), China Association for Science and Technology, Open Fund of State Key Laboratory of Advanced Optical Communication Systems and Networks (Shanghai Jiao Tong University) (2022GZKF006), Open Fund of IPOC (BUPT), and Natural Science Research Start-up Foundation of Recruiting Talents of Nanjing University of Posts and Telecommunications (NY221114). S. X. Ng would like to acknowledge the financial support of the EPSRC project EP/L018659/1. L. Hanzo would like to acknowledge the financial support of the Engineering and Physical Sciences Research Council projects EP/P034284/1 and EP/P003990/1 (COALESCE) as well as of the European Research Council's Advanced Fellow Grant QuantCom (789028). This paper was conceived, when Dr. Cao was hosted by Prof. Hanzo at the University of Southampton, U.K. *(Corresponding author: Yongli Zhao.)*

Yuan Cao and Qin Wang are with the Institute of Quantum Information and Technology, Key Lab of Broadband Wireless Communication and Sensor Network Technology of the Ministry of Education, National Engineering Research Center of Communication and Network Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003, China (e-mail: yuancao@njupt.edu.cn; qinw@njupt.edu.cn).

Yongli Zhao and Jie Zhang are with the State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China (e-mail: yonglizhao@bupt.edu.cn; lgr24@bupt.edu.cn).

Soon Xin Ng and Lajos Hanzo are with the School of Electronics and Computer Science, University of Southampton, Southampton SO17 1BJ, U.K. (e-mail: sxn@ecs.soton.ac.uk; lh@ecs.soton.ac.uk).

OSPF	Open Shortest Path First
OTP	One-Time Pad
PLS	Physical Layer Security
PM	Phase-Matching
PON	Passive Optical Network
PPP	Point-to-Point Protocol
QaaS	Quantum Key Distribution as a Service
QBER	Quantum Bit Error Rate
QBN	Quantum Key Distribution Backbone Node
Qinternet	Quantum Internet
QKD	Quantum Key Distribution
QKP	Quantum Key Pool
QoS	Quality of Service
QRN	Quantum Key Distribution Relay Node
QSDC	Quantum Secure Direct Communication
Qubit	Quantum Bit
REST	Representational State Transfer
ROADM	Reconfigurable Optical Add Drop Multiplexer
RSA	Rivest-Shamir-Adleman
SARG04	Scarani-Acín-Ribordy-Gisin-2004
SDM	Space-Division Multiplexing
SDN	Software Defined Networking
SMF	Single-Mode Fiber
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TDM	Time-Division Multiplexing
TF	Twin-Field
TLS	Transport Layer Security
VKP	Virtual Key Pool
VPN	Virtual Private Network
WDM	Wavelength-Division Multiplexing

I. Introduction

INFORMATION systems are widely used in all aspects of our daily lives, where a variety of information security issues arise and security threats are becoming more and more extensive and anabatic. How to ensure the security of confidential information transmitted through the Internet has become a significant issue that has raised increasingly more attention from both academia and industry. Meanwhile, with the development of quantum computers [1]–[7], their increased computational power threatens conventional cryptosystems. To motivate the need for this survey, Table I compares the threats imposed on different cryptosystems in the presence of quantum computers [8]. Most of the public-key cryptosystems such as those proposed by Rivest-Shamir-Adleman (RSA) [9], Diffie-Hellman [10], and elliptic curve cryptography (ECC) [11], [12] will become insecure once quantum computing reached maturity, since their security relying on the integer factorization and discrete logarithmic problems can be compromised by using Shor's algorithm [13] in a quantum computer. Consequently, there is an urgent need for conceiving powerful information security solutions to guard against quantum attacks. Such solutions are referred to as quantum-safe methods [8].

TABLE I
Comparison of Different Cryptosystems in the Presence of Quantum Computers

Cryptosystem	**Type**	**Impact**
RSA	Public-key	Insecure
Diffie-Hellman	Public-key	Insecure
ECC	Public-key	Insecure
AES	Symmetric-key	Larger key sizes required
OTP	Symmetric-key	Proven secure
Code-based	Post-quantum	Not yet broken
Hash-based	Post-quantum	Not yet broken
Lattice-based	Post-quantum	Not yet broken
Multivariate	Post-quantum	Not yet broken
QKD	Quantum	Proven secure

At the time of writing, two quantum-safe candidate methods have been proposed, namely post-quantum cryptography and quantum cryptography. The family of post-quantum cryptography [14]–[16] consists of code-based [17], hash-based [18], lattice-based [19], and multivariate [20] cryptosystems that have been proven safe against the known quantum attacks. They have the advantage of being compatible with existing cryptographic infrastructures and can reach high secret-key rates over relatively long distances. However, their security might be broken by hitherto unknown algorithms in the future, since they can only be resilient against known quantum attacks. By contrast, quantum cryptography [21]–[24] is capable of achieving the information-theoretic security[1] by exploiting the principles of quantum physics, as exemplified by the quantum no-cloning theorem [25] and the Heisenberg's uncertainty principle [26]. Its security remains indestructible even in the face of future advances in computational power or algorithms. Despite the above advances, quantum cryptography is unable to replicate all the functions of conventional cryptosystems at the time of writing. It is expected to be combined with post-quantum cryptography to jointly build the infrastructure for future quantum-safe cryptosystems [27].

As one of the most successful applications of quantum cryptography, quantum key distribution (QKD) [28]–[31] promises information-theoretic security [32], [33] based on the laws of quantum physics for distributing symmetric secret keys between a pair of legitimate parties. These secret keys can then be used by symmetric-key cryptosystems for encrypting confidential messages to be transferred over a public channel. An example of the symmetric-key cryptosystem is the so-called one-time pad (OTP) [34], which has been proven by Shannon [35] to facilitate information-theoretically secure message encryption. Its disadvantage is however that the key has to be at

[1] Information-theoretic security is often referred to as unconditional security. It refers to a cryptosystem that derives its security solely from information theory. The cryptosystem is uncrackable even if an adversary has unlimited computing power.

least as long as the message, which can be encrypted by taking their modulo-two addition. By using larger key sizes, other symmetric-key cryptosystems such as the advanced encryption standard (AES) [36] are also considered to be quantum-safe [8]. A pivotal challenge of symmetric-key cryptosystems is that of securely sharing the secret key, which can be circumvented by QKD. In particular, although quantum computers are in their infancy, QKD is still required at the time of writing, because it can provide long-term security. For instance, eavesdroppers may intercept and store the encrypted messages that they are not able to decrypt at the time of capturing them and wait for mature quantum computers or algorithms to decrypt these messages. Some important information such as government secrets that have to be kept confidential for decades will substantially benefit from QKD. Thus, QKD technology has the promise of becoming the cornerstone of ultimate information security.

A. *Motivation*

QKD is also a salient quantum communication technique [37]. The basic element of QKD is the QKD transmitter and receiver connected via a QKD link, allowing two legitimate parties to share the secret keys in a point-to-point manner. In recent years, point-to-point QKD has made significant progress in terms of its protocols, devices, systems, and so on. For example, a variety of QKD protocols and devices have been developed for improving the QKD performance quantified in terms of its secret-key rate, distance, and security. As a result, QKD systems are already commercially available on the market [38]–[40].

However, point-to-point QKD links can only support a few pairs of users, which has restricted the popularity of QKD. Extending QKD to network settings beyond point-to-point allows them to evolve from academic research into a range of preliminary applications [41] to offer security for networked users instead of point-to-point scenarios, which has the potential of protecting industrial and governmental networks from security threats.

Given this motivation, a number of fiber-based QKD networks have been deployed in the field, such as the DARPA [42], SECOQC [43], Tokyo [44], SwissQuantum [45], Beijing-Shanghai [46], and Cambridge [47] QKD networks. Furthermore, a satellite-based intercontinental QKD network demonstration [48] and an integrated space-to-ground QKD network [49] have been reported. More broadly, the QKD network can also be used to secure numerous other applications in the areas of finance and banking, government and defense, cloud and data center, critical infrastructure, healthcare, etc.

B. *Comparison to Existing Surveys*

The QKD network has been regarded as the stepping stone for the development of the quantum Internet (Qinternet)[2] [50], as detailed below and summarized in Table II:

- Gisin *et al.* [22] provided an early review of the progress in both the theory and experimental investigations of QKD.
- Kimble [51] described several basic principles associated with the physical implementation of a Qinternet, such as the quantum memories and repeaters required for the reliable transportation of quantum states across networks.
- Scarani *et al.* [28] focused on the practical aspects of QKD and summarized the theoretical tools used for assessing the security of experimental platforms.
- Lo *et al.* [33] reviewed QKD techniques in terms of their security model, experimental progress and challenges, as well as quantum hacking and countermeasures. Several QKD network implementation examples were also described.
- Alléaume *et al.* [52] compared QKD to classical key distribution techniques and described the generic scenarios of using QKD in cryptographic infrastructures, where the QKD networks are discussed in a generic scenario.
- Diamanti *et al.* [53] outlined the principle, security, and implementation of distributing secret keys relying on continuous valued variables.
- Diamanti *et al.* [29] surveyed several practical challenges in terms of the attainable secret-key rate, distance, size, cost, and practical security in QKD. They also discussed the practicalities of building a QKD network.
- Sasaki [54] discussed how QKD networks could be used in existing fiber-based as well as wireless networks.
- Dür *et al.* [55] elaborated both on the potential applications as well as on the theoretical and experimental challenges of implementing the Qinternet.
- Shenoy-Hejamadi *et al.* [56] covered the progress of QKD and other applications of quantum cryptography, such as quantum random number generation and quantum secret sharing.
- Zhang *et al.* [30] provided a survey of both the challenges and solutions conceived for large scale QKD, including the security of practical QKD, QKD metropolitan as well as backbone networks, and satellite-based QKD.
- Wehner *et al.* [50] categorized the different stages of developing the Qinternet and outlined the technological advances required for reaching these stages.
- Laudenbach *et al.* [57] detailed the theoretical foundations to be laid down for the practical implementation of continuous-variable QKD (CV-QKD) relying on idealized Gaussian modulation.
- Gyongyosi *et al.* [58] provided a review of QKD protocols and their applications in the classical Internet and the Qinternet.
- Kozlowski *et al.* [59] surveyed the state-of-the-art of quantum networks from the perspective of computer science and discussed the major challenges to be overcome in order to make the Qinternet a reality.
- Hosseinidehaj *et al.* [60] outlined the technical advances

[2] The quantum Internet [50] is a network that interconnects quantum devices through quantum channels, which can provide new Internet technologies by using quantum communication to enable applications that are out of reach for the classical Internet. Qinternet is defined as the abbreviation for Quantum Internet in this paper.

TABLE II
COMPARISON OF THIS SURVEY TO EXISTING SURVEYS

Reference	Year	QKD basics	Advances in QKD networks	QKD networking architecture	Enabling techniques for QKD networks		QKD network standardization	QKD network applications	Open topics of QKD networks	Design guidelines for QKD networks
					Physical layer	Network layer				
[22]	2002	✓								
[51]	2008				✓				✓	
[28]	2009	✓			✓					
[33]	2014	✓	✓		✓					
[52]	2014	✓	✓			✓		✓	✓	
[53]	2015	✓								
[29]	2016	✓			✓					
[54]	2017							✓	✓	
[55]	2017				✓				✓	
[56]	2017	✓			✓				✓	
[30]	2018	✓	✓		✓					
[50]	2018	✓	✓		✓				✓	
[57]	2018	✓								
[58]	2019	✓			✓	✓		✓	✓	
[59]	2019				✓	✓			✓	
[60]	2019	✓			✓				✓	
[61]	2020	✓			✓		✓	✓	✓	
[31]	2020	✓	✓		✓				✓	
[24]	2020	✓			✓				✓	
[62]	2020		✓			✓	✓			
This survey		✓	✓	✓	✓	✓	✓	✓	✓	✓

related to satellite-based continuous-variable quantum communications.

- Cavaliere *et al.* [61] reviewed quantum communication with particular attention to evolving QKD technologies from labs to the markets following an industrial perspective.
- Xu *et al.* [31] reviewed both the theoretical and experimental progress in secure QKD relying on realistic devices, and they prophesized that numerous QKD networks would be deployed in many countries to achieve the ultimate goal of a global QKD network.
- Pirandola *et al.* [24] provided an overview of research advances in the domain of both theoretical and experimental QKD.
- Mehic *et al.* [62] surveyed several typical QKD networks and the challenges of QKD networking in terms of the quality of service (QoS), as well as their simulation techniques, and software defined networking (SDN) approaches.

These valuable surveys have provided insights into diverse perspectives on the family of QKD technologies and the Qinternet, but none of them paid attention to the details of QKD networks. For example, many of them focused on the enabling technologies in the physical layer of QKD networks, with little attention paid to the network layer. Thus there is a paucity of literature on the details of QKD networks. Again, Table II boldly and explicitly compares this survey against the existing surveys. More concretely, we cover the details of QKD networks, including their current advances and networking architecture, their physical and network layer solutions, as well as their standardization and applications. To the best of our knowledge, this survey is the first one to provide a comprehensive up-to-date review of QKD networks.

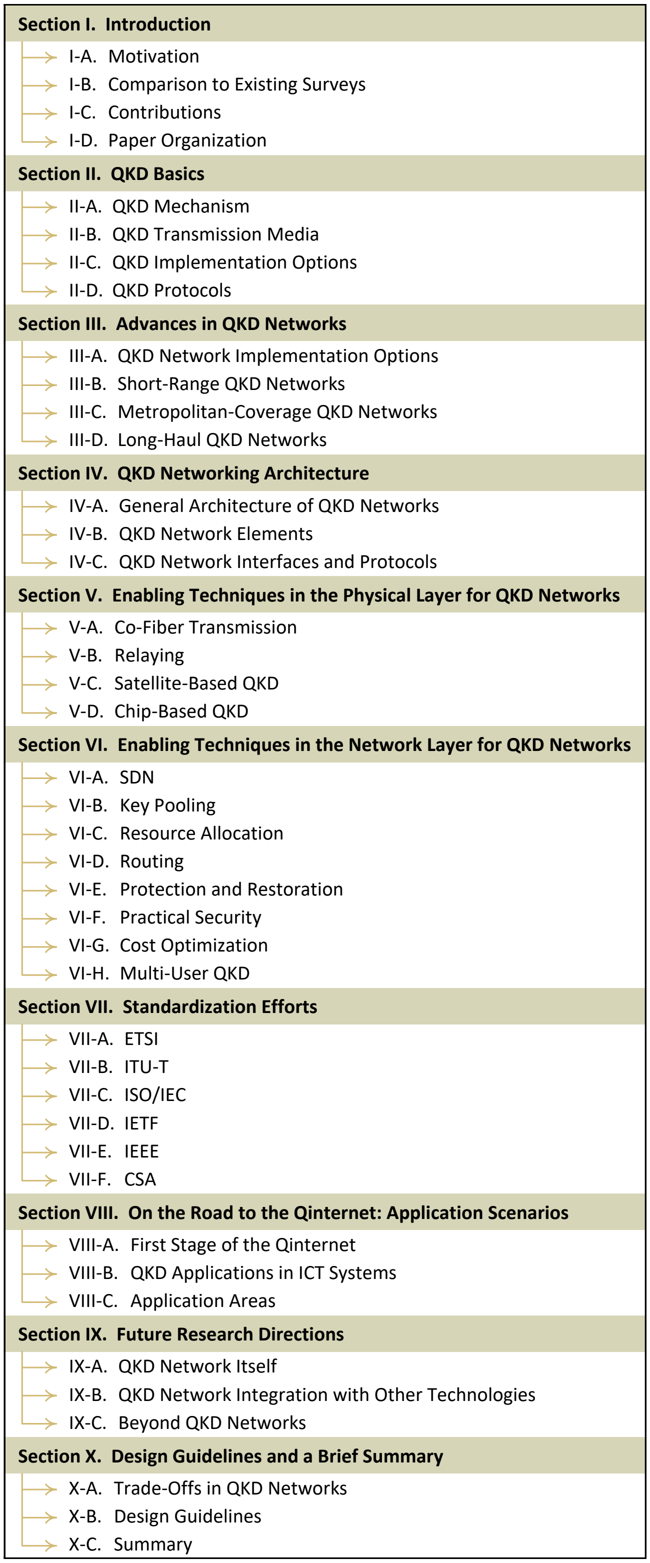
C. *Contributions*

More specifically, the major contributions of this survey are summarized as follows:

1) We survey the development of practical QKD network implementations conceived both for covering short-range as well as metropolitan communications, and long-haul QKD networks, with special emphasis on the associated engineering perspectives. (Section III)
2) We describe the general QKD network architecture, its elements, as well as its interfaces and protocols. (Section IV)
3) We provide an in-depth survey of the QKD network's enabling techniques, highlighting the interactions of the physical and network layers. Specifically, the issues of physical layer co-fiber transmission, relaying, satellite-based QKD, and chip-based QKD technologies are discussed. In the network layer we critically appraise SDN, key pooling, resource allocation, routing, protection

and restoration, as well as practical security solutions, cost optimization, and multi-user QKD solutions. (Sections V and VI)

4) We outline the standardization efforts related to QKD networks and proposals emerging from multiple bodies, including the International Telecommunication Union (ITU) Telecommunication Standardization Sector (ITU-T), the European Telecommunications Standards Institute (ETSI), the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), the Internet Engineering Task Force (IETF), the Institute of Electrical and Electronics Engineers (IEEE), and the Cloud Security Alliance (CSA). (Section VII)



Section I. Introduction
- I-A. Motivation
- I-B. Comparison to Existing Surveys
- I-C. Contributions
- I-D. Paper Organization

Section II. QKD Basics
- II-A. QKD Mechanism
- II-B. QKD Transmission Media
- II-C. QKD Implementation Options
- II-D. QKD Protocols

Section III. Advances in QKD Networks
- III-A. QKD Network Implementation Options
- III-B. Short-Range QKD Networks
- III-C. Metropolitan-Coverage QKD Networks
- III-D. Long-Haul QKD Networks

Section IV. QKD Networking Architecture
- IV-A. General Architecture of QKD Networks
- IV-B. QKD Network Elements
- IV-C. QKD Network Interfaces and Protocols

Section V. Enabling Techniques in the Physical Layer for QKD Networks
- V-A. Co-Fiber Transmission
- V-B. Relaying
- V-C. Satellite-Based QKD
- V-D. Chip-Based QKD

Section VI. Enabling Techniques in the Network Layer for QKD Networks
- VI-A. SDN
- VI-B. Key Pooling
- VI-C. Resource Allocation
- VI-D. Routing
- VI-E. Protection and Restoration
- VI-F. Practical Security
- VI-G. Cost Optimization
- VI-H. Multi-User QKD

Section VII. Standardization Efforts
- VII-A. ETSI
- VII-B. ITU-T
- VII-C. ISO/IEC
- VII-D. IETF
- VII-E. IEEE
- VII-F. CSA

Section VIII. On the Road to the Qinternet: Application Scenarios
- VIII-A. First Stage of the Qinternet
- VIII-B. QKD Applications in ICT Systems
- VIII-C. Application Areas

Section IX. Future Research Directions
- IX-A. QKD Network Itself
- IX-B. QKD Network Integration with Other Technologies
- IX-C. Beyond QKD Networks

Section X. Design Guidelines and a Brief Summary
- X-A. Trade-Offs in QKD Networks
- X-B. Design Guidelines
- X-C. Summary

Fig. 1. Outline of this survey paper.

5) We identify a range of detailed application scenarios and areas to illustrate how QKD networks can be used for securing numerous real-life applications. (Section VIII)

6) We discuss the open topics of QKD networks for future research. (Section IX)

7) Finally, we conclude by providing tangible design guidelines for QKD networks. (Section X)

D. *Paper Organization*

A detailed outline of this survey paper is depicted in Fig. 1. The remainder of this paper is organized as follows. Section II briefly introduces the QKD basics, while Section III reviews the practical development of QKD networks, followed by Section IV elaborating on their general architecture. Various emerging physical and network layer solutions are surveyed in Sections V and VI, respectively, complemented by the QKD network standardization efforts outlined in Section VII. Beneficial QKD network application scenarios are identified in Section VIII, while Section IX provides a range of future research directions. Finally, we summarize the design guidelines of QKD networks and conclude in Section X.

II. QKD Basics

In this section, we provide a rudimentary introduction to the essential basics of the QKD mechanism, transmission media, implementation options and protocols for making this treatise self-contained. A much more detailed review of QKD progress can be found in [24], [28]–[31], [33].

A. *QKD Mechanism*

Let us continue by illustrating a pair of conventional techniques conceived for achieving information security, as shown in Figs. 2(a) and 2(b). A classic cryptographic scheme is depicted in Fig. 2(a), in which a pair of legitimate parties (called Alice and Bob) use the public-key cryptosystem for key distribution and the symmetric-key cryptosystem for message encryption. The process of message encryption will transform the plaintext into ciphertext. By contrast, as depicted in Fig. 2(b), Alice and Bob can generate the secret keys directly from their common classical channel, and then the secret keys generated can be used by the symmetric-key cryptosystem to encrypt messages. The scheme in Fig. 2(b) is referred to as a physical layer security (PLS)-based cryptographic scheme [63], [64].

A QKD-based cryptographic scheme is illustrated in Fig. 2(c). Compared to the conventional approaches, the difference is that QKD exploits the laws of quantum physics to distribute

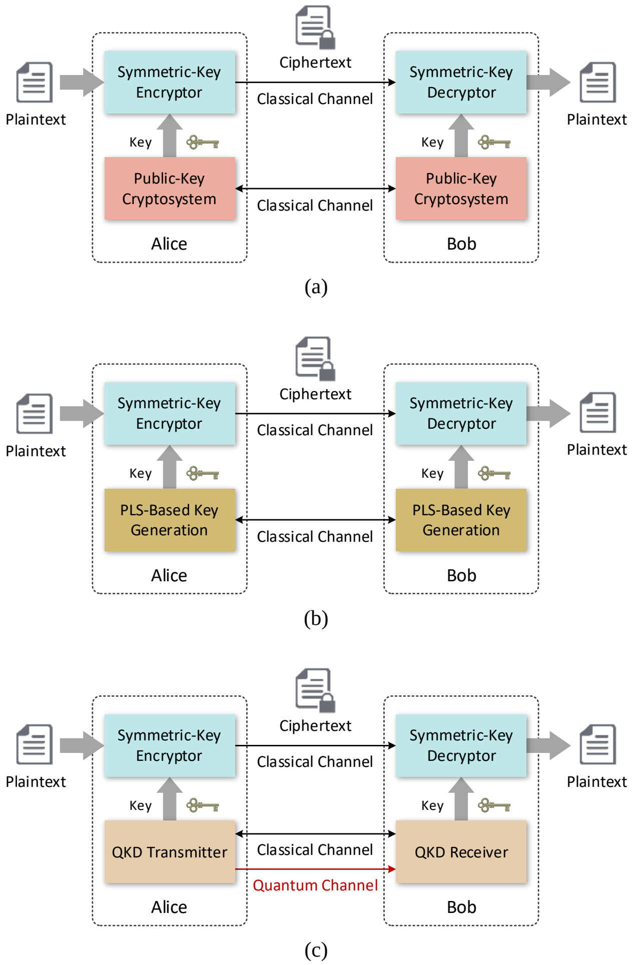


Fig. 2. Illustration of (a) a classic cryptographic scheme; (b) a PLS-based cryptographic scheme; (c) a QKD-based cryptographic scheme.

unconditionally secure symmetric secret keys between Alice and Bob, whereas the similarity is that the secret keys generated can also be used by a symmetric-key cryptosystem for message encryption. Generally, the basic elements of a QKD system are a transmitter and a receiver as well as a QKD link connecting the transmitter and receiver. The combination of the transmitter and receiver is commonly referred to as the QKD transceiver. The QKD transmitter/receiver encapsulates a set of hardware and software components used for QKD within a defined secure boundary. The QKD link relies on both a quantum channel and a classical channel. The quantum channel is used for transmitting quantum signals in which information is conveyed by quantum states, such as the polarization of a single photon. The classical channel is used to exchange classical information for synchronization and key distillation[3] between Alice and Bob [65], [66]. The unique features of the quantum channel as well as the fundamental differences between the quantum and classical channels have been discussed in [67], [68]. If an eavesdropper (called Eve) captures some of the quantum states during the passage of single photons through the quantum channel, those quantum states will not be used to distill secret keys, since they are not received by Bob. Eve can then potentially measure those quantum states, but the laws of quantum physics guarantee that following measurement or observation by Eve the quantum state collapses back into the classical domain. Hence, any potential eavesdropping on QKD can be detected.

Once the secret keys have been shared between Alice and Bob based on QKD or the conventional approaches shown in Fig. 2, they can be used for message encryption. More specifically, the secret keys generated can be fed into the symmetric-key encryptor and decryptor owned by Alice and Bob, respectively. Alice will encrypt the plaintext using the secret keys by the symmetric-key cryptosystem, and then transmits the ciphertext to Bob through a classical channel. Then Bob decrypts the ciphertext and obtains the plaintext. Consequently, QKD provides an information-theoretically secure way of distributing the symmetric secret keys, whereas message encryption can be carried out by the symmetric-key cryptosystem in just the same way as before.

B. QKD Transmission Media

The QKD links are constituted by the classical and quantum channels, both of which can be public, but they must be authenticated. The classical channel employed for transmitting classical signals can use the same medium as classical data communications, which is not detailed here. Compared to classical signals, quantum signals are much more vulnerable to propagation impairments such as the scattering and loss over optical fibers as well as the atmospheric turbulence encountered by free-space optical links. Unfortunately they cannot be readily amplified, because amplifying the quantum signals would require measuring and cloning the quantum states, which is contrary to the quantum no-cloning theorem [25]. Table III compares the features of current fiber-based QKD and free-space QKD schemes.

1) Optical Fiber: Optical fiber has a low loss and a high stability, hence it is more suitable for transmitting quantum signals. In recent years, substantial theoretical and experimental efforts have been invested into the design of QKD

TABLE III
OPTICAL FIBER VS. FREE SPACE FOR QKD

	Optical fiber	**Free space**
Stability	High	Low
Flexibility	Low	High
Maturity	High	Low
Cost	Low	High
Commercialization	Available	Unavailable
Achievable distance without relaying	605 km (104.8 dB) [73]	1,200 km (<33 dB) [75]
Future direction	Complement each other towards a global network	

[3] Key distillation [65], [66] is a bidirectional communication process used to send classical information from Alice to Bob or Bob to Alice, which typically performs sifting and post-processing. Sifting is used for Alice and Bob to agree on a subset of the raw data for subsequent post-processing. Post-processing usually includes error correction, verification, and privacy amplification for Alice and Bob to agree on a secret key.

over optical fibers, substantially improving both the attainable distance and the secret-key rate. Experimentally, QKD was shown to achieve secret-key rates of 1.2 Mbps over 50.5 km using a fiber link [69] and of 6.5 bps over a 405 km fiber link [70]. Indeed, in recent demonstrations, the achievable distance of the fiber-based QKD scheme has reached ~500 km in [71], [72] and ~600 km in [73]. Clearly, QKD systems relying on optical fiber are available on the market at the time of writing [38]–[40]. In the field, QKD can be implemented based on the existing pervasive fiber infrastructure to realize its practical deployment at a low cost. However, a grave limitation of fiber-based QKD is that it cannot readily pass through certain challenging terrains, rivers, etc. Furthermore, the achievable point-to-point distance remains limited to a few hundred kilometers owing to the absorption and noise of the quantum signals during long-distance transmission in optical fibers.

2) Free Space: Free-space optical links have the advantages of wide coverage and high flexibility, since they can be readily redirected on demand. Recently, there has been substantial progress on the experimental side of QKD over free-space optical links. Air-to-ground QKD has been demonstrated between an aeroplane and a ground station over a distance of 20 km in free space [74]. The first quantum satellite, named after Micius, has been launched in August 2016, demonstrating the feasibility of satellite-to-ground QKD at night between a low Earth orbit (LEO) satellite and the ground station over a distance of 1,200 km in free space [75]. Furthermore, free-space QKD has also been demonstrated over 53 km at daylight [76], and the feasibility of an underwater quantum channel has been verified in [77]–[80]. In 2020, the first experiment of free-space measurement-device-independent QKD (MDI-QKD) over a 19.2 km urban atmospheric channel was reported in [81]. In [82], the feasibility of air-water QKD was experimentally demonstrated. The theoretical upper limit for the achievable distance of QKD is influenced by diverse factors such as the relay type, the QKD protocol, and propagation loss. The relays and QKD protocols will be detailed in Sections V-B and II-D, respectively. The propagation loss scales exponentially in fibers, while only quadratically in free space and it becomes even negligible in vacuum above the Earth’s atmosphere [83]. Hence, provided that the quantum signals can survive after penetrating the Earth’s atmosphere, free-space QKD holds the promise of achieving longer distances than fiber-based QKD. However, free-space QKD is not as mature as fiber-based QKD, hence further studies are needed for advancing free-space QKD from experiments to practical environments. It is anticipated that QKD over optical fiber and free space will be integrated [49] for developing a global QKD network and the Qinternet.

C. QKD Implementation Options

QKD implementations rely either on discrete-variable QKD (DV-QKD) or on CV-QKD. A number of experiments have been performed both in the context of DV-QKD [69]–[76], [84]–[87] and CV-QKD [88]–[91], demonstrating the feasibility of these two options in practice. Both options tend to rely on the so-called prepare-and-measure approach [21], [92]–[98] for practical QKD implementations, where the quantum states are prepared by Alice and sent to Bob for measurement. Another attractive technique is the entanglement-based approach [99], [100], where the entangled states are prepared externally to Alice and Bob, which is more robust to environmental impairments. However, it is technologically less mature than the prepare-and-measure approach, hence we focus our attention on the prepare-and-measure approach in this survey. In this regard, the differences between DV-QKD and CV-QKD are briefly summarized in Table IV and elaborated on as follows.

TABLE IV
DV-QKD VS. CV-QKD

	DV-QKD	**CV-QKD**
Quantum state	Polarization, phase, or time bin of a single photon	Quadrature components of quantized electromagnetic field
Source	Single-photon source	Coherent-state or squeezed-state source
Detector	Single-photon detector	Homodyne or heterodyne detector
Channel model	Lossy qubit channel	Lossy bosonic channel
Distance limitation	Performance of single-photon detectors	Efficiency of post-processing techniques

1) DV-QKD: In DV-QKD systems, the information is mapped to discrete quantum states, such as the polarization, phase, or time bin of a single photon. At the transmitter side, a single-photon source is preferred. However, significant technological challenges have to be tackled to realize a perfect single-photon source. At the current state-of-the-art hence weak pulses of laser light are used for approximating the single-photon sources. On the receiver side, single-photon detectors are utilized. As for the channel model, typically a lossy quantum bit (qubit) channel is considered. The achievable point-to-point distance of DV-QKD is mainly limited by the performance (e.g., detection efficiency) of single-photon detectors [101].

2) CV-QKD: In CV-QKD systems [60], the information is mapped to continuous-valued quantum states, such as the quadrature components of the quantized electromagnetic field (including coherent states and squeezed states). At the transmitter side, a coherent-state source or a squeezed-state source is widely used. At the receiver side, homodyne or heterodyne detectors are employed. With respect to the channel model, a lossy bosonic channel is considered. The achievable point-to-point distance of CV-QKD is mainly limited by the efficiency of the post-processing techniques used.

A more detailed description and comparison of DV-QKD and CV-QKD can be found in [24], [31], [60]. At the time of writing, DV-QKD systems are technologically more mature than CV-QKD systems. Hence CV-QKD systems have recently attracted more intense research attention and achieved technical advances owing to their high grade of compatibility with the

TABLE V
SUMMARY OF TYPICAL QKD PROTOCOLS

Protocol	Type	Approach	Year	Ref.
BB84	DV	Prepare-and-measure	1984	[21]
E91	DV	Entanglement-based	1991	[99]
BBM92	DV	Entanglement-based	1992	[100]
GG02	CV	Prepare-and-measure	2002	[92]
DPS	DV	Prepare-and-measure	2002	[93]
Decoy-state	DV	Prepare-and-measure	2003–2005	[94]–[96]
SARG04	DV	Prepare-and-measure	2004	[97]
COW	DV	Prepare-and-measure	2005	[98]
MDI	DV/CV	Prepare-and-measure	2012	[106]
TF	DV	Prepare-and-measure	2018	[107]
PM	DV	Prepare-and-measure	2018	[108]

existing telecommunication devices [102], [103]. Ultimately, hybrid DV-QKD and CV-QKD systems [104], [105] constitute flexible design alternatives for further research.

D. QKD Protocols

Based on the different QKD implementation options, several QKD protocols have been invented. Table V summarizes a number of typical QKD protocols, including the seminal Bennett-Brassard-1984 (BB84) [21], Grosshans-Grangier-2002 (GG02) [92], differential-phase-shift (DPS) [93], decoy-state [94]–[96], Scarani-Acín-Ribordy-Gisin-2004 (SARG04) [97], coherent-one-way (COW) [98], Ekert-91 (E91) [99], Bennett-Brassard-Mermin-1992 (BBM92) [100], measurement-device-independent (MDI) [106], twin-field (TF) [107], and the phase-matching (PM) [108] protocols. A comprehensive overview of QKD protocols can be found in [24], [28], [31], [33], [53]. Here we briefly introduce three typical QKD protocols.

1) BB84 Protocol: The BB84 protocol is the seminal QKD protocol invented by Bennett and Brassard in 1984 [21], which may be readily used for DV-QKD. It is still widely used at the time of writing, and it is the starting point for developing more sophisticated QKD protocols. In the BB84 protocol, five stages are performed, as illustrated in Fig. 3 and explained as follows.

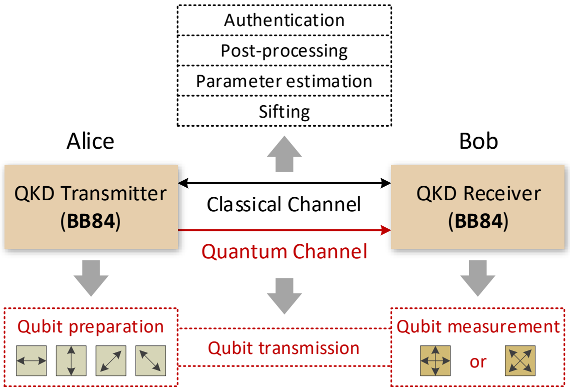


Fig. 3. Illustration of five stages in the BB84 protocol.

1) *Qubit preparation, transmission, and measurement:* Alice generates a sequence of classical bits (called raw keys) and encodes them into a stream of single photons to generate qubits. Each single photon possesses one of the four polarization states, namely, horizontal (0°), vertical (90°), diagonal (+45°), and antidiagonal (−45°) corresponding to the classical bits 0, 1, 1, and 0, respectively. The qubits are then sent to Bob through a quantum channel. Bob receives the incoming qubits and carries out measurement of each qubit relying on one of the two conjugate bases, namely the rectilinear (+) and diagonal (×) bases. Bob also records the measurement bases and results.
2) *Sifting:* Alice and Bob, respectively, share their encoding and measurement bases through a classical channel, which may however be accommodated within a single fiber using wavelength-division multiplexing (WDM). The specific qubits associated with mismatched polarization states and measurement bases are discarded, while the remaining qubits corresponding to the matching bases are decoded into a stream of bits (called sifted keys).
3) *Parameter estimation:* At this stage, the quantum bit error rate (QBER) is estimated by sacrificing a portion of the sifted keys to verify that it is below a predetermined threshold value. Notably, this is not the only option for QBER estimation. For example, Alice and Bob can first correct the errors, based on which they can more accurately specify the QBER without losing part of the data. If the estimated QBER is above the threshold value, the QKD process will be aborted and restarted from the first stage due to potential eavesdropping on the quantum channel, which contaminates the quantum states.
4) *Post-processing:* Alice and Bob perform error correction, verification, and privacy amplification through a classical channel to distill the final string of secure bits (called secret keys).
5) *Authentication:* The first QKD session is authenticated using the full pre-shared secret key between Alice and Bob. Subsequent QKD sessions can be authenticated using a small part of the agreed secret keys to avoid the man-in-the-middle attack[4] [109].

A perfect single-photon source is required by the BB84 protocol, but this is still unavailable in practice. Instead, a highly attenuated laser source that can generate weak coherent pulses is commonly adopted by the BB84-protocol-based QKD systems. Such a laser source may emit multiple photons in a pulse, making the QKD system vulnerable to a photon number splitting attack [5] [110], [111]. Fortunately, the so-called

[4] The man-in-the-middle attack [109] is a cyberattack where an attacker in the middle of Alice and Bob intercepts the message from Alice and sends his message to Bob, while both Alice and Bob believe that they are directly communicating with each other.

[5] The photon number splitting attack [110] is a physical attack in which an eavesdropper splits a pulse comprising two or more photons through a physical interaction [111] to keep one photon, such that the eavesdropper can then obtain the secret-key information relying on the intercepted photons.

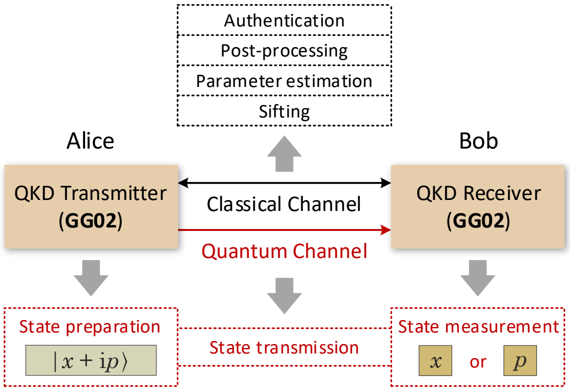


Fig. 4. Illustration of five stages in the GG02 protocol.

decoy-state method [94]–[96] has been proposed for overcoming the photon number splitting attack by adding decoy states in the BB84 protocol. To elaborate a little further, in a decoy-state QKD system, Alice generates some decoy states in which the number of photons is different from that in the original signal state. Hence there is only one genuine signal state and several decoy states represented by multiple intensity levels. Alice and Bob can monitor and analyze the statistical characteristics of both types of states, where the decoy states are used for detecting photon number splitting attacks and the genuine signal state is used for producing the secret keys. Thanks to the discovery of the decoy-state method, QKD becomes practical even with the aid of weak coherent pulses, in the absence of perfect single-photon sources at the time of writing.

2) GG02 Protocol: The GG02 protocol was developed by Grosshans and Grangier in 2002 [92], which can implement Gaussian-modulated CV-QKD relying on coherent states. It is one of the most widely used CV-QKD protocols and has been adopted in commercial CV-QKD systems [112]. Similar to the BB84 protocol, the GG02 protocol also consists of five stages, as illustrated in Fig. 4 and described below.

1) *State preparation, transmission, and measurement:* Alice prepares the coherent state $|x + ip\rangle$, in which x and p are the real and imaginary components of the electromagnetic field corresponding to the two quadratures of a coherent state. The coherent state is sent to Bob through a quantum channel. Bob randomly measures one of the two quadratures of the coherent state and records which measurement he made.
2) *Sifting:* Bob informs Alice through a classical channel about which quadrature he measured, based on which Alice discards the irrelevant data. At this stage, Alice and Bob share a set of correlated Gaussian variables (called key elements).
3) *Parameter estimation:* Alice and Bob reveal a random portion of their key elements through the classical channel to estimate the transmission efficiency and excess noise of the quantum channel.
4) *Post-processing:* Even with no eavesdropper present and with perfect state preparation as well as measurement, errors are typically unavoidable owing to the intrinsic quantum noise. The first task in post-processing is the discretization of the analogue (continuous) data, which is usually performed in conjunction with error reconciliation to maximize the efficiency. Error reconciliation is invoked for transmission over the classical channel, and then Alice and Bob share a string of bits that might be partially captured by Eve. Next, a verification step is performed for ascertaining that Alice and Bob have identical secret keys. Finally, Alice and Bob perform privacy amplification to eliminate the information that Eve can obtain, and distill the final secret keys.
5) *Authentication:* An authentication step (as in the BB84 protocol) can be implemented to authenticate the QKD sessions in order to prevent the man-in-the-middle attack [109].

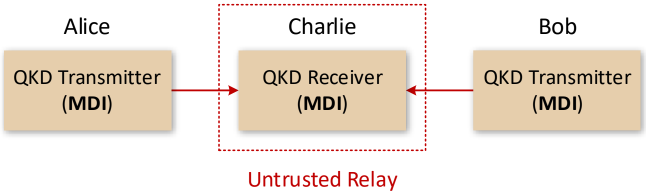


Fig. 5. Illustration of MDI-QKD.

3) MDI[6] Protocol: The MDI-QKD protocol was first proposed by Lo *et al.* [106] in 2012 to fill the detection loophole (i.e., all detector side channels [31]) in practical QKD systems, which allows Alice and Bob to share the secret keys via an untrusted relay (called Charlie) located in the middle. As shown in Fig. 5, both Alice as well as Bob have a transmitter, and they generate as well as transmit quantum signals to Charlie. The positions of Alice and Bob are symmetric in general. Charlie then performs a Bell state measurement to project the incoming quantum signals into a Bell state, and publicly announces the measurement results to correlate the key information of Alice and Bob. Inspired by this idea, several discrete-variable MDI-QKD [113]–[115] and continuous-variable MDI-QKD [116]–[118] schemes have been invented. Remarkably, novel variants of MDI-QKD protocols, such as the TF-QKD [107] and PM-QKD [108] protocols, were shown to be capable of overcoming the rate-distance limit of conventional MDI-QKD. Meanwhile, asymmetric protocols have also been proposed to overcome the symmetric channel limitation (i.e., Alice and Bob have symmetric distances with similar losses to the untrusted relay) of MDI-QKD [119], [120]. The only assumption in MDI-QKD is that Alice and Bob trust their sources. Even this assumption can be relaxed with the aid of the device-independent QKD (DI-QKD) philosophy [121]–[123]. In contrast to the MDI-QKD protocol that is feasible to implement in practical

[6] MDI implies that the security of QKD does not depend on the measurement device at the receiver side, that is, the MDI-QKD process remains secure even if the measurement device is controlled by an eavesdropper.

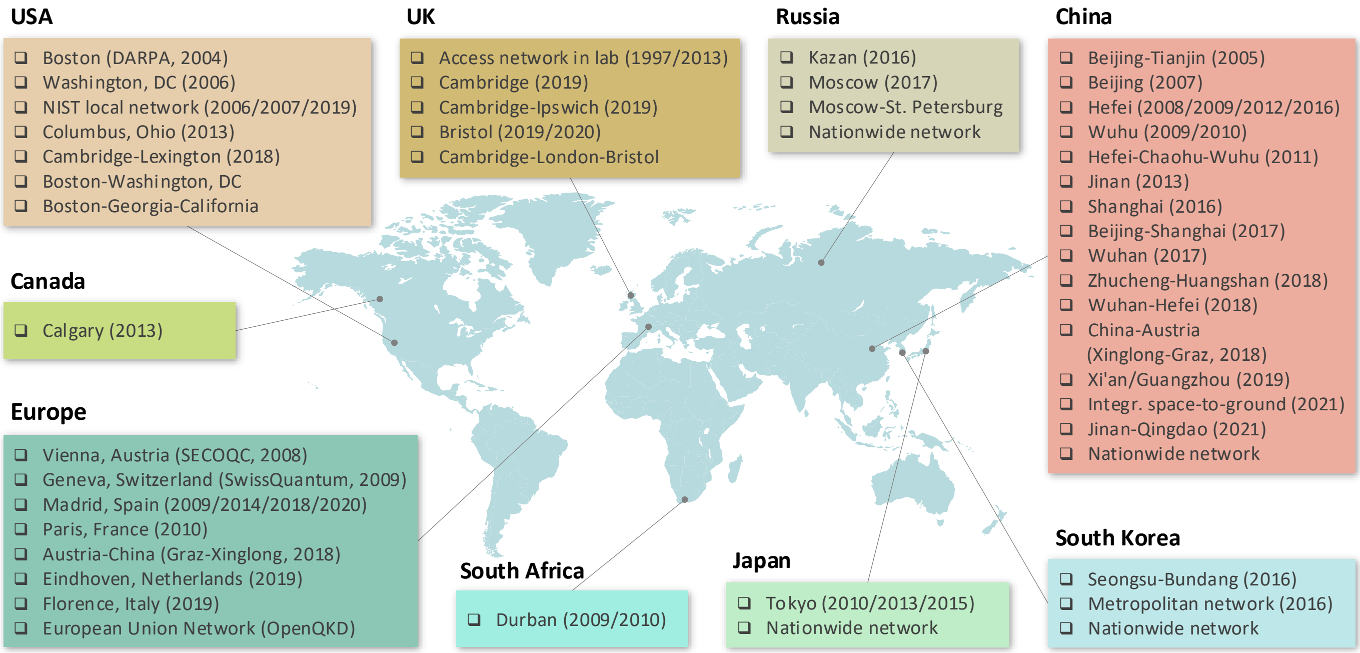


Fig. 6. Overview of QKD network testbeds and field trials around the world.

QKD systems, the DI-QKD implementation remains a challenge and further advances are needed to make DI-QKD more practical [124].

At the time of writing, already numerous QKD systems have been commercialized by using various protocols (e.g., BB84 and COW) belonging to the prepare-and-measure approach and in a pattern in which the QKD transmitter and receiver have a one-to-one relationship [38]–[40]. A realistic QKD system is constrained by many impairments, such as the fiber type and length, wavelength-dependent attenuation, temperature, and hacking attacks. Furthermore, the critical parameters are the clock rate, secret-key rate, QBER, and key failure probability (i.e., the probability that at least one bit of the key is leaked to an eavesdropper). These parameters are typically dependent on the type of systems based on dissimilar QKD protocols in real-world environments. As a new parameter example, a QKD system with 1 GHz clock rate implemented by Toshiba can achieve a secret-key rate over 1 Mbps at 1550 nm wavelength for 10 dB loss (equivalent to 50 km of standard fiber) using an efficient BB84 protocol with decoy states, where the QBER is less than 5% and the key failure probability is less than 10^{-10} [125]. It has been reported to support coexistence with >32×10 Gb/s data channels, single/dual fiber channel and room temperature operation, as well as protection against several hacking attacks [40]. As a result, the practicability of QKD systems provides a solid foundation for QKD networking in the real world. Some of the practical QKD systems are: the Cambridge QKD metro network [47] using Toshiba's QKD systems; the Madrid QKD metro network [126] based on Huawei's QKD systems; the Bristol QKD metro network [127] and the Cambridge-Ipswich QKD backbone network [128] relying on ID Quantique QKD systems; the Hefei QKD metro network [129] relying on QuantumCTek QKD systems. These networks will be detailed in the next section.

III. Advances in QKD Networks

The penetration of QKD networks is growing rapidly around the world, evolving from testbeds to the field, as depicted in Fig. 6. In this section, we first give a brief introduction to the popular QKD network implementation options. Then, we continue with the critical appraisal of QKD networks spanning from short-range to metropolitan-coverage and long-haul QKD scenarios.

A. *QKD Network Implementation Options*

Based on the specific node functionalities, QKD network implementations tend to rely on either optical switching or on trusted relays, untrusted relays or alternatively, on quantum repeater based solutions. Table VI compares the basic features

TABLE VI
Comparison of Different QKD Network Implementation Options

	Optical switching	**Trusted relay-based**	**Untrusted relay-based**	**Quantum repeater**
Achievable distance	Relatively short	Arbitrary	Relatively long	Arbitrary
Scalability	Relatively low	High	Relatively low	High
Applicability	Limited	Wide	Limited	Wide
Security	High	Relatively low	High	High
Maturity	High	High	Relatively low	Low
Field trial	Available	Available	Available	Unavailable

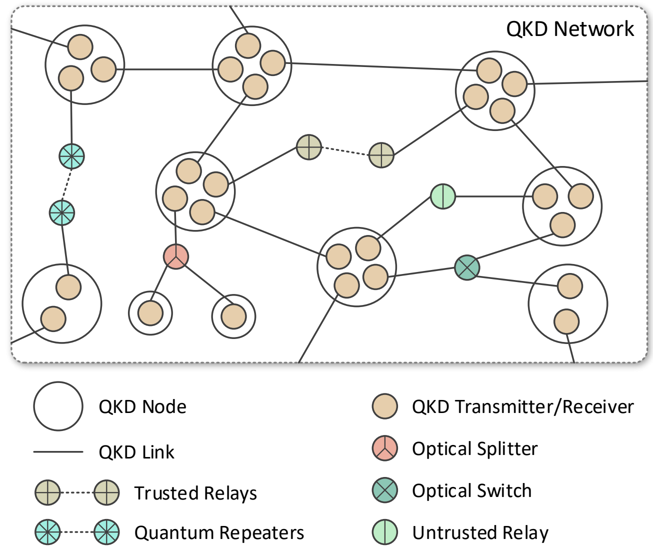


Fig. 7. Illustration of a QKD network incorporating the four relaying options.

of these options. At the time of writing, the optical switching and trusted relay schemes are more mature than the untrusted relay and quantum repeater based schemes.

1) Optical Switching Based QKD Networks: In an optical switching based QKD network, several classical optical functions such as beam splitting and switching can be applied to the quantum signals transmitted over a quantum channel for connecting a pair of QKD nodes, which can be readily implemented using commercial technologies. The quantum signals can be transmitted through short quantum links without any interaction with untrusted nodes. Hence these short links are less prone to eavesdropping than their long-haul counterparts. However, they are only suitable for small-scale access networks [130] and for relatively small metropolitan networks [131], because the attenuation of quantum signals cannot be eliminated by amplification.

2) Trusted Relay Based QKD Networks: In contrast to the above short-range scenario, in a trusted relay based QKD network (commonly referred to as a trusted-node QKD network), local secret keys are produced for each QKD link and then stored in the nodes that are located at both ends of each QKD link. Long-distance QKD between two end nodes can be realized along a chain of concatenated QKD links relying on a one-dimensional chain of trusted relays connected by the QKD links. The secret keys are forwarded from the source node to the destination node in a hop-by-hop manner along the QKD path, where the one-time pad technique is used for encryption to ensure end-to-end information-theoretic security of the secret keys. This QKD network implementation option is practical and eminently scalable, hence it has been widely adopted for the deployment of QKD networks in the field. It should be noted that each trusted relay is assumed to be protected against any intrusion or attack. In this paper, the commercial feasibility of trusted relays will be discussed in Section V-B. However, we have to note in closing that all networking protocols, which exploit the idealized simplifying assumption that the relays are trusted are inherently less secure than their counterparts, which assume that the relays cannot be trusted. Hence more robust security protocols must be conceived for realistic untrusted relays.

3) Untrusted Relay Based QKD Networks: In contrast to the trusted relay scheme of Table VI that can be used in conjunction with any QKD protocols, an untrusted relay based QKD network has to rely on more secure QKD protocols such as MDI and the family of entanglement-based protocols. An untrusted relay relying on the MDI protocol typically has better security than a trusted relay based protocol, because it can remove all security loopholes at the measurement side. It even allows the untrusted relay to be controlled by an eavesdropper without affecting the security of QKD. An untrusted relay based protocol is also capable of extending the secure distance of QKD quite considerably. For example, the attainable distance of a stand-alone untrusted relay is limited to ~500 km in [72] and ~600 km in [73] using TF-QKD protocols. However, the untrusted relay cannot extend QKD to an arbitrary distance, since the QKD protocol does not allow the direct connection of two untrusted relays. Hence, this QKD network is more suitable for limited-range access and metropolitan networks [132], while its large-scale extension requires its integration with trusted relays. However, this reduces its security level.

4) Quantum Repeater Based QKD Networks: In the quantum repeater based QKD network of Table VI, quantum repeaters [51], [133]–[135] are adopted for mitigating the distance-dependent impairments imposed on quantum signals. A quantum repeater at an intermediate node can create long-distance entanglement between the source and destination nodes relying on a physical process known as entanglement swapping[7] [51], [133]–[135]. Explicitly, a quantum repeater is expected to decontaminate and forward the quantum signals without directly measuring or cloning them. However, such an idealized quantum repeater is still unavailable at the time of writing, hence long-haul quantum repeater based QKD networks are yet to be rolled out in the field. In this paper, the progress on quantum repeaters will be outlined in Section V-B.

To elaborate a little further, a QKD network incorporating the above four relaying options is shown in Fig. 7. In addition to the QKD transmitter/receiver, a QKD node may incorporate the functionality of the optical switch/splitter, and the trusted/untrusted relay or the quantum repeater. The secret keys are generated between any pair of QKD nodes or trusted relays. The position of the trusted relay may be referred to as a secret-key relay point. By contrast, the position of the optical switch/splitter, and of the untrusted relay or the quantum repeater may be referred to as a quantum-signal relay point, where no secret keys are generated or relayed. Hence the quantum-signal relay point does not have to be trusted.

[7] Entanglement swapping can extend entanglement distances by splicing two Bell pairs spanning short distances between adjacent nodes into one pair over the longer distance [51], [133]–[135]. For example, if nodes A and B share a Bell pair as well as nodes B and C share another Bell pair, then node B can perform entanglement swapping to create a Bell pair between nodes A and C.

B. Short-Range QKD Networks

The short-range QKD networks allow multiple users to communicate securely, but only in access/local networks.

1) QKD Access Networks: A QKD access network may serve a multitude of end users as a last mile solution by relying on point-to-multipoint connections, where the downstream and upstream QKD access networks [130] are illustrated in Figs. 8(a) and 8(b), respectively, which employ optical switching based solutions. Observe in Fig. 8(a) that a transmitter is placed at the network node and each user has a receiver in the downstream QKD access network. By contrast, a receiver is located at the network node and each user has a transmitter in the upstream QKD access network. A passive optical splitter is adopted for directing the quantum signals from a transmitter to a receiver based on the unidirectional nature of the QKD process. In 1997, Townsend [136] was the first author, who reported the implementation of a downstream QKD access network relying on a single transmitter and three receivers in the lab. In 2013, an upstream QKD access network was successfully demonstrated in the lab [130], allowing up to 64 users to share a single-photon detector at a network node. In 2011, the futuristic quantum-to-the-home concept has been proposed for providing perfect end-to-end security to users [137], which may be offered in the near future by the Eindhoven QKD network testbed [138]. In this paper, the progress on the design of multi-user QKD over access networks will be presented in Section VI-H.

2) QKD Local Networks: In addition to the above-mentioned passive optical splitter, other optical components such as optical switches can also be used by local QKD networks. Tang *et al.* [139] and Ma *et al.* [140] reported on the demonstration of a local QKD network at the National Institute of Standards and Technology (NIST) in 2006 and 2007, respectively. As shown in Fig. 9, this network contained a transmitter and two receivers, where an optical switch was used for dynamically switching the QKD connections. Specifically, the application of QKD-secured video surveillance was demonstrated. In 2019, Ma *et al.* reported in [141] on their plan of building a field testbed on the NIST campus, in which the feasibility and compatibility of QKD integration with optical fiber networks will be tested.

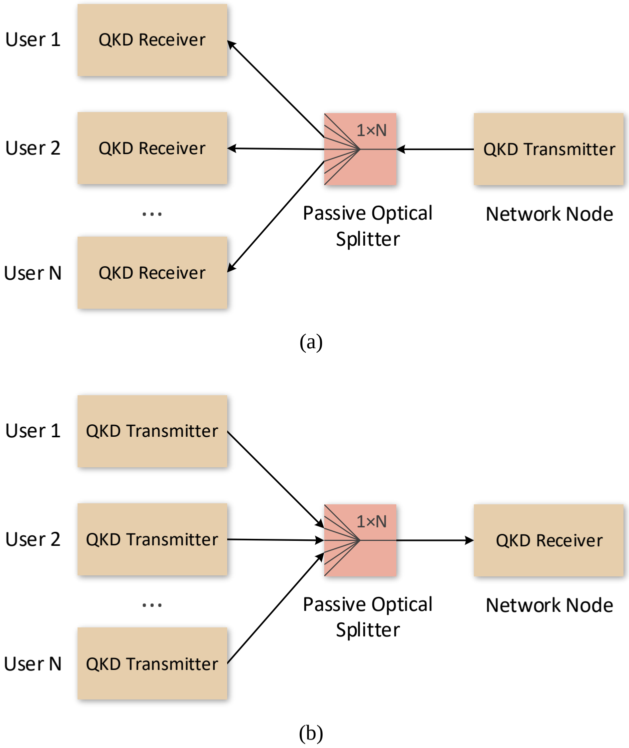


Fig. 8. Illustration of (a) downstream and (b) upstream QKD access networks.

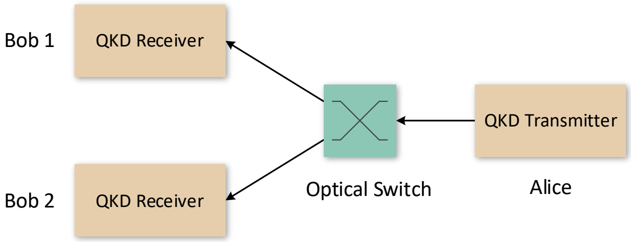


Fig. 9. Illustration of a local QKD network.

C. Metropolitan-Coverage QKD Networks

Again, a growing number of QKD networks have been deployed in the metropolitan-coverage field. They serve as the bridge between the access/local network and the backbone/core network. Tables VII and VIII chronologically list and summarize the basic features of QKD networks and links deployed in various metropolitan areas, respectively. Some details of typical QKD metropolitan networks are exemplified below.

1) Boston Metropolitan Network: The DARPA QKD network [42], [142] is the world's first QKD metropolitan network deployed in Boston, USA. This network was first operated in the Bolt Beranek and Newman (BBN) lab in October 2003, and then it was extended to six nodes spanning BBN, Harvard University and Boston University in June 2004. In 2005, four more nodes were planned to be added in this network. Finally, this network evolved to ten nodes and relied on optical switches and trusted relays.

2) Beijing Metropolitan Network: In 2007, Chen *et al.* [143] reported on a wavelength-routing based star-type QKD metropolitan network in Beijing, China. The BB84 and the decoy-state BB84 [94]–[96] protocols were utilized. This network relied on the commercial telecommunication network infrastructure, demonstrating the feasibility of integrating QKD into existing networks. Based on a four-port QKD router [177] designed for this four-node network, passive routing was implemented with the aid of WDM techniques.

3) Vienna Metropolitan Network: The European project termed as the secure communication based on quantum cryptography (SECOQC) based QKD network [43], [144]–[146] is a trusted relay based QKD metropolitan network installed in Vienna, Austria. This network contained six nodes connected by eight QKD links (including seven optical fiber links and a free space link), which was put into operation in 2008. Multiple QKD protocols were adopted in this network, including several DV-QKD protocols (e.g., BB84, SARG04, decoy-state BB84, COW, and BBM92) and a CV-QKD protocol. Diverse applications, including OTP-encrypted telephone conversations, AES-encrypted video conferencing, and traffic rerouting required by heavy tele-traffic have been demonstrated in this network.

4) Geneva Metropolitan Network: The SwissQuantum QKD network [45] was installed in Geneva, Switzerland and operated over the period spanning from March 2009 to January 2011. This network consisted of three nodes and three QKD fiber links relying on trusted relays. Only the SARG04 protocol was used for QKD and commercial devices were applied in this network. The reliability and robustness of this network have been tested and verified in a realistic environment, demonstrating that QKD can be integrated into complex network infrastructures.

5) Tokyo Metropolitan Network: The Tokyo QKD network [44] was operated in 2010, which was composed of six trusted QKD nodes connected by six optical fiber links. Four different QKD protocols were utilized in this network, namely the decoy-state BB84, BBM92, DPS, and SARG04. A common application interface was developed for supporting the interoperability of the different QKD systems. The applications supported by this network included secure video conferencing and a secure mobile phone.

6) Hefei Metropolitan Network: In 2008, Chen *et al.* [147] portrayed a three-node trusted relay based QKD network in Hefei, China, in which the decoy-state BB84 protocol and a commercial optical fiber link were utilized. OTP-encrypted real-time audio communication was realized. In 2016, Tang *et al.* [132] reported on the field trial of a MDI-QKD metropolitan network in Hefei city, as shown in Fig. 10. This network has a star-type topology with four nodes, including an untrusted relay and three QKD nodes, which are connected by optical fiber links, demonstrating that the MDI-QKD scheme is eminently

TABLE VII
SUMMARY OF THE BASIC FEATURES OF DIFFERENT QKD NETWORKS DEPLOYED IN VARIOUS METROPOLITAN AREAS

Metropolitan area	**Optical switching**	**Trusted relay**	**Number of nodes**	**Link type**	**Longest link**		**Maximum secret-key rate**	**QKD type**	**Year**	**Reference**
					Length	**Loss**				
Boston	✓	✓	10	Optical fiber Free space	29.8 km	16.6 dB	10 kbps	DV	2004	[42], [142]
Beijing	✓	×	4	Optical fiber	42.6 km	16.4 dB	N/A	DV	2007	[143]
Vienna	×	✓	6	Optical fiber Free space	85 km	20.4 dB	17 kbps	DV CV	2008	[43], [144]–[146]
Hefei	×	✓	3	Optical fiber	20 km	5.6 dB	1.6 kbps	DV	2008	[147]
Geneva	×	✓	3	Optical fiber	17.1 km	–5.3 dB	2.4 kbps	DV	2009	[45]
Durban	✓	✓	4	Optical fiber	27 km	N/A	891 bps	DV	2009	[148]
Wuhu	✓	✓	7	Optical fiber	10 km	6.23 dB	2.53 kbps	DV	2009	[149]
Hefei	✓	✓	5	Optical fiber	60 km	17 dB	4.5 kbps	DV	2009	[150]
Madrid	✓	×	3	Optical fiber	N/A	N/A	N/A	DV	2009	[151]
Wuhu	✓	×	5	Optical fiber	N/A	14.77 dB	4.91 kbps	DV	2010	[152]
Tokyo	×	✓	6	Optical fiber	90 km	27 dB	304 kbps	DV	2010	[44]
Hefei	✓	✓	46	Optical fiber	N/A	N/A	N/A	DV	2012	[46], [153]
Columbus	×	✓	4	Optical fiber	N/A	N/A	N/A	DV	2013	[154], [155]
Jinan	✓	✓	56	Optical fiber	N/A	N/A	N/A	DV	2013	[30], [46], [153]
Madrid	✓	×	3	Optical fiber	16 km	5.12 dB	N/A	DV	2014	[156]
Hefei	✓	×	4	Optical fiber	55 km	17.3 dB	38.8 bps	DV	2016	[132]
Shanghai	×	×	4	Optical fiber	19.92 km	15.1 dB	10 kbps	CV	2016	[157]
Kazan	×	✓	4	Optical fiber	12.4 km	6.8 dB	19.6 kbps	DV	2016	[158]
South Korea	×	×	5	Optical fiber	107 km	N/A	N/A	DV	2016	[159], [160]
Moscow	×	✓	3	Optical fiber	30 km	13 dB	0.1 kbps	DV	2017	[161]
Wuhan	✓	✓	>60	Optical fiber	N/A	N/A	N/A	DV	2017	[162]
Madrid	×	✓	3	Optical fiber	26.4 km	11 dB	70 kbps	CV	2018	[126], [163]
Bristol	✓	×	4	Optical fiber	2.7 km	N/A	3.17 kbps	DV	2019	[127]
Cambridge	×	✓	3	Optical fiber	10.6 km	3.9 dB	2.58 Mbps	DV	2019	[47]
Madrid	✓	✓	11	Optical fiber	55 km	12 dB	N/A	CV	2020	[164]
Bristol	×	×	8	Optical fiber	16.9 km	29 dB	83.9 kbps	DV	2020	[165]
Hefei	✓	✓	46	Optical fiber	18 km	N/A	60.5 kbps	DV	2021	[129]

TABLE VIII
SUMMARY OF THE BASIC FEATURES OF DIFFERENT QKD LINKS DEPLOYED IN VARIOUS METROPOLITAN AREAS

Metropolitan area	**Node location**	**Number of nodes**	**Link type**	**Link length**	**Link loss**	**Secret-key rate**	**QKD type**	**Year**	**Reference**
Intercity	Beijing, Tianjin	2	Optical fiber	125 km	26 dB	N/A	DV	2005	[166]
Washington	Two sites in Washington	2	Optical fiber	25 km	9 dB	1.09 kbps	DV	2006	[167], [168]
Durban	Two sites in Durban	2	Optical fiber	2.8 km	2.1 dB	N/A	DV	2010	[169]
Paris	Massy, Palaiseau	2	Optical fiber	17.7 km	5.6 dB	600 bps	CV	2010	[170]
Calgary	Three sites in Calgary	3	Optical fiber	18.6 km	9 dB	N/A	DV	2013	[171]
Tokyo	Koganei, Otemachi	2	Optical fiber	90 km	30 dB	1.1 kbps	DV	2013	[172]
Hefei	Three sites in Hefei	3	Optical fiber	30 km	9.2 dB	16.9 bps	DV	2014	[173]
Tokyo	Otemachi, Koganei	2	Optical fiber	45 km	14.5 dB	301 kbps	DV	2015	[174]
South Korea	Seongsu, Bundang	2	Optical fiber	35 km	N/A	N/A	DV	2016	[159], [160]
Intercity	Cambridge, Lexington	2	Optical fiber	43 km	16.4 dB	157 kbps	DV	2018	[175]
Xi’an	Two sites in Xi’an	2	Optical fiber	30.02 km	12.48 dB	7.57 kbps	CV	2019	[91]
Guangzhou	Two sites in Guangzhou	2	Optical fiber	49.85 km	11.62 dB	7.43 kbps	CV	2019	[91]
Florence	Two sites in Florence	2	Optical fiber	40 km	21 dB	4.53 kbps	DV	2019	[176]

suitable for the construction of a QKD network using untrusted relays. In reality, MDI-QKD networks still need extensive development before they are mature enough to be widely deployed.

7) Madrid Metropolitan Network: In 2018, Martin *et al.* [126] reported on the field trial of a SDN-enabled QKD network in the metropolitan area of Madrid, which is shown in Fig. 11. This network connected three different sites using CV-QKD. The flexibility of this network was enhanced with the aid of an SDN technique [163], and the co-propagation of quantum and classical signals in the same optical fiber was demonstrated in [178]. In this paper, the issues of co-fiber transmission and SDN aided QKD networking will be discussed in Sections V-A and VI-A, respectively.

8) Shanghai Metropolitan Network: In 2016, Huang *et al.* [157] described the field trial of a full-mesh CV-QKD metropolitan network in Shanghai, China. A CV-QKD protocol based on Gaussian-modulated coherent states [179] was applied. This network is composed of four nodes connected by six QKD links using commercial optical fibers, which can provide all-to-all interconnections without the use of optical switching or trusted relays. In this network, classical and quantum signals coexist in the same fiber using the WDM technique, demonstrating the feasibility of deploying CV-QKD in a practical telecommunication environment.

9) Cambridge Metropolitan Network: In 2019, Dynes *et al.* [47] reported on the field trial of a three-node ring-type QKD metropolitan network in Cambridge, UK, as illustrated in Fig. 12. This network relied on DV-QKD and on an efficient version of the BB84 protocol using decoy states [125]. The quantum and classical channels were multiplexed in the same fiber with the aid of dense wavelength-division multiplexing (DWDM). Based on a long period of testing, the secret keys were shown to be produced at high rates of 2–3 Mbps on each QKD link, which can be used for AES-encrypted data

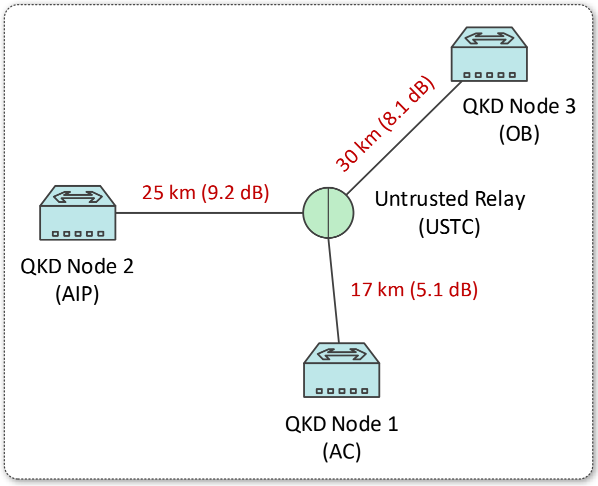


Fig. 10. Illustration of a MDI-QKD metropolitan network in Hefei [132].

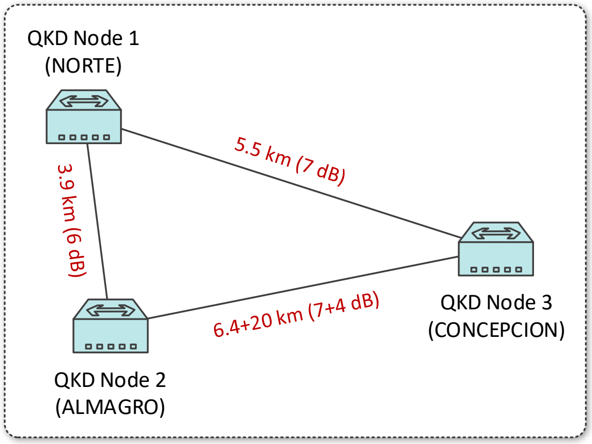


Fig. 11. Illustration of a SDN-enabled CV-QKD metropolitan network in Madrid [126], [163].

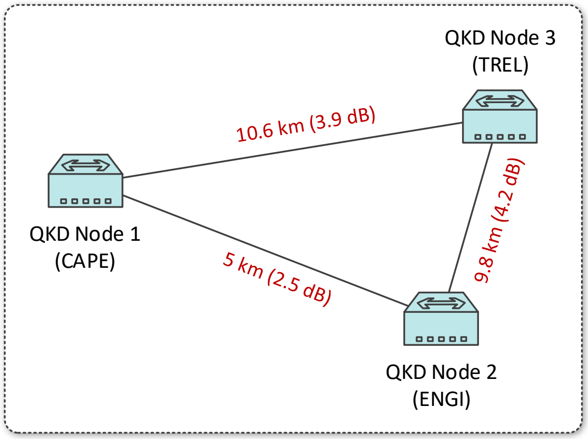
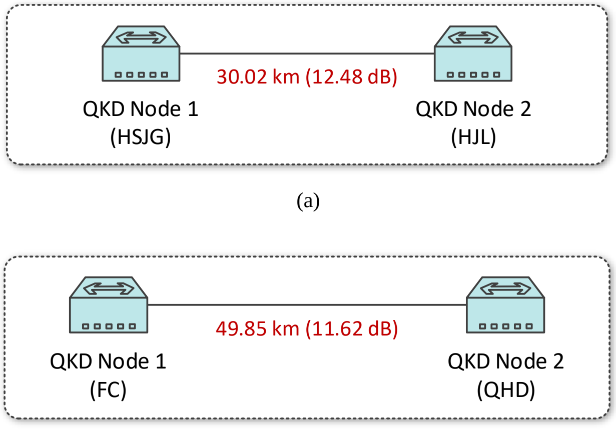


Fig. 12. Illustration of a DV-QKD metropolitan network in Cambridge [47].



(a)

(b)

Fig. 13. Illustration of two different CV-QKD metropolitan links in (a) Xi'an and (b) Guangzhou [91].

transmission.

10) Bristol Metropolitan Network: In 2019, Tessinari *et al.* [127] reported on the field trial of a fully meshed metropolitan network relying on dynamic QKD networking capabilities across four nodes in Bristol, UK. Again, the coexistence of quantum and classical channels in the same fiber was demonstrated. In particular, the SDN technique was utilized for supporting dynamic quantum/classical switching and for providing QKD-secured connectivity. In 2020, Joshi *et al.* [165] demonstrated a fully connected QKD network without trusted nodes in Bristol. Specifically, an entanglement-based QKD protocol, namely the BBM92 protocol, was utilized to support secure connections between the 28 different pairs of eight users. Hence, the feasibility of entanglement-based QKD networking was demonstrated.

11) Xi'an/Guangzhou Metropolitan Link: In 2019, Zhang *et al.* [91] reported two different field tests of their metropolitan CV-QKD fiber link in Xi'an and Guangzhou, China, as illustrated in Figs. 13(a) and 13(b), respectively. The fiber lengths of these field tests in Xi'an and Guangzhou were 30.02 km and 49.85 km, respectively, where the maximum secret-key rates of 7.57 kbps and 7.43 kbps were achieved.

Finally, the secret-key rate versus distance (link length) for the above-mentioned QKD networks/links deployed in various metropolitan areas is briefly summarized in Fig. 14. The distance (link length) is not representative of the fiber loss, since the fiber loss is not only affected by the fiber length, but also relies on the fiber type. It can be seen in Fig. 14 that the secret-key rate of QKD networks is typically at the kbps level within ~100 km of realistic metropolitan areas at the time of writing. Furthermore, it is anticipated that metropolitan QKD would evolve towards high-speed, long-distance, low-cost and multi-protocol networking.

D. Long-Haul QKD Networks

With the advent of trusted relays, long-haul QKD networks have been implemented in practice, which tend to rely on backbone/core networks. The basic features of long-haul QKD networks demonstrated in different locations across the globe are summarized in Table IX and described as follows.

1) Hefei-Chaohu-Wuhu QKD Network: Wang *et al.* [180]

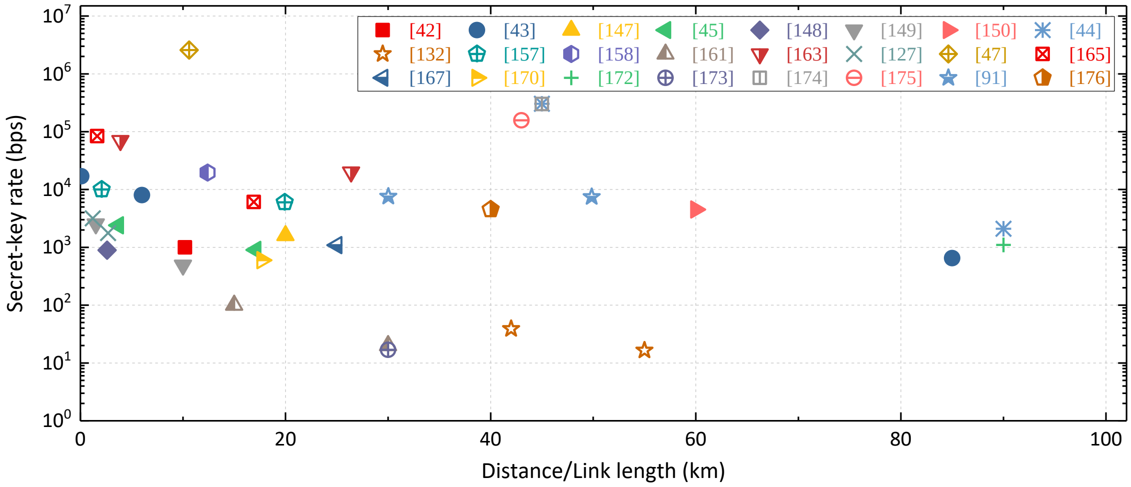


Fig. 14. Secret-key rate versus distance (link length) for different QKD networks/links deployed in various metropolitan areas.

TABLE IX
SUMMARY OF THE BASIC FEATURES OF LONG-HAUL QKD NETWORKS DEMONSTRATED IN DIFFERENT LOCATIONS

Long-haul network	**Trusted relay**	**Number of nodes**	**Number of links**	**Link type**	**Link span**	**QKD type**	**Year**	**Reference**	**Remark**
Hefei-Chaohu-Wuhu	✓	9	8	Optical fiber	199 km	DV	2011	[180]	Long-term demonstration
Beijing-Shanghai	✓	32	31	Optical fiber	2,000 km	DV	2017	[46], [181]	Ultra-long QKD network Real-world applications
Zhucheng-Huangshan	×	2	1	Optical fiber	66 km	DV	2018	[182]	QKD integration with a commercial backbone network
Wuhan-Hefei	✓	11	10	Optical fiber	609 km	DV	2018	[183]	Real-world applications
China-Austria	✓	3	2	Free space	7,600 km	DV	2018	[48]	First satellite-relayed intercontinental QKD network
Cambridge-Ipswich	✓	5	4	Optical fiber	121 km	DV	2019	[128]	Co-fiber transmission of quantum and classical traffic
Integrated Space-to-Ground (China)	✓	Multiple	>702	Optical fiber Free space	4,600 km	DV	2021	[49]	Large-scale integrated space-to-ground QKD network
Jinan-Qingdao	×	3	2	Optical fiber	511 km	DV	2021	[184]	Field deployment of TF-QKD

reported on the deployment of the Hefei-Chaohu-Wuhu QKD network across these three cities in China. This wide area network was operational from December 2011 to July 2012, which contained nine nodes connecting two metropolitan QKD networks in Hefei and Wuhu cities with the total fiber length of 199 km. The decoy-state BB84 protocol was implemented for QKD. The applications of OTP-encrypted public switch telephone conversations and AES-encrypted virtual private network (VPN) functions were demonstrated over this network.

2) *Beijing-Shanghai QKD Network:* This QKD network [46], [181] is a trusted relay based backbone network, which is illustrated in Fig. 15. This network consists of 32 nodes connected by 31 fiber links, which connects four QKD metropolitan networks in the cities of Beijing, Jinan, Hefei, and Shanghai with its total length exceeding 2,000 km. The deployment of this network was initiated in June 2013 and it was completed in December 2016. After long-term performance tests and evaluation, this network has been in operation since August 2017. Numerous real-world applications in the fields of finance and government have been secured by using this network.

3) *China-Austria QKD Network:* In 2018, Liao *et al.* [48] reported on the experimental demonstration of a satellite-based intercontinental QKD network. As shown in Fig. 16, this network used the Micius satellite [75] as a trusted relay connecting the ground station in Xinglong, China and that in Graz, Austria spanning a total distance of 7,600 km. Again, the decoy-state BB84 protocol was utilized in the QKD system. Specifically, this network was combined with metropolitan QKD networks to support an AES-encrypted intercontinental video conference. The demonstration of this network clearly indicates the feasibility of a global QKD network. In this paper, a detailed overview of satellite-based QKD will be provided in Section V-C.

4) *Cambridge-Ipswich QKD Network:* In 2019, a trusted relay based QKD backbone network was launched between

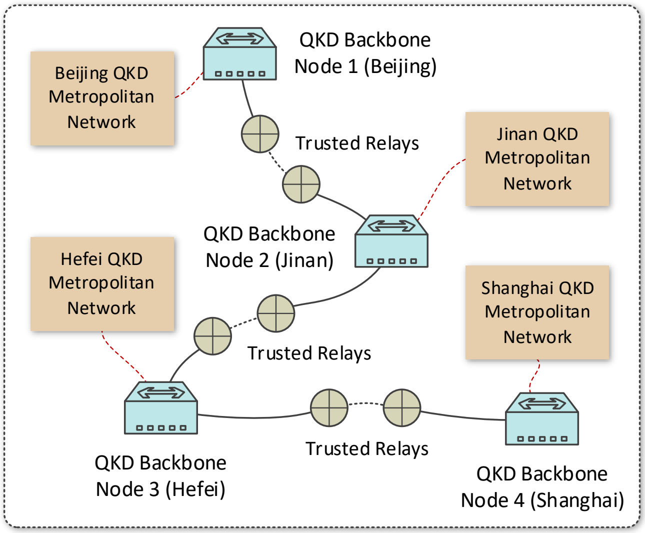

Beijing QKD Metropolitan Network
QKD Backbone Node 1 (Beijing)
Trusted Relays
Jinan QKD Metropolitan Network
QKD Backbone Node 2 (Jinan)
Hefei QKD Metropolitan Network
Shanghai QKD Metropolitan Network
Trusted Relays
Trusted Relays
QKD Backbone Node 3 (Hefei)
QKD Backbone Node 4 (Shanghai)

Fig. 15. Illustration of the Beijing-Shanghai QKD backbone network [46].

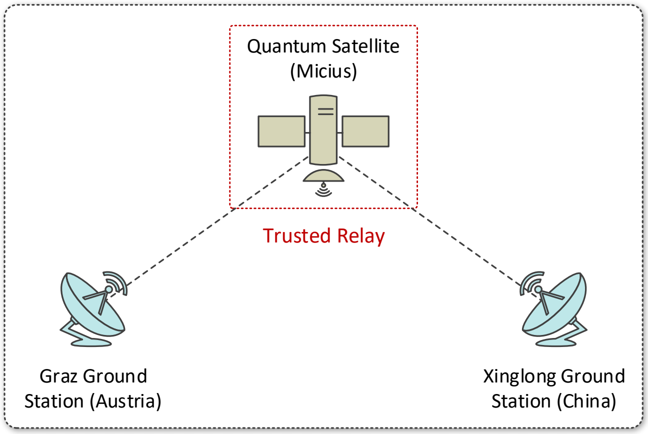

Quantum Satellite (Micius)
Trusted Relay
Graz Ground Station (Austria)
Xinglong Ground Station (China)

Fig. 16. Illustration of the satellite-based intercontinental QKD network between China and Austria [48].

Cambridge and Ipswich, UK [128], which is composed of five nodes and four links, where the quantum and classical signals are transmitted over the same fiber with the total length of 121 km.

5) Integrated Space-to-Ground QKD Network: In 2021, Chen *et al.* [49] reported on the construction of an integrated space-to-ground QKD network in China, covering more than 700 QKD fiber links and two satellite-to-ground free-space links. This network contains the Beijing-Shanghai QKD network, four metropolitan QKD networks deployed in Beijing, Jinan, Hefei and Shanghai, as well as two satellite-ground QKD links connecting the ground stations in Xinglong and Nanshan. Long-term stability and security tests of this network have been carried out, where its applications in diverse fields such as governments, finance and energy have been demonstrated.

6) Nationwide QKD Network Construction Initiatives: Nationwide QKD networks are currently being deployed or planned in many countries. In China, five-horizontal and six-vertical QKD trunk lines were planned to be constructed during 2017 to 2025, along with more quantum communication satellites to be launched to constitute a global satellite-based QKD network [181], [185]. In the USA, a QKD backbone network is being deployed relying on 800 km optical fiber spanning from Boston to Washington, DC [186], while a nationwide QKD network was planned to stretch from Boston to Georgia, and eventually reaching California [187]. In the UK, a QKD network spanning Cambridge-London-Bristol was planned and has been tested in the laboratory [188], [189]. In Europe, a quantum communication infrastructure based on integrated terrestrial-satellite QKD networks launched by the OpenQKD project [190] is being explored for employment across the European Union. In Russia, a 7,000-km quantum network has been scheduled to be constructed by 2024, with one of the first pilot projects exploring a QKD backbone network connecting Moscow and St. Petersburg with a total length of 700 km [191], [192]. In South Korea, the different phases of building a nationwide QKD network have been discussed in [193]. In Japan, a large-scale network that can accommodate over 100 quantum cryptographic devices and 10,000 users is projected to be developed by 2024 [194], [195]. Moreover, a number of satellite-based quantum initiatives [196] have been announced around the world. In June 2021, seven countries, including UK, USA, Japan, Canada, Italy, Belgium and Austria, announced their collaborations for developing a satellite-based quantum encryption network [197].

IV. QKD Networking Architecture

Let us now continue by surveying the QKD network architectures, elements, as well as interfaces and protocols. Given that the untrusted relay and quantum repeater based QKD networks are still immature for practical use, the focus of this section is on networks based on optical switching and

TABLE X
Summary of Beneficial Layered Network Architectures Supporting QKD

Architecture	Feature (from bottom to top layers)	Manner	Year	Ref.	Remark
Three-layer architecture	Quantum layer, Secret's layer, Data layer	Field trial	2008	[43]	SECOQC QKD network
	Quantum layer, Key management layer, Application layer	Field trial	2009	[45]	SwissQuantum QKD network
	Quantum layer, Key management layer, Communication layer	Field trial	2010	[44]	Tokyo QKD network
	Quantum layer, Key management layer, Application layer	Field trial	2010	[170]	Paris QKD link
	Physical layer, Quantum key management layer, Application layer	Experiment	2013	[198]	Network-centric quantum communication
	Infrastructure layer, Control and management layer, Application layer	Theory	2016	[199]	Quantum-aware SDN
	Quantum layer, Network key delivery layer, Application layer	Field trial	2019	[47]	Cambridge QKD network
	QKD layer, Control layer, Application layer	Theory	2019	[200]	SDN-based QKD network
	Infrastructure layer, Control layer, Application layer	Experiment	2019	[201]	SDN-based QKD network
	QKD layer, Control layer, Application layer	Experiment	2019	[202]	SDN-based QKD network
Four-layer architecture	Data layer, Key generation layer, Connection layer, Key management layer	Experiment	2009	[203]	QKD integrated optical network
	Optical layer, QKD layer, Control layer, Application layer	Theory	2017	[204]	QKD integrated optical network
	Data layer, QKD layer, Control layer, Application layer	Theory	2017	[205]	QKD integrated optical network
	Quantum layer, Key management layer, Key supply layer, Application layer	Experiment	2017	[206]	QKD network
	Data layer, QKD layer, Control layer, Application layer	Theory	2018	[207]	QKD integrated optical network
	Optical layer, QKD layer, Control layer, Application layer	Theory	2019	[208]	QKD integrated optical network
Five-layer architecture	Quantum physical layer, Quantum logical layer, Classical physical layer, Classical logical layer, Application layer	Field trial	2021	[49]	Integrated space-to-ground QKD network
Six-layer architecture	Quantum layer, Key management layer, QKD network control layer, QKD network management layer, Service layer, User network management layer	Recommendation	2019	[65]	QKD network and user network

trusted relaying techniques.

A. *General Architecture of QKD Networks*

A QKD network is inseparable from the classical network, since it also requires an authenticated classical network (e.g., an optical network) and multiple secure cryptographic applications in a classical network. As seen in Section III, QKD networks have now found preliminary applications in the existing communication and secure infrastructures. Furthermore, beneficial layered network architectures supporting QKD have also been proposed, which are summarized in Table X. The proposed architectures have different number of layers depending on their specific definitions and applications, such as the three-layer architecture of [43]–[45], [47], [170], [198]–[202], the four-layer architecture of [203]–[208], the five-layer architecture of [49] and the six-layer architecture of [65].

To elaborate a little further, the conceptual structures of a QKD network and a user network have been illustrated in the ITU-T Y.3800 recommendation [65]. Given the diversity of the proposed network architectures supporting QKD, we illustrate a general three-layer architecture of QKD networks from a holistic view based on the six-layer network architecture illustrated in [65]. As depicted in Fig. 17, this architecture consists of three logical layers: 1) the infrastructure layer; 2) the control and management layer; 3) the application layer. The three logical layers of this architecture are detailed next, along with the QKD network elements and devices as well as interfaces depicted in Fig. 17.

1) Infrastructure Layer: This layer of Fig. 17 is constituted by the QKD network infrastructure, which consists of various physical devices [65] conceived for QKD networking. The physical devices found in the same location are installed in a secure and reliable node for protecting them against physical attacks. Such a node is referred to as a QKD node. Based on the diverse QKD network implementation options described in Section III-A, the specific physical devices can be different, as it will be detailed in the next sub-section. The pairs of QKD nodes may be interconnected either by optical fiber or by free-space links, where each pair of QKD nodes can generate symmetric random bit strings as secret keys. Hence the QKD protocols or physical devices developed independently by different vendors may be adopted [43], [44]. The secret keys generated will then be readily stored in the QKD nodes [65], since the secret keys are composed of classical bit strings. Each QKD node holds its detailed secret-key parameters, such as the so-called identifier, size, rate, and type of secret keys, as well as the physical device identifier and time stamp of generating and storing secret keys [206]. Each QKD node also stores the link parameters, such as the length and type of links, and the error rate of quantum channels.

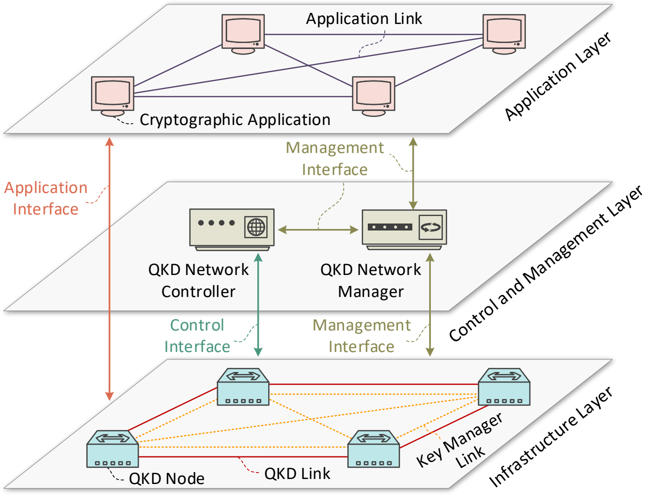


Fig. 17. General architecture of QKD networks.

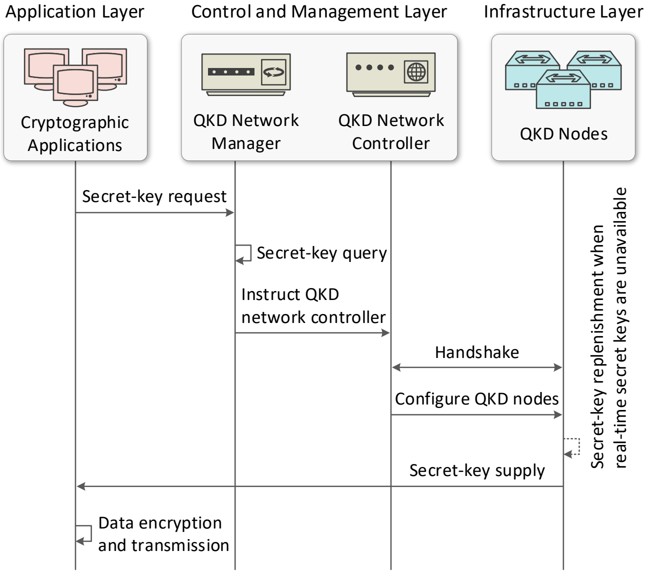

Application Layer
Control and Management Layer
Infrastructure Layer
Cryptographic Applications
QKD Network Manager
QKD Network Controller
QKD Nodes
Secret-key request
Secret-key query
Instruct QKD network controller
Handshake
Configure QKD nodes
Secret-key supply
Secret-key replenishment when real-time secret keys are unavailable
Data encryption and transmission

Fig. 18. Illustration of a simple workflow of service provision for cryptographic applications.

2) Control and Management Layer: This layer of Fig. 17 is constituted by the QKD network controller and manager [65], where all the QKD nodes are controlled by the QKD network controller, which activates, de-activates, and calibrates the QKD nodes. By contrast, the QKD network manager monitors and manages the QKD network as a whole. It monitors the status of all the QKD nodes and links (e.g., obtaining the real-time secret-key parameters and link parameters from the QKD nodes), and supervises the QKD network controller. The statistical data obtained through monitoring and management can be collected at a certain relative frequency, and then be registered and updated in a database. In particular, the real secret keys stored in the QKD nodes will not be delivered across different physical locations and cannot be accessed by the QKD network controller or manager [200], [201], thereby the security of secret keys is still guaranteed after the addition of the control and management layer.

3) Application Layer: This layer of Fig. 17 is constituted by the cryptographic applications required by the users. The simple workflow of service provision for cryptographic applications in a QKD network is illustrated in Fig. 18. First, cryptographic applications inform the QKD network manager of their security requests, such as secret-key request, including the secret-key size, rate, updating period, and so on. According to these requests, the QKD network manager queries the availability of secret keys required from the corresponding QKD nodes. If the real-time secret keys are available for supporting the cryptographic applications, the QKD network manager instructs the QKD network controller to notify the corresponding QKD nodes to supply secret keys for the cryptographic applications in an appropriate format. Otherwise, the cryptographic applications should wait for secret-key replenishment. Finally, the transmission of data over the application link can be encrypted using the secret keys. In particular, each cryptographic application uses the secret keys at its own responsibility, once the secret keys have been supplied to it, while the QKD nodes and QKD network manager have no responsibility concerning those secret keys afterward. The number of users that each QKD network/system can accommodate is determined by the available secret-key resources in the QKD network/system and the secret-key requirements of the users. Hence, there is a trade-off between the secret-key resources and user requirements. As an example, the Cambridge QKD metro network [47] with 2.5 Mbps of secret-key resources on each QKD link can support tens of thousands of users with a secret-key requirement of >1 kbps per user.

B. *QKD Network Elements*

Based on the general architecture of QKD networks shown in Fig. 17, the associated QKD network elements are elaborated on next.

1) QKD Node: In a heterogeneous QKD network constituted by diverse network segments of different sizes, the QKD nodes may be classified as backbone node and access node [144], [146], [149], [156], [180]. By contrast, for a QKD network based on trusted relays or untrusted relays, the QKD nodes may be constituted by user nodes and relay nodes [132], [150], [201]. Each QKD node of Fig. 17 consists of various physical devices, depending on the specific networking requirements. As illustrated in Fig. 19, some of the pivotal physical devices are described as follows.

- *QKD transmitter/receiver (transceiver):* A pair of QKD devices such as a transmitter and a receiver can generate the local secret keys, which are forwarded to their respectively connected key managers [65]. Some of the QKD transceivers commercially available on the market at the time of writing are mentioned in [38]–[40]. Generally, a QKD node contains one or more QKD transceivers.
- *Key manager:* The key manager is a distributed server used for managing the secret keys generated by QKD transceivers and for providing the secret keys to cryptographic applications [44], [45], [65], [209]. A QKD node usually contains a single key manager, which is connected to all QKD transceivers in the same QKD node, and receives as well as stores secret keys generated by the QKD transceivers. It can perform secret-key relaying to enable the generation of global secret keys between any pair of QKD nodes in an end-to-end manner, and it is capable of supplying secret keys for diverse cryptographic applications. The key manager looks after the secret keys from the instant of their generation by QKD transceivers to their employment by cryptographic applications.
- *Optical switch:* The optical switch is a device facilitating the connection of a quantum channel from a transmitter to any receiver or from a receiver to any transmitter within a limited distance. It can realize the time-division multiplexing (TDM) of quantum channels and the time-sharing of QKD devices [131], [139], [140], [210], as well as facilitate the node bypass [211]. Naturally, the frequency band of an optical switch has to cover the entire frequency band of quantum channels.
- *Multiplexer/demultiplexer:* The multiplexer/demultiplexer is used for bundling and separating multiple channels such as quantum and classical channels. There are multiple types of multiplexers/demultiplexers for different multiplexing techniques such as WDM and TDM. Additionally, M wavelength-division multiplexers can be used to form an M-port QKD router [143], [177].
- *Secure infrastructure:* The secure infrastructure is utilized for providing effective safeguards for QKD nodes to guarantee that they can operate reliably.

2) QKD Link: The QKD link of Fig. 17 is used for connecting a transmitter and receiver pair, which usually consists of a quantum channel for quantum state transmission, and a classical channel for synchronization and key distillation [65], [66]. The quantum and classical channels do not have to be physically bundled. The QKD link can be implemented over optical fiber or as a free space optical link.

3) Key Manager Link: The key manager link of Fig. 17 involves a classical channel connecting several key managers to perform secret-key management such as secret-key relaying, which can be implemented either over optical fiber or free space.

4) QKD Network Controller: The QKD network controller of Fig. 17 is generally a centralized server used for orchestrating the operation of all the QKD nodes in a QKD network infrastructure, which includes the activation, de-activation, and calibration of the QKD nodes. It performs

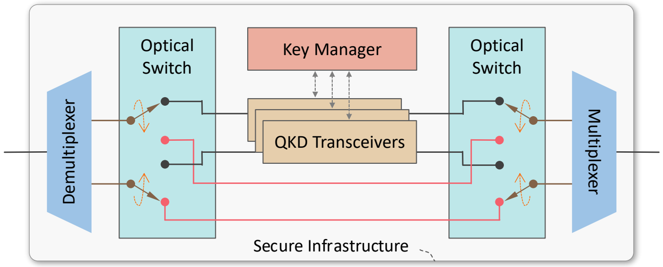


Fig. 19. Illustration of a QKD node structure.

several network control functions, such as QKD connection control (including node access control and node authentication), routing control (including routing for secret-key relaying and rerouting for failure recovery), and QoS control (including QoS-differentiated customization and end-to-end QoS assurance) [212].

5) QKD Network Manager: The QKD network manager seen in Fig. 17 is a centralized server used for monitoring and managing the QKD network, including all the QKD nodes and QKD links as well as key manager links, which also supervises the QKD network controller. It performs fault, configuration, accounting, performance and security management of the QKD network. The QKD network manager differs from the QKD network controller mainly in that it performs typical network management functions and instructs the QKD network controller based on the secret-key requests received. This is arranged without directly providing specific control policies and functions, such that diverse network environments and requirements cannot be seamlessly accommodated by a separate QKD network manager.

6) Cryptographic Application: The cryptographic application seen at the top layer of Fig. 17 is a user that has a specific security request, such as secret-key request (including secret-key size, rate, and updating period). A cryptographic application usually has to be in the same physical location as a QKD node to receive the secret keys.

7) Application Link: The application link seen at the top layer of Fig. 17 is a classical channel used for exchanging the encrypted data between two cryptographic applications.

C. *QKD Network Interfaces and Protocols*

As shown in Fig. 17, there are several interfaces (including management, control, and application interfaces) connecting the different layers in the general architecture of QKD networks. Here we describe the QKD network interfaces and discuss several typical protocols supporting these interfaces. The internal interfaces within each QKD network element or device are beyond the scope of this paper, some of which can be found in [213]. Table XI briefly summarizes the QKD network interfaces and protocols. Given the wide diversity of QKD network protocols, they do not necessarily comply with those discussed below.

TABLE XI
SUMMARY OF QKD NETWORK INTERFACES AND PROTOCOLS

Interface	**Location**	**Protocol**	**Use case**
Management interface	Between QKD network manager and QKD nodes	SNMP, CORBA	[38], [39]
	Between QKD network manager and controller		
	Between QKD network manager and applications		
Control interface	Between QKD network controller and QKD nodes	OpenFlow, NETCONF	[201], [202]
Application interface	Between QKD nodes and applications	REST API (HTTPS, JSON)	[47], [222]

1) Management Interface and Protocol: The management interfaces of Fig. 17 in a QKD network involve those related to the QKD nodes, to the QKD network controller, and to the cryptographic applications. By using the management interface conceived for QKD nodes, the QKD network manager communicates with all QKD nodes in the infrastructure layer. The QKD nodes can report their detailed information to the QKD network manager, which involves all the relevant information concerning the status of devices, boards, ports, modules, software, resources, links, and so on. Furthermore, the QKD network manager may request information related to the secret keys, to the relaying process, and to the routing from the QKD nodes. By using the management interface dedicated to the QKD network controller, the QKD network manager supervises the QKD network controller. By employing the management interface provided for cryptographic applications, the QKD network manager communicates with the associated cryptographic applications in the application layer, which can collect multiple security requests from the cryptographic applications.

A management interface can be implemented by the simple network management protocol (SNMP) of [214], [215], which has been widely used for network management as well as monitoring, and can be used for collecting information about the managed network elements and devices of a QKD network. For example, the information concerning the devices, boards, ports, modules, software, resources, and links from QKD nodes as well as the information related to multiple security requests arriving from cryptographic applications can be collected via the SNMP. The reporting of alarms and notification of events as well as any queries concerning secret-key information can also be implemented using the SNMP. Furthermore, in order to support the interoperability of the QKD network elements and devices developed by different companies, the common object request broker architecture (CORBA) of [216] can be utilized for harmonizing the heterogeneous network elements and devices of a multi-vendor or multi-domain QKD network. The SNMP and CORBA have been utilized in commercial systems for QKD networking [38], [39].

2) Control Interface and Protocol: The QKD network controller communicates with all QKD nodes in the infrastructure layer via the control interface of Fig. 17. By using this interface, the QKD network controller exchanges control and configuration messages with the QKD nodes in order to implement several control functions, such as QKD connection control, routing control, and QoS control.

The SDN controller may serve as the QKD network controller, as it has been demonstrated in practical QKD networks [126], [127], [163]. In particular, the QKD control interface provided via SDN is specified in the ETSI GS QKD 015 [217] and the recommendation ITU-T Y.3805 [218]. The OpenFlow of [219] and NETCONF of [220] constitute a pair of protocols that can implement the control interface provided for a SDN controller. The control and configuration request/response messages can be transmitted by using these two protocols. OpenFlow can define a protocol through which a SDN-enabled QKD network controller can control the OpenFlow-enabled QKD nodes [201], [202]. The NETCONF protocol is a transaction-based entity and its data encoding usually relies on the Extensible Markup Language, which provides mechanisms for installing, manipulating, and deleting the configuration of QKD nodes. A detailed overview of SDN designed for QKD networks is provided in Section VI-A.

3) Application Interface and Protocol: The application interface of Fig. 17 in a QKD network is between the infrastructure layer and the application layer. The local key manager in a QKD node communicates with the local cryptographic applications via the application interface. The secret keys are delivered from the local key manager to the local cryptographic applications by using this interface. Moreover, the application interface has been specified in the group specification ETSI GS QKD 004 [221].

The application interface is used for secret-key delivery, which can be implemented by the Representational State Transfer (REST) application programming interface (API). The REST API can use the HyperText Transfer Protocol Secure (HTTPS) version and the JavaScript Object Notation (JSON) data format for delivering secret keys to cryptographic applications. The REST API is regarded as a simple, lightweight, and widely used technique in many application domains, which has been adopted in the Cambridge QKD network [47]. Recently, the REST API specification formulated for secret-key delivery in a QKD network has been described in the group specification ETSI GS QKD 014 [222].

V. Enabling Techniques in the Physical Layer for QKD Networks

In recent years, sophisticated technologies have been developed for supporting the QKD network infrastructure at a moderate cost, while aiming for wide coverage and high robustness. In this section, we conduct an in-depth survey of the enabling technologies in the physical layer domain, covering the techniques of co-fiber transmission, relaying, satellite-based QKD and chip-based QKD.

A. Co-Fiber Transmission

The co-fiber transmission terminology is introduced as a compact expression to indicate that the QKD and classical channels are travelling on the same fiber. The pivotal challenge of co-fiber transmission arises from the extreme contrast in the intensities of quantum and classical signals, since each quantum signal typically contains less than one photon per pulse on average, while a classical pulse may contain 10^6 photons or more for a Gb/s link. Another challenge is that the nonlinear noise generated by impairments such as Raman scattering and four-wave mixing (FWM) will cause severe contamination of the quantum signals.

In order to protect the vulnerable quantum signals from the deleterious impact of high-power classical signals, many practical QKD networks have been rolled out by relying on dark fibers. Nevertheless, given the difficulty of installing new fibers and the shortage of dark fiber resources in existing optical networks, the dark fiber has become a scarce and costly resource that may no longer be available for the widespread deployment of QKD networks. Hence the option of rolling out the QKD network infrastructure by sharing the established fiber infrastructure has attracted much attention, paving the way for the coexistence of quantum signals with classical signals in the same fiber. In 1997, Townsend [223] reported the first co-fiber transmission experiment by using the WDM technique for multiplexing the quantum and classical channels in a SMF, which provided a blueprint for the co-fiber transmission investigations that followed. Hence, a variety of theoretical, experimental, and in-field studies using the WDM technique for supporting the coexistence of quantum and classical signals in the same fiber have been reported [224]–[261]. Moreover, several new multiplexing techniques have been conceived for co-fiber transmission [262]–[281]. In the following paragraphs, we review the research efforts dedicated to the co-fiber transmission of quantum and classical signals from the perspective of WDM theories, WDM experiments, WDM field trials, and new multiplexing techniques.

1) Theoretical WDM Investigation: WDM is one of the most widely used techniques in commercial optical networks, which is beneficial for increasing the throughput of optical fibers used in the transmission line. Hence, it is natural to combine QKD transmissions with the existing optical networks using the WDM technique, which can accelerate the commercialization of QKD networks. A schematic diagram of multiplexing quantum and classical (data) channels in a SMF using WDM is shown in Fig. 20. The quantum channel is launched into a SMF accompanied by classical channels such as the classical channel used both for QKD and for high-speed data channels. Inevitably, various physical-layer impairments are inflicted during co-fiber transmission, such as Raman scattering, FWM, and amplified spontaneous emission (ASE) [224]. The performance of the quantum channel and the QKD system may be severely deteriorated by these impairments.

The potential impact and their mitigation strategies suitable for various physical-layer impairments imposed by classical channels on the performance of QKD have been theoretically analyzed in [225]–[228]. Specifically, the effects of Raman noise, and of spontaneous Raman scattering inflicted by a classical channel on a quantum channel have been

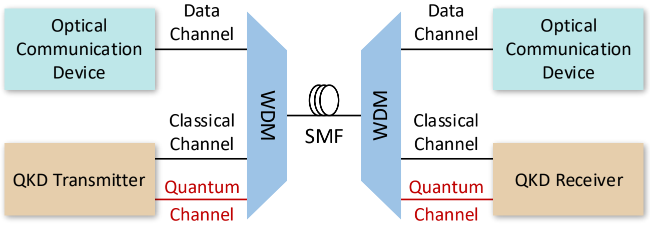


Fig. 20. Illustration of multiplexing quantum and classical (data) channels in a SMF using WDM.

quantitatively evaluated in [229]. On a similar note, the impact of spontaneous Raman scattering on a quantum channel coexisting with multiple classical channels in a SMF has been analyzed in [230]. To overcome the limitations engendered by Raman noise, Fröhlich *et al.* [231] designed a dual feeder architecture for integrating multi-user QKD transmissions into a Gigabit passive optical network (GPON). To reduce the FWM noise, Sun *et al.* [232] developed a user-specific channel-interleaving aided WDM approach combined with unequal frequency spacing. For jointly suppressing the Raman noise and FWM noise, Niu *et al.* [233] proposed an optimized channel allocation scheme, allowing QKD to tolerate the presence of high-power classical signals conveying many classical channels within a SMF. Based on WDM, a prototype of the quantum metropolitan optical network [156] has been described and characterized, allowing the deployment of a technologically realistic and cost-effective QKD network over commercial telecommunication networks.

2) WDM System Experiment: Both the C-band (1530–1565 nm) and O-band (1260–1360 nm) within a SMF can be used for the joint transmission of quantum and classical signals. Hence, different WDM layouts can be considered for quantum and classical channels within a SMF for their co-fiber transmission. Table XII summarizes the system experiments dedicated to the co-fiber transmission of quantum and classical channels using WDM, which are detailed in the following paragraphs according to their different WDM layouts.

By choosing the O-band as the quantum band and C-band as the classical band, the sufficient isolation of the quantum and classical channels can be ensured. In his seminal work, Townsend [223] first used WDM to multiplex a quantum channel accommodated at 1300 nm with a 1.2 Gb/s data channel near 1550 nm over a 28 km length of installed fiber. Toliver *et al.* [234] demonstrated the coexistence of 1310 nm quantum signals with amplified DWDM signals over a 10 km SMF. In [235], the minimum required wavelength difference between a quantum channel at 1310 nm and a classical channel near 1550 nm over a 10 km fiber link was experimentally analyzed. Runser *et al.* [236] presented an experimental demonstration of the co-fiber transmission of quantum signals at 1310 nm and classical signals around 1550 nm over a 25 km SMF. In [237], an erbium doped fiber amplifier (EDFA) bypass

TABLE XII
SUMMARY OF SYSTEM EXPERIMENTS FOR CO-FIBER TRANSMISSION OF QUANTUM AND CLASSICAL CHANNELS USING WDM

Quantum band (wavelength)	**Classical band**	**Number of classical channels**	**Classical signal launch power**	**Multiplexed data bandwidth**	**Achievable distance**	**Maximum secret-key rate**	**QKD type**	**Year**	**Reference**
O-band (1300 nm)	C-band	1	Tunable	1.2 Gbps	28 km	N/A	DV	1997	[223]
O-band (1310 nm)	C-band	4	Tunable	N/A	10 km	100 bps	DV	2004	[234]
O-band (1310 nm)	C-band	1	6 dBm	N/A	10 km	70 bps	DV	2005	[235]
O-band (1310 nm)	C-band	4	Tunable	17.5 Gbps	25 km	9 bps	DV	2005	[236]
O-band (1310 nm)	C-band	4	–21 dBm	40 Gbps	15 km	8 bps	DV	2006	[237]
C-band (1549.3 nm)	C-band	4	–2 dBm	10 Gbps	50 km	N/A	DV	2006	[240]
O-band (1310 nm)	C-band	4	Tunable	N/A	10 km	100 bps	DV	2009	[168]
C-band (1549.32 nm)	C-band	2	–5 dBm	N/A	25 km	6 bps	DV	2009	[241]
C-band (1551.72 nm)	C-band	4	Tunable	1 Gbps	50 km	11 bps	DV	2010	[242]
C-band (1550 nm)	L-band	3	Tunable	1.25 Gbps	90 km	7.6 kbps	DV	2012	[253]
C-band (1548.52 nm)	C-band	2	Tunable	20 Gbps	70 km	52 kbps	DV	2014	[244]
C-band (1531.12 nm)	C-band	1	−3 dBm	N/A	75 km	490 bps	CV	2015	[245]
C-band (1550 nm)	L-band	3	Tunable	1.25 Gbps	25 km	1 Mbps	CV	2015	[254]
C-band (1550.12 nm)	O- and C-band	2	−5 dBm	100 Mbps	45 km	4 kbps	DV	2015	[255]
C-band (1547.72 nm)	C-band	2	Tunable	200 Gbps	101 km	10 kbps	DV	2016	[69]
O-band (1310 nm)	C-band	32	10 dBm	7.168 Tbps	80 km	1 kbps	DV	2017	[239]
C-band (1548.51 nm)	C-band	1	−5 dBm	100 Gbps	150 km	1 kbps	DV	2017	[87]
C-band (1550 nm)	C-band	20	18 dBm	560 Gbps	5 km	N/A	CV	2017	[246]
C-band (1549.2 nm)	C-band	7	4 dBm	87.5 Gbps	10 km	50 kbps	CV	2018	[247]
C-band (1549.6 nm)	C-band	18	14 dBm	3.5 Tbps	10 km	75 kbps	CV	2018	[248]
C-band (1550 nm)	C-band	10	3 dBm	100 Gbps	20 km	90 kbps	CV	2018	[249]
C-band (1549.5 nm)	C-band	100	12.9 dBm	18.3 Tbps	10 km	28.9 kbps	CV	2019	[250]
S-band (1504.98 nm)	C-band	56	13.6 dBm	5.6 Tbps	25 km	N/A	CV	2019	[256]
C-band (1532.68 nm)	C-band	5	−14 dBm	50 Gbps	40 km	N/A	DV	2019	[251]
C-band (1550 nm)	C-band	1	6 dBm	N/A	13 km	300 kbps	CV	2020	[103]
C-band (1531.9 nm)	C-band	11	15.6 dBm	N/A	13.2 km	12 Mbps	CV	2020	[252]

and filtering architecture was proposed, allowing a quantum channel at 1310 nm to coexist with four classical channels operating around 1550 nm and amplified in mid-span over a 15 km fiber link. Chapuran *et al.* [168] experimentally characterized the coexistence of a quantum channel at 1310 nm and four classical data channels near 1550 nm in the same fiber, where the impact of Raman noise on the quantum signals was measured. Aleksic *et al.* [238] experimentally characterized the feasibility of QKD integration into metropolitan area networks, where the effect of Raman noise was analyzed. Furthermore, amplifier and node bypass solutions were also presented. In [239], the co-propagation of quantum signals and Terabit classical signals over a distance of 80 km was realized in an experiment, where a quantum channel was supported at 1310 nm and 32 classical data channels were conveyed within the C-band.

The lower attenuation and the resultant excellent transmission performance of the C-band is eminently suitable for conveying both the vulnerable quantum and the more robust classical signals. Xia *et al.* [240] conducted an experiment by multiplexing a quantum channel accommodated at 1549.3 nm and four classical channels in the C-band over a 50 km long optical fiber. Peters *et al.* [241] demonstrated the co-fiber transmission of a 1549.32 nm quantum channel and two classical channels using a reconfigurable optical add drop multiplexer (ROADM), where the impact of spontaneous Raman scattering and FWM on the quantum signals were measured and analyzed. Eraerds *et al.* [242] performed an experiment relying on multiplexing four classical channels with a quantum channel over a single fiber of 50 km length, in which both the quantum and classical channels were accommodated in the C-band. In [243], an experiment of simultaneous QKD transmission and bidirectional 10 Gb/s classical transmission was described within a single fiber, where a dual feeder fiber technique and a filtering scheme were used for reducing the Raman noise. In [244], the coexistence of QKD with bidirectional 10 Gb/s classical data signals was demonstrated within the same fiber, achieving secret-key rates of 2.38 Mbps over a 35 km fiber link and of 52 kbps over a 70 km fiber link. Kumar *et al.* [245] conducted several experimental tests for characterizing the coexistence of CV-QKD with a classical channel in the same fiber, where a secret-key rate of 490 bps was achieved over a 75 km fiber. Dynes *et al.* [69] experimentally multiplexed a quantum channel accommodated at 1547.72 nm along with two 100 Gb/s classical data channels around 1530 nm over a 101 km fiber link. Fröhlich *et al.* [87] demonstrated the coexistence of quantum signals at 1548.51 nm with 100 Gb/s data signals within the C-band in a 150 km optical fiber. In [246], the coexistence of a quantum channel hosted at 1550 nm along with 20 classical channels (including 4×100 Gb/s and 16×10 Gb/s) in the C-band of a SMF was experimentally investigated. In [247], the co-propagation of a quantum channel centred at 1549.2 nm and seven 12.5 Gb/s classical channels hosted in the C-band over a 10 km single fiber was investigated, achieving a secret-key rate in the range of 20 to 50 kbps. In [248], the coexistence of CV-QKD and 3.5 Tbps classical channels was demonstrated in a 10 km SMF, where the influence of in-band ASE noise on CV-QKD was analyzed. Karinou *et al.* [249] experimentally realized the co-fiber transmission of a quantum channel and 10 classical channels within the C-band, supporting a secret-key rate of 90 kbps over a 20-km fiber link in a CV-QKD system. Eriksson *et al.* [250] demonstrated the joint propagation of a quantum channel located at 1549.5 nm and 100 classical data channels associated with an aggregate transmission rate of 18.3 Tb/s in the C-band, achieving a secret-key rate of 28.9 kbps over a 10 km SMF. Valivarthi *et al.* [251] characterized the simultaneous operation of MDI-QKD with five 10 Gb/s bidirectional classical channels in the vicinity of the 1550 nm wavelength over the same fiber of 40 km length. In [103], the coexistence of a CV-QKD system with a classical channel operating in the C-band was demonstrated, and a secret-key rate of 300 kbps was attained for a link length of 13 km. In [252], the co-propagation of a quantum channel accommodated at 1531.9 nm and 11 classical DWDM channels conveyed within the C-band was accomplished over a 13.2 km fiber link, while supporting a secret-key rate of 12 Mbps.

In addition to the aforementioned pair of typical WDM layouts, some studies have also considered other WDM layouts for the co-fiber transmission of quantum and classical channels. In [253], the coexistence of quantum signals at 1550 nm and Gigabit classical data signals within the L-band (1565–1625

TABLE XIII
SUMMARY OF FIELD TRIALS FOR CO-FIBER TRANSMISSION OF QUANTUM AND CLASSICAL CHANNELS USING WDM

Quantum band (wavelength)	**Classical band**	**Number of classical channels**	**Classical signal launch power**	**Multiplexed data bandwidth**	**Achievable distance**	**Maximum secret-key rate**	**QKD type**	**Year**	**Reference**
C-band (1550 nm)	L-band	1	−33.3 dBm	N/A	97 km	820 bps	DV	2008	[260]
C-band (1547.72 nm)	C-band	4	–10 dBm	40 Gbps	26 km	160 kbps	DV	2014	[261]
C-band (1550.12 nm)	L-band	3	Tunable	1 Gbps	2.08 km	10 kbps	CV	2016	[157]
O-band (1310 nm)	C-band	20	21 dBm	3.6 Tbps	66 km	5.1 kbps	DV	2018	[182]
C-band (1550 nm)	C-band	2	Tunable	200 Gbps	10.6 km	2.58 Mbps	DV	2019	[47]
C-band (1550 nm)	C-band	17	N/A	N/A	3.9 km	70 kbps	CV	2019	[163]
C-band (1551.7 nm)	C-band	4	Tunable	400 Gbps	1.9 km	1.28 kbps	DV	2019	[127]
O-band (1310 nm)	C-band	5	Tunable	500 Gbps	14.2 km	1.95 kbps	DV	2019	[128]

TABLE XIV
SUMMARY OF SYSTEM EXPERIMENTS FOR CO-FIBER TRANSMISSION OF QUANTUM AND CLASSICAL CHANNELS USING SDM

Fiber type	**Quantum channel location (wavelength)**	**Classical channel location (band)**	**Classical signal launch power**	**Multiplexed data bandwidth**	**Achievable distance**	**Maximum secret-key rate**	**QKD type**	**Year**	**Reference**
7-core MCF	Central core (1547.72 nm)	Outer cores (C-band)	0 dBm	20 Gbps	53 km	605 kbps	DV	2016	[273]
7-core MCF	Central core (1550 nm)	Outer cores (C-band)	Tunable	112 Gbps	2.5 km	N/A	DV	2018	[274]
7-core MCF	Central core (1551.7 nm)	Outer cores (C-band)	Tunable	9.6 Tbps	1 km	191 bps	DV	2018	[275]
19-core MCF	One outer core (1550.35 nm)	Neighboring cores (C-band)	Tunable	N/A	10.1 km	47 Mbps	CV	2019	[276]
7-core MCF	One outer core (1549.32 nm)	Neighboring cores (C-band)	0 dBm	N/A	1 km	10.9 kbps	DV	2019	[277]
37-core MCF	All cores (1550 nm)	All cores (C-band)	N/A	370 Gbps	7.9 km	62.8 Mbps	DV	2019	[278]
7-core MCF	Central core (1551.7 nm)	All cores (C-band)	Tunable	11.2 Tbps	1 km	920 bps	DV	2020	[280]
Weakly-coupled FMF	LP_{01} mode (1550.12 nm)	LP_{02} mode (C-band)	–2.6 dBm	100 Gbps	86 km	1.3 kbps	DV	2020	[281]

nm) over a 90 km fiber link was reported, in which the Raman noise was mitigated by a sophisticated filtering technique. Huang *et al.* [254] multiplexed a quantum channel hosted at 1550 nm along with three classical channels accommodated in the L-band of a 25 km SMF, achieving a secret-key rate of 1 Mbps for a CV-QKD system. Wang *et al.* [255] transmitted quantum signals at 1550.12 nm along with a pair of classical signals near 1310 nm and 1550 nm in a 45 km fiber. In [256], the coexistence of a quantum channel at 1504.98 nm in the S-band (1460–1530 nm) with 56 classical channels located in the C-band in a 25 km SMF was realized. Moreover, multiple quantum channels can be multiplexed onto a single fiber by using the WDM technique in order to achieve high secret-key rates in a QKD system [257]–[259].

3) WDM Field Trials: Several field trials have investigated the coexistence of quantum and classical signals in a field-installed fiber [47], [127], [128], [157], [163], [182], [260], [261]. Table XIII summarizes the field trials studying the co-fiber transmission of quantum and classical channels using WDM. Tanaka *et al.* [260] transmitted quantum signals at 1550 nm coexisting with clock signals in the L-band over a 97-km installed SMF. Choi *et al.* [261] reported on their field trial of simultaneous transmission of a quantum channel multiplexed with four 10 Gb/s classical data channels through a 26 km field-installed fiber. In [157], the field trials of a four-node CV-QKD network were reported on, in which a quantum channel located at 1550.12 nm and three classical channels hosted in the L-band were transmitted through the same fiber. In this CV-QKD network, the maximum secret-key rate has reached 10 kbps on one of the links having a length of 2.08 km. In [182], a field trial of integrating QKD with a commercial optical network conveying 3.6 Tb/s classical data signals in a 66 km commercial fiber was reported, where both the co-direction propagation and opposite-direction propagation of the quantum and classical signals were tested. In a three-node QKD metropolitan network deployed in the field [47], a quantum channel coexisting with 200 Gb/s classical data channels within the C-band was characterized, and the maximum secret-key rate of 2.58 Mbps was achieved on a 10.6 km fiber link. In [163], a field trial of a quantum channel combined with 17 classical channels on a 3.9 km fiber link of a QKD metropolitan network was demonstrated, achieving a secret-key rate of 70 kbps. As a further development, in [127], a field demonstration of a four-node DV-QKD network was reported, where the coexistence of quantum signals with 400 Gb/s classical data signals was accommodated in the C-band over a 1.9 km fiber link. Wonfor *et al.* [128] reported on a field trial of transmitting quantum signals at 1310 nm integrated with 500 Gb/s classical data signals in the C-band in a single fiber, achieving the maximum secret-key rate of 1.95 kbps on a 14.2 km fiber link.

4) New Multiplexing Techniques: In order to optimize the co-fiber transmission performance of quantum and classical signals, several novel multiplexing techniques have also been explored. Some of these investigations have harnessed orthogonal frequency-division multiplexing (OFDM) [262], TDM [137], [263], and other subcarrier multiplexing [264]–[267] techniques into co-fiber transmission, but these still tend to be less mature.

Inspired by the idea of using space-division multiplexing (SDM) for further increasing the throughput of optical networks, SDM has recently attracted much interest also in the context of quantum and classical channels in the same fiber. In contrast to the WDM technique that uses a SMF for signal transmission, SDM techniques usually employ a multi-core fiber (MCF) or a few-mode fiber (FMF). Specifically, a SMF has to rely on multiple wavelengths, whereas the MCF and FMF add the extra resource dimensions of additional cores and modes in a single fiber, respectively. However, MCFs and FMFs suffer from a new physical-layer impairment, namely inter-core and inter-mode crosstalk. With respect to the theoretical investigations on quantum-classical coexistence based on SDM, a system model of integrating QKD into SDM transmission over MCFs and FMFs has been presented in [268], while the theoretical characterization of inter-core spontaneous Raman scattering on QKD in MCFs has been established in [269]. Additionally, Xavier *et al.* [270] provided an overview of quantum information processing in the context of SDM optical fibers. As a further advance, the theoretical models for characterizing the Raman noise and FWM noise impacts of classical signals on QKD transmissions over MCFs have been proposed in [271], [272].

In recent years, an increased number of system-level experiments has been performed for characterizing the co-fiber transmission of quantum and classical channels using SDM, which are summarized in Table XIV. Most of these experiments use MCFs. Dynes *et al.* [273] performed an experiment transmitting quantum signals in the central core and bi-directional 10 Gb/s classical signals in two of the six outer cores over a 53 km 7-core MCF. Lin *et al.* [274] experimentally characterized QKD coexisting with 112 Gb/s data transmission in two different types of 7-core MCFs. In [275], the simultaneous transmission of quantum signals and 9.6 Tb/s classical signals over a 1 km 7-core MCF was demonstrated, where the central core was used for a quantum channel located at 1551.7 nm and each of the six outer cores was used for 1.6 Tb/s classical data transmission. Eriksson *et al.* [276] experimentally characterized the impact of crosstalk on CV-QKD in an outer core inflicted by classical channels in three neighboring cores of a 19-core MCF, verifying that the in-band crosstalk from neighboring cores may prohibit the high-integrity generation of secret keys. In [277], a quantum-classical interleaving scheme (i.e., interleaving the wavelengths in a quantum-signal core and a classical-signal core, with no wavelength overlap between these two types of cores) was proposed to alleviate the inter-core crosstalk imposed on quantum signals transmitted in an outer core by the classical signals propagating in three neighboring cores of a 7-core MCF. Bacco *et al.* [278] demonstrated the co-propagation of classical and quantum channels over a 37-core MCF and achieved a total secret-key rate of 62.8 Mbps, where each core consisted of a 10 Gb/s classical channel and a quantum channel using different wavelengths. In [279], the QKD coexistence with classical signals was evaluated over two types of MCFs, where the impacts of inter-core crosstalk and intra-core spontaneous Raman scattering on the quantum signals engendered by high-speed classical data signals were characterized. Hugues-Salas *et al.* [280] characterized the coexistence of 11.2 Tb/s classical channels in all cores with a quantum channel in the central core over a 1 km 7-core MCF. In addition to the experiments associated with MCF, Wang *et al.* [281] characterized the co-propagation of QKD with a 100 Gb/s classical data channel in a weakly-coupled FMF, achieving a secret-key rate of 1.3 kbps over 86 km FMF.

B. *Relaying*

The distance and secret-key rate of QKD systems are limited by several physical-layer impairments, such as the scattering and loss of faint quantum signals transmitted in quantum channels. In particular, amplifying a quantum signal would require measuring and cloning its related quantum states, which is against the quantum no-cloning theorem. Consequently, the realization of long-distance QKD networks has to rely on repeaters/relays.

A quantum repeater facilitates the restoration of quantum information without directly measuring the quantum states, which was first proposed in 1998 [133]. Initially, it was believed that the implementation of quantum repeaters requires matter quantum memories [282], [283] or matter qubits [284]. However, this hypothesis was later disproved by a proposal of all-photonic quantum repeaters [285] purely relying on optical devices. Given the compelling security benefits of QKD networks, quantum repeaters have attracted increasing research efforts [50], [286]–[289], as also indicated by the detailed overviews found in [51], [134]. Nonetheless, the design of quantum repeater networks is still in its infancy [59], [135], [290], and a practical quantum repeater that can be deployed in real-world QKD networks has yet to be implemented.

A viable solution to increase both the secret-key rate and the range of QKD without quantum repeaters is by inventing repeaterless schemes to overcome the fundamental rate-distance limit of QKD defined in [291]. The maximum achievable secret-key rate for a given distance was quantified by the secret-key capacity of the quantum channel in [292], hence QKD schemes presented before 2018 can never surpass the secret-key capacity bound. However, in 2018, Lucamarini *et al.* [107] proposed a TF-QKD protocol, which was capable of exceeding the point-to-point secret-key capacity of a quantum channel without using a quantum repeater. Subsequently, Minder *et al.* [293] experimentally characterized the TF-QKD protocol in a high channel loss regime, providing the experimental evidence that it is indeed possible to exceed the repeaterless secret-key capacity of [292], which has also been further validated by several additional experiments [293]–[296]. However, the TF-QKD technique is unable to extend the QKD range to an arbitrary distance and its distance record in experiments at the time of writing is 605 km [73]. Similarly, Ma *et al.* [108] presented a PM-QKD protocol,

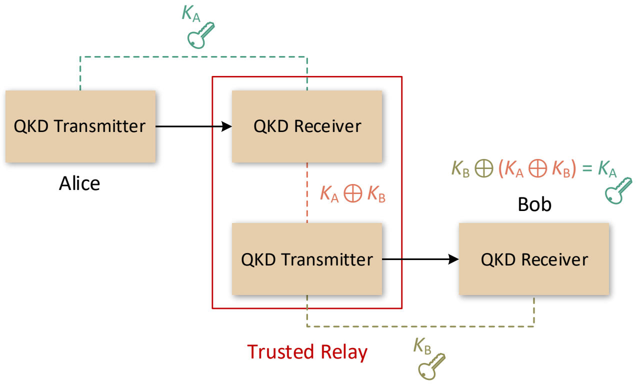


Fig. 21. Illustration of the QKD distance extension via a trusted relay between Alice and Bob.

which was also capable of surpassing the linear rate-transmittance bound of [292], since it achieved a distance of 502 km in the experiments [71].

A compromise solution that allows for an arbitrary extension of the QKD distance is that of using trusted relays, which have been widely adopted in real-world QKD networks [42]–[49]. An example of extending the distance of QKD via a trusted relay between Alice and Bob is depicted in Fig. 21. The trusted relay establishes a QKD link to both Alice and Bob. Both QKD links produce their independent secret keys, namely K_A and K_B of the same string length. The trusted relay combines the secret keys K_A and K_B with the aid of the OTP method, i.e., performs a bitwise exclusive OR operation between K_A and K_B, and then sends the result $K_\mathrm{A} \oplus K_\mathrm{B}$ to Bob. Based on $K_\mathrm{B} \oplus (K_\mathrm{A} \oplus K_\mathrm{B}) = K_\mathrm{A}$, Bob can retrieve the secret keys K_A. It should be noted that there are several optional secret-key relay schemes based on the trusted relay concept, which have been discussed in the Y.3803 recommendation produced by ITU-T [297]. The benefits of the trusted relay technique is its reduced complexity and its ability to support long-distance QKD networking, but it must be physically isolated and trustable, since it will know the secret keys.

There are several trusted relay variants. For example, Stacey *et al.* [298] presented a simplified trusted relay and examined its security level. Such a trusted relay may indeed simplify the associated computations and reduce the communication overhead during the relaying process at the expense of an eroded secret-key rate. Elkouss *et al.* [299] drew on the idea of network coding to alleviate the system's dependence on trusted relays, and proposed the concept of weakly trusted relays for QKD networks. Zou *et al.* [300] described a partially trusted relay based QKD networking solution by combining the MDI-QKD protocol with trusted relays, since MDI-QKD allows the use of untrusted relays [301], [302]. Moreover, the entanglement-based approach of [303] holds the promise of establishing QKD links that are capable of completely dispensing with any level of trust, but it is still not mature enough to be used in practical large-scale QKD networks.

C. *Satellite-Based QKD*

The fiber-based QKD networks cannot be readily supported in harsh terrain, and the signal is typically attenuated at the rate of 0.2 dB/km in the optical fiber [304]. Therefore, establishing QKD networks over ultra-long distances is facing enormous technological hurdles. One solution is that of resorting to free space, since the atmospheric attenuation in free space is less significant than in optical fiber, especially in the vacuum above the Earth's atmosphere. Satellites have the potential of distributing secret keys to ground stations via free space links, which can be used as intermediate trusted relays for interconnecting QKD networks in different physical locations on the ground [196]. Hence, the satellite-based QKD holds the promise of increasing the range of QKD networks to a global scale [49].

Hence, several successful free-space QKD experiments [305]–[313] have been performed with the goal of satellite-based QKD realization. In [314], a feasibility analysis of QKD transmissions over Earth-satellite links and inter-satellite links was provided. Bourgoin *et al.* [315] conducted a numerical simulation relying on realistic simulated orbits and analyzed the performance of the LEO satellite uplink and downlink for quantum-signal transmissions. In [316], three independent experiments were performed for verifying the feasibility of ground-satellite QKD. In [74], the air-to-ground QKD between an aeroplane and a ground station was experimentally demonstrated. Vallone *et al.* [317] demonstrated space-to-ground QKD by employing so-called corner cube retroreflectors as transmitters in orbit to the Matera Laser Ranging Observatory of the Italian Space Agency in Matera, Italy.

In August 2016, the first quantum satellite, named after Micius [75], was launched in Jiuquan, China, which is a LEO satellite and can be used to perform satellite-to-ground QKD experiments at night. In this context, significant progress has been made in the design of photon sources [318], [319], optical links [320], [321], and detectors [322], [323] for satellite-based QKD. As for satellite-based QKD, Bedington *et al.* [196] reviewed the technical challenges and summarized the quantum satellite initiatives around the world, while Khan *et al.* [83] provided an overview of the principles and engineering challenges as well as the airborne and space missions associated with QKD.

In 2018, Liao *et al.* [48] reported the experimental demonstration of a satellite-based QKD network, where a quantum satellite (i.e., Micius [75]) was used as a trusted relay

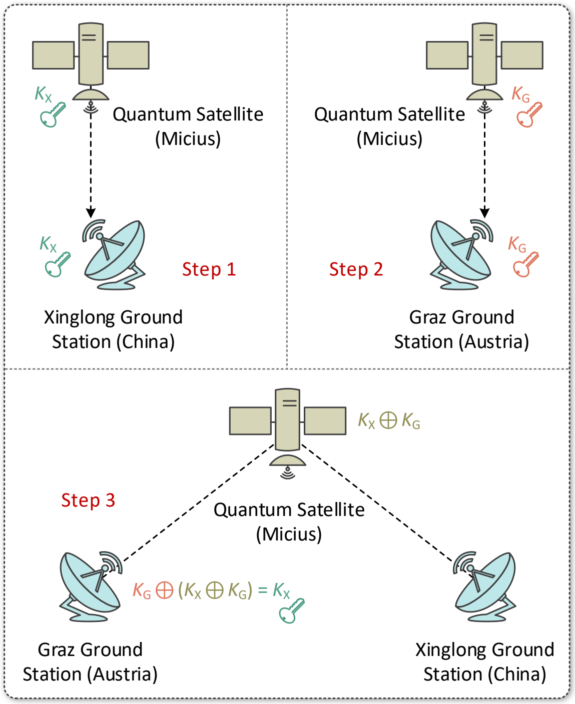

K_X
Quantum Satellite (Micius)
K_X
Step 1
Xinglong Ground Station (China)
Quantum Satellite (Micius)
K_G
K_G
Step 2
Graz Ground Station (Austria)
$K_X \oplus K_G$
Step 3
Quantum Satellite (Micius)
$K_G \oplus (K_X \oplus K_G) = K_X$
Graz Ground Station (Austria)
Xinglong Ground Station (China)

Fig. 22. Illustration of the three steps to enable two ground stations to share a secret key based on the quantum satellite.

for connecting Xinglong ground station in China and Graz ground station in Austria. In this network, three steps have to be carried out to enable two ground stations to share a secret key based on the quantum satellite, as illustrated in Fig. 22. In the first two steps, the quantum satellite implements satellite-to-ground QKD with both ground stations to produce independent secret keys with each of them, e.g., K_X with Xinglong ground station and K_G with Graz ground station. The quantum satellite holds all the secret keys, while each ground station only has access to its own secret keys. In the last step, the quantum satellite combines the independent secret keys K_X and K_G with the aid of the OTP method, i.e., performs a bitwise exclusive OR operation between K_X and K_G of the same string length, and then broadcasts the result $K_X \oplus K_G$. Using this announcement, the Xinglong ground station and Graz ground station can retrieve each other's secret keys, since $K_X \oplus (K_X \oplus K_G) = K_G$ and $K_G \oplus (K_X \oplus K_G) = K_X$. Notably, the quantum satellite must be trusted in this network. However, the requirement of trustworthiness can be eliminated by employing a robust QKD protocol capable of maintaining security even in the face of untrusted relays. In particular, in June 2020, an experimental demonstration of entanglement-based QKD was carried out between two ground stations separated by 1,120 km in China [324], relying on the Micius satellite as an untrusted relay for distributing the entangled states to the corresponding two ground stations to implement the BBM92 protocol.

To increase the coverage time for a satellite-based QKD network, daytime operation should also be supported by a quantum satellite. Liao *et al.* [76] validated the feasibility of free-space QKD in daylight for inter-satellite communications. To miniaturize the quantum satellites and reduce the cost of satellite-based QKD networks, low-cost microsatellites and nanosatellites should be adopted. In this spirit, Takenaka *et al.* [325] implemented a microsatellite-based LEO-to-ground link and verified its applicability to QKD. Grieve *et al.* [326] demonstrated the feasibility of QKD using CubeSat nanosatellites. In order to expand the coverage area as a first step towards an efficient global satellite-based QKD network, higher-orbit quantum satellites can be launched and seamless satellite constellations can be established. Explicitly, a satellite constellation consists of multiple quantum satellites operating in LEO or high earth orbit such as the geosynchronous orbit. Vergoossen *et al.* [327] proposed a model for a satellite-constellation based QKD network, in which the concept of a LEO quantum satellite acting as a trusted relay was defined and its efficiency in different constellations was investigated. In [328], a trusted relay based double-layer QKD network architecture relying on both LEO and geosynchronous satellites was proposed, where the problem of routing and secret-key assignment was addressed by jointly considering both LEO and geosynchronous satellite resources.

D. Chip-Based QKD

The large-scale practical deployment of QKD requires chip-scale integrated photonic devices for miniaturization, low power consumption, reduced cost, and high robustness [329].

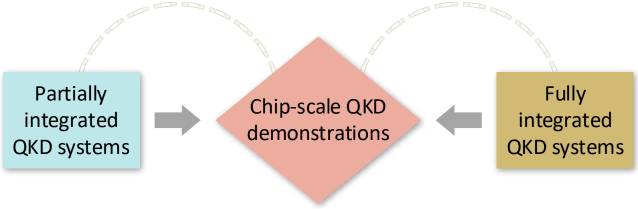

Partially integrated QKD systems
Chip-scale QKD demonstrations
Fully integrated QKD systems

Fig. 23. The evolution of chip-based QKD.

The evolution of chip-based QKD solutions is shown in Fig. 23. Early steps in this direction exploited a Mach-Zehnder interferometer using planar lightwave circuit technology [330] for stabilized operation in a QKD system [331]–[334]. Duligall *et al.* [335] designed a low-cost and compact QKD system using off-the-shelf integrated circuit components in a driver circuit for the transmitter module. As a further development, Zhang *et al.* [336] conceived a client-server QKD scheme, where all the bulky components are located at the server side (receiver side) and the client side (transmitter side) requires only an integrated photonic device that can be further integrated into a hand-held device. Vest *et al.* [319] designed a compact transmitter having an effective size of 25 mm × 2 mm × 1 mm, aiming for incorporating the QKD transmitter module in a hand-held device such as a smartphone.

The integration efforts at the transmitter side have accelerated the development of chip-scale transmitters conceived for QKD systems. A QKD transmitter chip has been fabricated using a standard silicon photonic foundry process [337], where several components can be integrated into a 1.3 mm × 3 mm die area [338]. The chip-scale transmitter has a bright application perspective in the upstream of QKD access networks [130], in which each user has a compact uplink transmitter, while the uplink receiver at the network node has sufficient space for accommodating the bulky components.

However, fully integrated compact chip-based QKD systems are required for a wide range of applications. Hence, Sibson *et al.* [329] designed chip-to-chip QKD systems relying on three different QKD protocols, namely the BB84, COW, and DPS schemes, where an indium phosphide transmitter chip and a silicon oxynitride receiver chip were fabricated. Apart from the integrated photonic indium phosphide and silicon oxynitride platforms, Sibson *et al.* [339] experimentally validated the feasibility of high-speed QKD integrated circuits based on standard silicon photonic fabrication.

Moreover, significant progress has been achieved in the demonstration of silicon photonic chips designed for SDM chip-to-chip QKD [340], high-dimensional QKD based on MCF [341], on-chip CV-QKD [342]–[344], and transceiver circuit [345], [346]. Recent experiments have demonstrated the feasibility of an MDI-QKD integrated measurement server [347] and of chip-based MDI-QKD transmitters [348], [349], suitable for cost-effective QKD access/metropolitan networks relying on untrusted relays. Furthermore, Orieux *et al.* [350] reviewed the advances in the field of integrated quantum communications, whereas Zhang *et al.* [351] surveyed the evolution of quantum photonic networks on chip.

Beyond the realms of laboratory based chip-scale QKD demonstrations, in 2018, Bunandar *et al.* [175] described their local and intercity field tests of metropolitan QKD using a high-speed silicon photonics-based encoder. Their encoder combined a Mach-Zehnder modulator with interleaved grating couplers for polarization-encoded QKD. Prior to this pioneering advance, a diverse range of different photonic degrees of freedom were explored, including the following domains: polarization [21], [305], time [85], [329], frequency [352], [353], phase [93], [331], [332], quadrature [89], [116], and orbital angular momentum [354]. They all have different pros and cons for employment in QKD systems. Polarization is generally considered to be unstable for practical fiber-based QKD, but as a remedy, silicon photonics-based encoders can correct the associated polarization drifts in a fiber link, ultimately resulting in a compact and stable platform for polarization-encoded QKD. These field tests have demonstrated that photonic integrated circuits can indeed serve as a promising and scalable platform for future metropolitan QKD networks. Notably, in 2021, Toshiba demonstrated a fully deployable chip-based QKD system [355], which served as a stepping stone for the realistic deployment of QKD based on quantum photonic chips.

VI. Enabling Techniques in the Network Layer for QKD Networks

In the past few years, numerous efforts have been made to address the technical challenges of practical QKD networking. This section provides an in-depth overview of the enabling techniques proposed for the network layer, covering the issues of SDN, key pooling, resource allocation, routing, protection and restoration, practical security, cost optimization, and multi-user QKD.

A. SDN

SDN [356], [357] constitutes an efficient network control and management technique, which enables the flexible and programmable configuration of the entire network from a central platform, namely the SDN controller. Based on this centralized controller containing all the pivotal information of a network, it becomes possible to maintain a global perspective and to react promptly in complex unexpected network scenarios. Hence, the SDN concept is capable of efficient QKD network control and management in order to improve the network performance [217], [218]. Additionally, the practical deployment of QKD services critically relies on the degree to which it can be integrated into the ubiquitous fiber infrastructure of the existing telecommunication networks. As a further benefit, the SDN concept can simplify the integration of new devices and technologies into the network.

Recently, a series of studies have investigated diverse use cases of SDN-enabled QKD networks. A software-defined quantum communication framework has been presented in [358], where a quantum communication terminal was represented in form of three layers, i.e., hardware, middleware, and software layers. In [359], a programmable multi-node quantum network was designed based on the SDN principles. Dasari *et al.* [360] described the network abstraction and configuration interfaces required for implementing a SDN-enabled programmable quantum network. Yu *et al.* [361] conceived a novel SDN-enabled QKD network architecture, requiring a reduced secret key, yet improving the QKD network's availability and performance. In [362], a SDN-based QKD network model relying on a sophisticated routing algorithm was proposed. Humble *et al.* [363] presented a quantum network switching solution based on cutting-edge SDN principles, in which a programmable quantum switch was used to support the establishment of a desired quantum channel. In addition, Wang *et al.* [364] provided a brief overview of the SDN-enabled QKD network architecture as well as of its related interfaces and protocols.

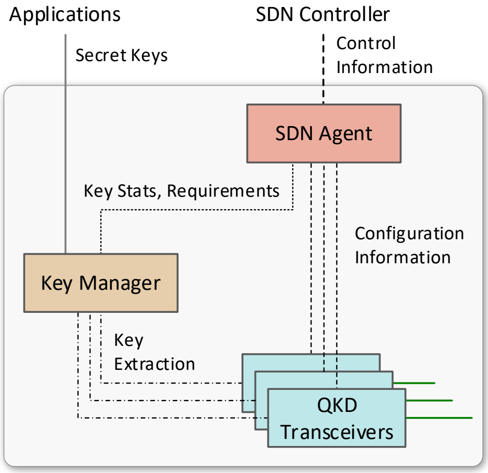


Fig. 24. Abstraction model of a SDN-enabled QKD node [163], [217].

On the experimental side, Cao *et al.* [201], [202], [365] exploited the SDN philosophy in support of QKD as a service (QaaS) [366], multi-tenant provision [200], and key on demand (KoD) service provision [204]. In these use cases, the above-mentioned specific functions were developed for the SDN controller, and the original OpenFlow protocol was extended and the associated detailed workflows were conceived. Moreover, an experimental testbed was established for demonstrating the efficiency and flexibility of the SDN-based approaches conceived for QaaS, multi-tenant provision, and KoD service provision.

As a further development, Aguado *et al.* [210] adopted SDN in a cost-efficient approach for time-sharing the QKD systems, where the ease of integrating QKD systems with a network function virtualization (NFV) platform was experimentally demonstrated. In [367], [368], the necessary workflows and protocol extensions of different SDN scenarios were defined and demonstrated for providing end-to-end quantum encryption services, in which the key synchronization process required for the subsequent encryption may be readily integrated into the main protocols for control interface implementation. Hugues-Salas *et al.* [369], [370] developed a SDN application for the real-time monitoring of the associated quantum parameters (e.g., QBER and secret-key rate) and for triggering the appropriate action in the event of link level attacks to ensure the uninterrupted distribution of the secret keys. Egorov *et al.* [371] investigated the capability of the SDN paradigm to support subcarrier based QKD systems relying on the OpenFlow protocol to orchestrate routing based on the associated link parameters. In [372], a machine learning aided SDN relying on optimal resource allocation was constructed for investigating the coexistence of quantum and classical channels in a QKD-integrated optical network field trial. In [373], the authors extended the standard Open Networking Foundation (ONF) transport API [374] of a SDN to enable quantum encryption in end-to-end services.

Further innovative SDN solutions were disseminated by Aguado *et al.* [163] reporting on a converged quantum-classical network constructed in Madrid, Spain. Such a network demonstrated the first SDN-based QKD network in the field. Furthermore, this network has been used to support path verification in the associated service function chains [375]. The abstraction model of an SDN-enabled QKD node used in this network is shown in Fig. 24, which has been defined within the ETSI GS QKD 015 [217]. Observe at the bottom of Fig. 24 that several QKD transceivers are placed in the same physical location, which are able to establish quantum channels and produce secret keys. The secret keys produced are stored in a key manager, which manages the secret keys derived from different QKD transceivers that are collected via a key extraction interface. This key manager can deliver the secret keys to multiple applications. By relying on the key manager and the QKD transceivers of Fig. 24 within the node, a SDN agent becomes capable of collecting important information from the node of communicating with the SDN controller, as well as satisfying the process configuration updates requested by the SDN controller.

B. *Key Pooling*

The achievable secret-key rates of most point-to-point QKD systems are very low at the time of writing, for example, 1.2 Mbps over a 50.5 km fiber link [69] and 6.5 bps over a 405 km fiber link [70]. In order to guarantee high security, the secret keys produced by the QKD systems in a QKD network cannot be reused, hence they constitute precious resources that have to be frugally employed.

Conventionally, the quantum key pool (QKP) is used as a repository of the local secret keys generated, which also has to be synchronized with other sites [203], [376]. The QKPs located at two directly connected sites of a QKD network must match in content so that the same secret keys can be referenced and discovered. When the QKPs are initialized, the secret keys are derived from QKD transceivers and injected into their connected QKPs. Once the QKP is full, naturally, no new secret keys may be injected, because the available secret keys would be overwritten by the new ones. It is also possible to increase the size of a QKP to contain more secret keys. Notably, the QKP should be physically protected so that it cannot be accessed directly by any illegitimate means. Additionally, a logical key pool was proposed in [203], which contains global secret keys produced by relying on key relaying between a pair of end nodes, which may be employed to facilitate the management of global secret keys. A temporary key pool of [376] acts as a key buffer that manages the temporary storage of the local secret keys being relayed by a local node, which improves the efficiency of key relaying.

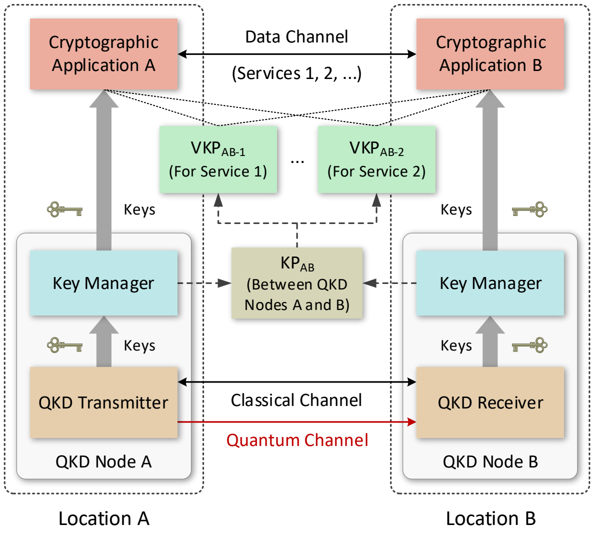


Fig. 25. Illustration of the new concepts of KP and VKP [208].

On the other hand, the overall lifetime of secret keys has to be monitored and managed efficiently, which involves several stages, such as the secret-key generation, storage, relay, supply, and destruction. In contrast to conventional key pools used to collect secret keys, several new key pooling techniques have been presented in the literature for improving the efficiency of secret-key monitoring and management [200], [204], [208], [377].

The new concepts of key pool (KP) and virtual key pool (VKP) have been described in [208] and they are illustrated at a glance in Fig. 25. The secret keys are synchronously generated between a pair of connected QKD transceivers and stored in the corresponding key managers. The key managers can supply secret keys to multiple services for their data encryption. The QKD transceivers and key managers are embedded into their corresponding QKD nodes. A KP (e.g., KP$_{AB}$ between QKD nodes A and B) abstracted from two key managers is able to monitor the real-time secret-key rate/volume information, and manage the secret-key generation, storage, relay, supply, and destruction in a pair-wise manner. A VKP abstracted from a KP may be granted management privileges for a portion of secret keys and use these secret keys for enhancing the security of a dedicated service, e.g., VKP$_{AB-1}$ and VKP$_{AB-2}$ abstracted from KP$_{AB}$ for Services 1 and 2, respectively. The secret keys are processed locally and the KPs/VKPs are used for improving the management efficiency of the associated secret keys. More

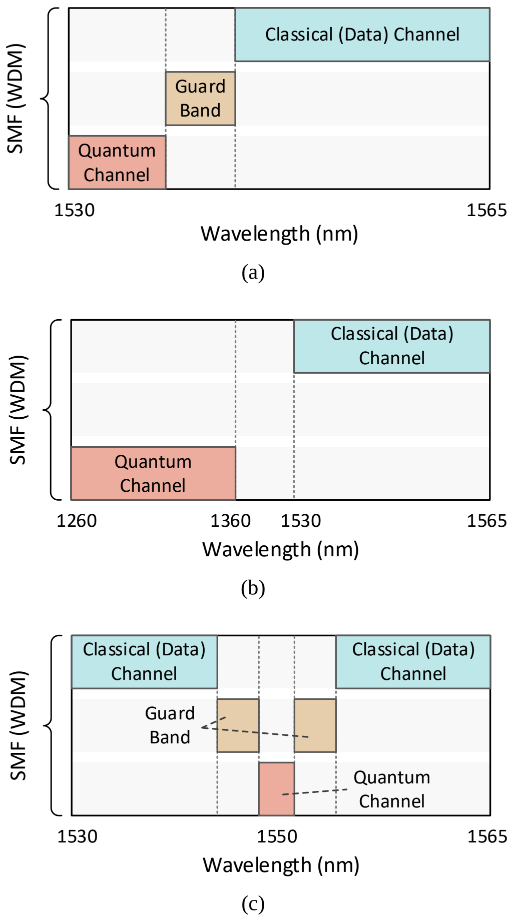


Fig. 26. Three schemes of wavelength allocation for different channels: (a) C-band for both quantum (near 1530 nm) and classical (data) channels [205]; (b) O-band for quantum channels and C-band for classical (data) channels [378]; (c) C-band for both quantum (near 1550 nm) and classical (data) channels.

concretely, all the stages during the overall lifetime of secret keys are handled within the QKD nodes across the QKD network in a distributed manner. Hence, the security of keys is not sacrificed when using KPs/VKPs, since they are not exchanged across different physical locations. In practice, the KPs and VKPs can be implemented based on the SDN controller.

C. *Resource Allocation*

In QKD networks, multiple resource dimensions have to be considered. Naturally, resource allocation for the quantum and classical channels hinges on the specific multiplexing techniques used in the network, as exemplified by the wavelength, time slot, and core/mode resources of WDM, TDM, and SDM, respectively. In contrast to the co-fiber transmission technology discussed above, the focus here is on resource allocation issues in the network layer.

In [205], [378], a pair of wavelength allocation schemes was designed for different channels in a QKD-over-WDM network, as depicted in Figs. 26(a) and 26(b). In Fig. 26(a), the fiber's C-band is chosen for both quantum and classical (data) channels in order to maintain a low attenuation for high quality quantum-signal transmission. The quantum channels can be accommodated at high frequencies (i.e., near 1530 nm wavelength) to reduce the effect of Raman scattering, whilst separating it by using a guard band from the classical (data) channels for mitigating the effect of FWM, and for improving the channel isolation. By contrast, in Fig. 26(b), the fiber O-band is chosen for quantum channels and the fiber C-band is chosen for the classical (data) channels in order to guarantee sufficient isolation for mitigating their linear crosstalk and the associated filtering specification. It should be noted that other wavelength allocation schemes can also be used, such as placing the quantum channels near the 1550 nm wavelength to achieve the lowest possible attenuation of the quantum signals, as illustrated in Fig. 26(c).

In order to improve resource utilization for QKD integration into a classical telecommunication network, WDM can be combined with TDM by seating multiple time slots for accommodating the quantum channels [205], [207]. A static routing, wavelength, and time-slot assignment (RWTA) problem has been addressed using the classic integer linear programming (ILP) model and a heuristic algorithm in [205], [377], whereas a dynamic RWTA problem has been solved with the aid of heuristic algorithms [207], [211], [379], [380]. To improve the achievable secret-key rates in a hybrid quantum-classical network, several low-complexity yet near-optimal wavelength assignment methods have been presented in [381], [382]. In particular, machine learning based techniques have been proposed for the near real-time prediction of the optimal channel allocation as well as for the accurate prediction of quantum parameters, facilitating the reallocation of quantum channels and the efficient parameter evaluation to ensure excellent performance [372], [383]–[385]. As a further advance, core and wavelength/spectrum resource allocation solutions have been proposed for MCF-based QKD-over-SDM networks [386]–[388], with the objective of maximizing the attainable secret-key rate and minimizing the resources required.

The secret key constitutes a unique resource dimension in the QKD network, since after it was utilized it must be destroyed. The flowchart of a simple secret-key allocation scheme is

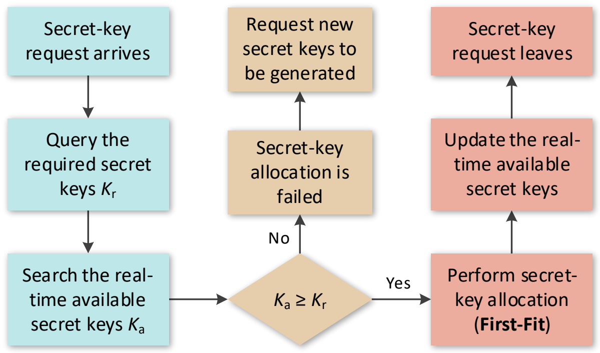

Secret-key request arrives
Query the required secret keys K_r
Search the real-time available secret keys K_a
$K_a \geq K_r$
No
Secret-key allocation is failed
Request new secret keys to be generated
Yes
Perform secret-key allocation (First-Fit)
Update the real-time available secret keys
Secret-key request leaves

Fig. 27. Illustration of the flowchart of a simple secret-key allocation scheme.

illustrated in Fig. 27, where the so-called first-fit algorithm of [200] is used for secret-key allocation. In the first-fit algorithm, all the available secret keys are numbered, where a lower-numbered secret key is selected before a higher-numbered one. In reality, the first-fit algorithm has been commonly utilized in numerous secret-key assignment strategies [200], [204], [208], [389], [390] as a benefit of its low complexity.

In order to achieve efficient secret-key resource exploitation, the new concept of KoD has been defined to allocate secret keys for satisfying the security requirements in a timely on demand manner, while an adaptive secret-key assignment strategy has been proposed for KoD in [204], which was also experimentally demonstrated [365]. Additionally, a heuristic algorithm has been designed in [200] to accomplish offline secret-key assignment for multiple tenants over a QKD network. A comparative study of heuristics and reinforcement learning based techniques designed for online multi-tenant secret-key assignment over a QKD network has been conducted in [389]. A suite of secret-key assignment schemes has also been conceived for securing virtual optical networks [208], [390], [391], multicast services [392], and passive optical networks (PONs) [393].

D. Routing

A routing mechanism is necessary when there is no direct point-to-point QKD link between two QKD nodes. Such a mechanism should be able to provide the required QoS in a QKD network [394]. Previously, an extended version of the Open Shortest Path First (OSPF) protocol was developed in [395] as a routing protocol for the SECOQC QKD network [43], [396], in which Dijkstra algorithm was used for finding the shortest path between the source and destination QKD nodes. Another commonly used routing protocol is the destination-sequenced distance-vector routing protocol [397], which has also been used in the modeling and simulation of a practical QKD network [398].

Specifically, Tanizawa *et al.* [399] discussed the associated routing requirements and designed bespoke routing solutions for a QKD network. As shown in Fig. 28, these routing requirements include choosing the optimal QKD link associated with sufficient secret keys, handling both encrypted and unencrypted traffic, allowing sufficiently frequent routing updates, while consuming no local secret keys through the routing protocol control packet exchanges. To elaborate a little further, the control packet exchange between QKD nodes is required for operating the routing protocol, since it is important for path selection during secret-key relaying. However, this traffic does not have the secret key information and is not required to be encrypted. Hence, it was suggested in [399] that no local secret keys are used during the control packet exchange, aiming for saving some precious local secret keys.

The routing solutions designed consist of four components: 1) an interface architecture of the QKD node for offering a pair of virtual interfaces to connect both with encrypted and unencrypted networks; 2) a routing algorithm extending the OSPF by considering the amount of secret keys available along each QKD link as a routing metric; 3) an Internet Protocol (IP) address allocation scheme connecting both encrypted and unencrypted interfaces; 4) a routing protocol deployment approach allowing the management of routing table entries without consuming any secret keys.

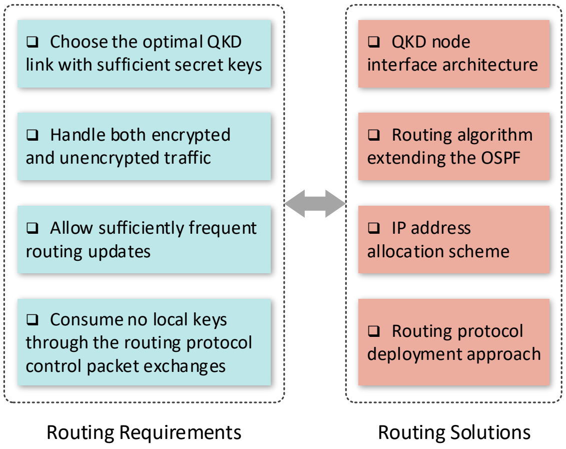

❑ Choose the optimal QKD link with sufficient secret keys
❑ Handle both encrypted and unencrypted traffic
❑ Allow sufficiently frequent routing updates
❑ Consume no local keys through the routing protocol control packet exchanges
❑ QKD node interface architecture
❑ Routing algorithm extending the OSPF
❑ IP address allocation scheme
❑ Routing protocol deployment approach
Routing Requirements
Routing Solutions

Fig. 28. Routing requirements and bespoke routing solutions for a QKD network [399].

In order to improve the QoS in QKD networks, several effective routing mechanisms have been presented [400]–[404]. The adaptive stochastic routing algorithms of [400], [401] have been designed for hiding the routing information and augmenting the secrecy. A multi-path search algorithm [402] and a dynamic routing scheme [403] have been designed for finding available paths in a QKD network, where the best path is selected as the route based on multiple factors. Yang *et al.* [404] proposed a secret-key-aware routing method for finding the optimal path in a QKD network, while increasing the success rate of key exchange as well as striking a trade-off between the secret-key generation and consumption rate on each QKD link.

The classical channel of the QKD link should also be considered in the routing decisions of QKD networks since its performance can affect the quantum channel and vice versa [405]. Mehic *et al.* [212] introduced a QoS model for QKD networks that includes several metrics for characterizing the states of the quantum and classical channels as well as of the overall QKD links. They also proposed a routing protocol that can determine the optimal route in terms of minimum secret-key consumption.

Moreover, the routing entanglement problem of quantum networks has recently attracted widespread attention [406]–[413]. However, the large-scale entanglement-based quantum networks are still not practical in the real world at the time of writing.

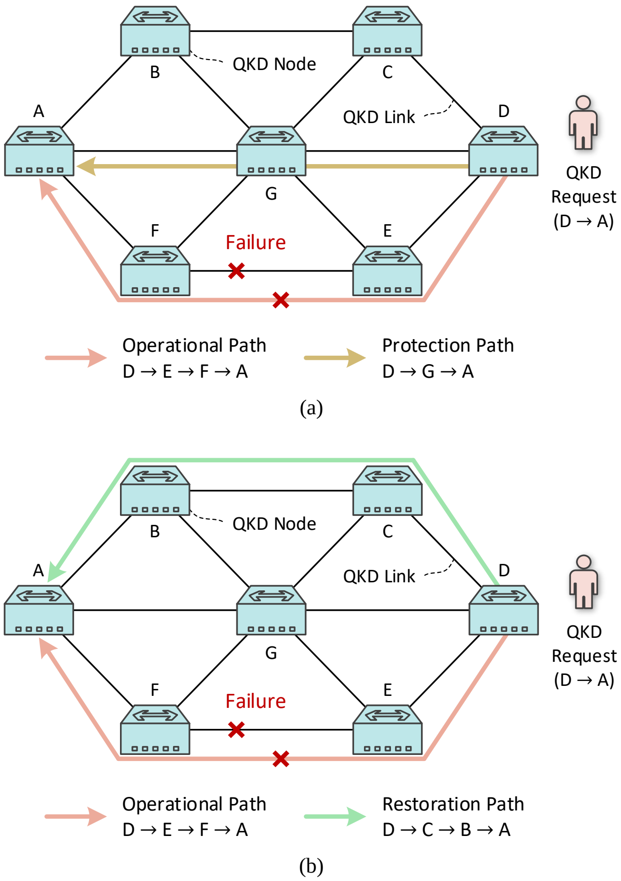
E. Protection and Restoration

To guarantee the uninterrupted distribution of secret keys in support of service continuity, a QKD network should be robust against both node and link failures. These failures can also be regarded as the physical infrastructure attacks. To construct a reliable QKD network and ensure its uninterrupted operation, protection and restoration schemes have to be designed.

The global path protection scheme and rerouting restoration scheme of QKD networks [379] are illustrated in Figs. 29(a) and 29(b), respectively. In the global path protection scheme, two paths (called operational path and protection path) are identified and configured for each QKD request in advance. A QKD request may opt for using the protection path, when its operational path encounters a failure. However, when both the operational path and the protection path encounter failures, new paths have to be found, such as the restoration path of Fig. 29(b).

For handling link failures, the so-called key-volume-adaptive dedicated protection and shared protection schemes have been conceived for QKD networks [414]. The authors demonstrated by simulations that the shared protection scheme outperforms its dedicated protection based counterpart in terms of its blocking probability and secret-key consumption. In order to further improve the secret-key resource utilization for the shared protection scheme, Wang *et al.* [415] designed a shared backup path protection scheme for QKD networks under a single link failure and demonstrated its benefits by simulations.

As a further development, Chapuran *et al.* [168] demonstrated the feasibility of automated QKD resynchronization following a network path reconfiguration event using a quantum clock recovery algorithm [167]. Moreover, Wang *et al.* [416] proposed a so-called secret-key restoration scheme that involves both one-path, as well as multi-path, and time-window-based restoration algorithms to recover normal services in the face of a single link failure in a QKD network. Their numerical results show that the network performance of the three algorithms was best for the time-window-based algorithm, followed by the multi-path and one-path restoration algorithms.


QKD Node
QKD Link
A
B
C
D
E
F
G
Failure
QKD Request (D → A)
Operational Path D → E → F → A
Protection Path D → G → A
Restoration Path D → C → B → A

(a)

(b)

Fig. 29. Illustration of the (a) global path protection scheme and (b) rerouting restoration scheme for QKD networks.

To elaborate a little further on the causes of link failure, given the sensitivity of quantum signals to various physical-layer impairments, an attack on a QKD link can be launched, for example by increasing the noise above the threshold to disrupt the distribution of secret keys without cutting the optical fiber. Such an attack may manifest itself in form of a denial of service attack, signal injection attack, etc. Hugues-Salas *et al.* [369], [370] experimentally investigated the mitigation of these attacks in a QKD network, achieving reliable link failure identification after the attack, followed by rerouting a path to recover the connection for a pair of QKD devices.

F. *Practical Security*

Given that the most important feature of QKD networks is their enhanced security, it is critical that its realistic implementation does not jeopardize it.

On the quantum side, the imperfections of realistic QKD devices might cause deviations from the idealized theoretical models, which may result in vulnerability to many special attacks. The attacks may occur both at the source and detection sides of a QKD system, applying photon number splitting [110], [111] and phase information [417] attacks to the source, Trojan horse attacks [418]–[420] on the source and detection, detector blinding and control attacks [421]–[425], and so on. For example, the photon number splitting attack on imperfect sources has been addressed by the decoy-state method [94]–[96], while MDI-QKD [106] can eliminate all detection attacks. Indeed, a considerable amount of work has been dedicated to reducing the gap between the theory of QKD and its corresponding implementations. We refer the reader to a recent review [31] for more details on various practical vulnerabilities and advanced countermeasures for QKD systems. Moreover, Walenta *et al.* [426] studied the security certification of commercial quantum technologies from a practical perspective, enabling commercial QKD network devices to conform to security standards.

On the classical side, Salvail *et al.* [427] proposed a method to guarantee the privacy and authenticity of secret keys, where some nodes were taken over by an adversary. The proposed method has the potential of differentiating between authentic and forged keys, but additionally, it can also reveal malicious parties in some cases. As a further advance, Cederlof *et al.* [428] analyzed the security effects of using a secret key generated by QKD in the current round for authentication in the subsequent

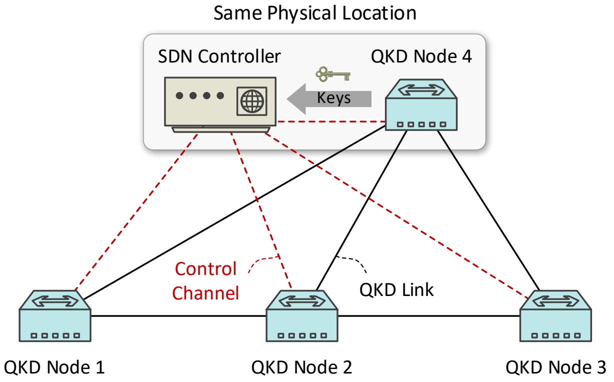


Fig. 30. Illustration of using the QKD-based secret keys to enhance the security of control channels in a SDN-enabled QKD network.

round, where a security weakness of authentication was discovered and an appealingly simple solution was proposed for addressing this weakness. Cho *et al.* [429] discussed a host of practical issues concerning the secure deployment of QKD in optical communication systems, and proposed a realistic system model as well as practical solutions to tackle the associated security issues. In [430], four mixed trusted/untrusted relay placement strategies were devised for enhancing the security level of QKD deployment over optical networks, achieving substantial security level improvements compared to the conventional purely trusted relay placement strategies.

In practice, the security of the control plane in a QKD network is very important, since the illegitimate disclosure or modification of any control/configuration information may compromise the entire QKD network. Kitayama *et al.* [431] used the secret keys of a QKD network to encrypt not only the user data but also the control signals arriving from the generalized multi-protocol label switching (GMPLS) controllers, where the OTP method can be utilized for control signal encryption, since the control signals tend to be compact. In particular, several types of control plane attacks may arise in the context of the SDN technique. These attacks and their corresponding classical defense techniques have been detailed in [357], [432]. With respect to the quantum defense techniques designed for protecting SDN from control plane attacks, Cao *et al.* [204] proposed an attractive technique relying on the secret keys to enhance the security of control channels in a software defined optical network. As illustrated in Fig. 30, by placing a QKD node next to the SDN controller and connecting it to other QKD nodes via QKD links, the security of control channels in a SDN-enabled QKD network can be enhanced using the QKD-based secret keys. Furthermore, regarding a hybrid combination of quantum and classical security schemes, the secret keys derived from QKD can be combined with conventional key exchange protocols (e.g., Diffie-Hellman) to secure the control plane in SDN and NFV environments [433].

G. *Cost Optimization*

The escalating cost of nodes and links is regarded as one of the major barriers to the practical deployment of QKD networks. Hence, cost optimization is essential for QKD networks, especially for a QKD backbone network owing to its large scale and hence potentially excessive cost [434]. At the time of writing, almost all the practical QKD backbone networks deployed in the field are trusted relay based QKD networks, where two types of QKD nodes are required, namely the QKD backbone node (QBN) and the QKD relay node (QRN). A QBN acts as the end node (i.e., the source or destination node of a QKD request[8]) for the users but it also incorporates the function of QRNs. The QRNs act as the intermediate nodes between two neighboring QBNs, which rely on trusted relays for QKD distance extension.

To satisfy the performance requirements of network users at a minimum cost, Alléaume *et al.* [435] introduced several analytical models for optimizing the spatial distribution of both the QKD nodes and of the QKD links during the QKD network deployment phase. They also determined where independent optical fibers have to be deployed as QKD links. By contrast, deploying QKD over a WDM backbone network is beneficial in terms of reducing the deployment difficulty and cost, where a certain fraction of wavelength channels in a WDM backbone network has to be reserved for QKD links. The cost of deploying QKD over a WDM backbone network has been discussed in [378], which is mainly determined by the following three aspects.

- *Cost of QKD transceivers in QKD nodes:* Let C_{U} denote the cost of a QKD transceiver (i.e., a transmitter and a receiver). The physical distance between a pair of neighboring QKD nodes (e.g., a QBN and a QRN, or two QRNs) is assumed to be fixed and denoted by D (~80 km). The achievable secret-key rate corresponding to the physical distance D on a single QKD link is denoted by k. The number of QKD transceivers required for a QKD request r at a secret-key rate requirement of v_r is
$$N_{\mathrm{U}}^{r}=\frac{v_r}{k}\left\lceil\frac{L_{sd}}{D}\right\rceil, \tag{1}$$
where L_{sd} is the physical distance between a pair of QBNs s_r and d_r. Let R denote the full set of QKD requests in a QKD network. Then, the total number of QKD transceivers required in a QKD network is
$$N_{\mathrm{U}}^{R}=\sum_{r\in R}N_{\mathrm{U}}^{r}\,. \tag{2}$$
- *Cost of auxiliary equipment (key manager, optical switch, multiplexer, demultiplexer, secure infrastructure, etc.) in QKD nodes for QKD networking:* The costs of auxiliary equipment in a QBN and a QRN are assumed to be fixed as C_{B} and C_{T}, respectively. The total number of QBNs in a QKD network is denoted by N_{B}. The number of QRNs required for a QKD request r is

[8] The QKD request is defined as a request that has a specific secret-key rate requirement between a pair of distant QKD users.

$$N_{\mathrm{T}}^{r} = \left\lceil \frac{L_{sd}}{D} - 1 \right\rceil . \tag{3}$$

Then, the total number of QRNs required in a QKD network is

$$N_{\mathrm{T}}^{R} = \sum_{r\in R} N_{\mathrm{T}}^{r} . \tag{4}$$

- *Cost of QKD links:* Two types of channels, i.e., quantum and classical channels have to be established as QKD links. The cost of QKD links is directly associated with the number of quantum and classical channels as well as the physical length of QKD links. Let C_{W} denote the cost per kilometer of a wavelength channel on a fiber link. The physical length of QKD links for a QKD request r is

$$L_{\mathrm{W}}^{r} = 2\frac{v_r}{k} L_{sd} . \tag{5}$$

Then, the total required physical length of QKD links in a QKD network is

$$L_{\mathrm{W}}^{R} = \sum_{r\in R} L_{\mathrm{W}}^{r} . \tag{6}$$

Based on the above formulation, Cao *et al.* [378] defined a cost-oriented model for deploying QKD over a WDM backbone network as follows:

$$C_{\mathrm{Total}} = C_{\mathrm{U}} N_{\mathrm{U}}^{R} + C_{\mathrm{B}} N_{\mathrm{B}} + C_{\mathrm{T}} N_{\mathrm{T}}^{R} + C_{\mathrm{W}} L_{\mathrm{W}}^{R} , \tag{7}$$

where C_{Total} is the total cost of QKD network deployment, which is composed of four terms, covering the cost of QKD transceivers in all the QBNs and QRNs, the cost of auxiliary equipment in all the QBNs, the cost of auxiliary equipment in all the QRNs, and the cost of QKD links. Notably, the physical-layer parameters such as secret-key rate, physical distance, and the layout of QRNs have been incorporated in this cost-oriented model. The above equations (1) to (7) correspond to the equations (1) to (7) formulated in [378], respectively. In the above formulation, the QBNs and some QRNs can be shared among different QKD requests (i.e., the components related to different requests may be placed at the same node), but the components such as QKD transceivers are not shared by different QKD requests. This is because the QKD requests are independent of each other.

In [378], two methods, i.e., an ILP model and a heuristic algorithm, have been proposed for optimizing the cost of QKD network deployment. Specifically, the items used for cost optimization of QKD networks are listed in Table XV, where three cases are considered, including a rather pessimistic case having fixed cost values (Case 1), an optimized case with fixed cost values (Case 2), and a dynamic case with flexible cost values (Case 3). It should be noted that the final results may be highly dependent on these assumed cost values.

Through numerical simulations, the total QKD network cost versus the number of QKD requests in three cases under the ILP model, heuristic algorithm, and a benchmark (involving random routing and random channel allocation) is illustrated in Fig. 31. The ILP model cannot be adopted in Case 3, where the cost-oriented model is nonlinear, because the cost values are made flexible. It can be observed in Fig. 31 that the heuristic algorithm delivers similar results to the ILP model. Furthermore, both the ILP model and heuristic algorithm significantly outperform the benchmark in Cases 1 and 2. The total QKD network cost increases with the number of QKD requests in Cases 1 and 2, since the required number of QKD network elements becomes larger and the cost values of the elements are fixed. In Case 3, the total QKD network cost increases non-linearly with the number of QKD requests, because the component cost values depend on the total number of QKD transceivers required. Hence, the cost optimization of the ILP model or heuristic algorithm relative to the benchmark in Case 3 is directly related to the assumptions about the component cost values. Moreover, Case 2 shows the lowest total QKD network cost because the optimized cost values based on photonic integration and publicly funded development are adopted.

TABLE XV
COST VALUES USED FOR COST OPTIMIZATION OF QKD NETWORKS [378]

	Case 1	Case 2	Case 3		
N_{U}^{R}	≥1	≥1	1	2–2,000	>2,000
C_{U} (US$)	40,000	10,000	40,000	$-15N_{\mathrm{U}}^{R}+40,000$	10,000
C_{B} (US$)	30,000	10,000	30,000	$-10N_{\mathrm{U}}^{R}+30,000$	10,000
C_{T} (US$)	20,000	5,000	20,000	$-7.5N_{\mathrm{U}}^{R}+20,000$	5,000
C_{W} (US$)	8	5	8	$-0.0015N_{\mathrm{U}}^{R}+8$	5

It is important to note that the above modeling and analysis is only one of the QKD network cost optimization options based on trusted relays. Depending on the diverse types and requirements of QKD networks as well as the different cost values, various novel cost optimization solutions for QKD networks may be conceived. Specifically, the cost optimization of hybrid trusted/untrusted relay based QKD deployment over optical backbone networks has been addressed in [436].

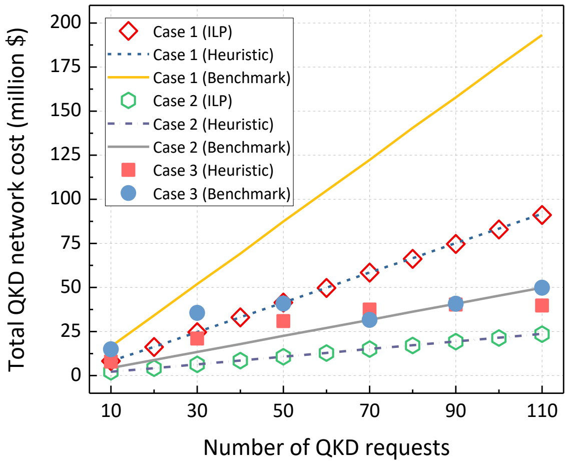


Fig. 31. Illustration of the total QKD network cost versus the number of QKD requests in three cases under the ILP model, heuristic algorithm, and benchmark (14-node 21-link NSFNET topology, $v_r = k$) [378].

H. Multi-User QKD

Multi-user QKD networks exhibit an improved cost efficiency. Since Townsend *et al.* [437] first exploited the properties of a PON to realize one-to-any QKD in 1994, numerous investigations have been dedicated to multi-user QKD access networks. By extending the schemes described in [437], Phoenix *et al.* [438] implemented any-to-any QKD in an optical network. Moreover, Townsend [136] designed a practical scheme for multi-user QKD and demonstrated its operation in a PON.

With respect to different PON techniques, Kumavor *et al.* [439] compared four different PON topologies (including passive-star, optical-ring, wavelength-routed, and wavelength-addressed bus architectures) in realizing multi-user QKD, demonstrating their applicability for serving networks of different sizes. The major findings of [439] were that the star network supported the lowest number of users, the ring topology had the highest key rate for networks with less than 60 users, the wavelength-routed network was independent of the number of users, and the wavelength-addressed bus network performed favorably for networks only supporting a few users. Based on a wavelength-addressed bus architecture, Kumavor *et al.* [440] implemented and experimentally investigated a six-user QKD network relying on a bus topology, where the bus was a standard telecommunication fiber with the total length of 30.9 km. As a further development, Fernandez *et al.* [441] tested both point-to-point and point-to-multipoint PON architectures in the context of multi-user QKD. In [442], different implementation options have been critically appraised for employment in multi-user QKD relying on optical access networks, covering point-to-point Ethernet, Ethernet PON, GPON, WDM PON, WDM/TDM PON, etc. Inspired by [439]–[442], the numbers of QKD users that can be accommodated by diverse PON architectures can be further compared and optimized. Meanwhile, a number of studies have been carried out for characterizing the different aspects of QKD over PONs, such as quantum information to the home [137], seamless integration [231], [443], and their security analysis [444].

Elmabrok *et al.* [445] proposed the practical setups that facilitate wireless access to hybrid quantum-classical networks. Some other available dimensions, such as the time and code domains, have been employed in the investigations of time-division multiple access and code-division multiple access (CDMA) based multi-user QKD networks [446]. Following the principle of CDMA, a quantum spread spectrum multiple access scheme has been designed in [447].

In particular, a multi-user quantum access network has been experimentally demonstrated in [130], which can bring QKD closer to practical applications. Several important issues such as the associated wavelength assignment [382] and finite-key effects [448] have also been investigated in the context of quantum access networks. Cai *et al.* [449] characterized a quantum access network supporting peer-to-peer multimedia service between optical network units (ONUs), while realizing direct quantum and classical ONU-ONU communications with an "N:N" splitter. Furthermore, a multi-user QKD network based on entanglement has been proposed and theoretically studied in [450].

When it comes to applications, the novel concept of QaaS has been proposed in [201], [366], which allows multiple users to apply for dedicated QKD services relying on secret keys acquired from the same QKD network infrastructure. On the other hand, multi-tenancy is regarded as a cost-effective technique of employing secret keys, where each tenant is a high-security user who needs secret keys from the QKD network infrastructure. The offline multi-tenant key provision problem has been addressed in the context of QKD networks by upon controlling a secret-key rate sharing scheme by a heuristic algorithm [200]. A more advanced online version has been optimized by using heuristics and reinforcement learning [389]. Finally, a multi-tenant metropolitan QKD network has been described and experimentally characterized in [202].

VII. Standardization Efforts

The industrial-scale roll-out of QKD networks still faces a lot of challenges, where standardization plays a crucial role in terms of ensuring the compatibility of components produced by different global suppliers. Motivated by the QKD advantages, multiple standardization bodies (e.g., ETSI, ITU-T, ISO/IEC, IETF, IEEE, and CSA) are working on QKD standards. Table XVI summarizes the standardization efforts in QKD and the Qinternet from these groups.

A. ETSI

The ETSI industry specification group for QKD (ISG-QKD) was established in 2008, and has been as instrumental in promoting QKD standardization as ITU-T. Specifically, ETSI ISG-QKD has developed a series of group specifications and reports for QKD. Länger *et al.* [484] detailed the intention of establishing the ETSI ISG-QKD, which is essentially the creation of universally accepted QKD standards. Weigel *et al.* [485] further emphasized the need for QKD standardization and highlighted the ETSI approach to standardizing QKD. In Table XVI we listed different group reports and specifications at a glance.

B. ITU-T

Since 2018, the ITU-T Study Group 13 (SG13) and Study Group 17 (SG17) have been working on new study items on the standardization of QKD networks, as listed in Table XVI. In October 2019, the first QKD-related ITU-T recommendation Y.3800 [65] was published to provide an overview on networks supporting QKD, covering the relevant conceptual structure, layered model, and basic functions facilitating the implementation of QKD networks. Table XVI lists a set of ITU-T recommendations that have reached different state of maturity.

Moreover, in order to provide a collaborative platform for pre-standardization aspects of quantum information technology with an emphasis on networks, the ITU-T Focus Group on Quantum Information Technology for Networks (FG-QIT4N) was established in September 2019.

C. *ISO/IEC*

The ISO/IEC JTC 1/SC 27 is a standardization subcommittee operating under the auspices of the Joint Technical Committee 1 (JTC 1) of ISO and IEC, contributing to the development of standards for the protection of information as well as

TABLE XVI
SUMMARY OF STANDARDIZATION EFFORTS IN QKD AND THE QINTERNET

Group	**Serial Number**	**Subject**	**Type**	**Year/ Status**	**Ref.**
ETSI	GS QKD 002	QKD use cases	Group specification	2010	[451]
	GR QKD 003	QKD components and internal interfaces	Group report	2018	[213]
	GS QKD 004	QKD application interface	Group specification	2020	[221]
	GS QKD 005	QKD security proofs	Group specification	2010	[452]
	GR QKD 007	QKD vocabulary	Group report	2018	[453]
	GS QKD 008	QKD module security specification	Group specification	2010	[454]
	GS QKD 011	Optical component characterization for QKD systems	Group specification	2016	[455]
	GS QKD 012	Device and communication channel parameters for QKD deployment	Group specification	2019	[66]
	GS QKD 014	Protocol and data format of REST-based key delivery API	Group specification	2019	[222]
	GS QKD 015	QKD control interface for SDN	Group specification	2021	[217]
	GS QKD 010	Protection against Trojan horse attacks in one-way QKD systems	Group specification	Drafting	[456]
	GS QKD 013	Characterization of optical output of QKD transmitter modules	Group specification	Drafting	[457]
	GS QKD 016	Common criteria protection profile for QKD	Group specification	Drafting	[458]
	GR QKD 017	QKD network architectures	Group report	Drafting	[459]
	GS QKD 018	QKD orchestration interface of SDN	Group specification	Drafting	[460]
	GR QKD 019	Design of QKD interfaces with authentication	Group report	Drafting	[461]
ITU-T	Y.3800	Overview on networks supporting QKD	Recommendation	2019	[65]
	Y.3801	Functional requirements for QKD networks	Recommendation	2020	[462]
	Y.3802	QKD networks - Functional architecture	Recommendation	2020	[463]
	Y.3803	QKD networks - Key management	Recommendation	2020	[297]
	Y.3804	QKD networks - Control and management	Recommendation	2020	[464]
	Y.3805	QKD networks - SDN control	Recommendation	2021	[218]
	Y.3806	QKD networks - Requirements for QoS assurance	Recommendation	2021	[465]
	X.1702	Quantum noise random number generator architecture	Recommendation	2019	[466]
	X.1710	Security framework for QKD networks	Recommendation	2020	[467]
	X.1712	Security requirements and measures for QKD networks - Key management	Recommendation	2021	[468]
	X.1714	Key combination and confidential key supply for QKD networks	Recommendation	2020	[469]
	Y.3807	QKD networks - QoS parameters	Recommendation	Drafting	[470]
	Y.3808	Framework for integration of QKD network and secure storage network	Recommendation	Drafting	[471]
	Y.3809	QKD networks - Business role-based models	Recommendation	Drafting	[472]
	Y.QKDN-qos-fa	Functional architecture of QoS assurance for QKD networks	Recommendation	Drafting	[473]
	X.sec-QKDN-tn	Security requirements and designs for QKD networks - Trusted node	Recommendation	Drafting	[474]
	X.sec_QKDN_intrq	Security requirements for integration of QKD networks and secure network infrastructures	Recommendation	Drafting	[475]
	X.sec_QKDN_CM	Security requirements for QKD networks - Control and management	Recommendation	Drafting	[476]
	X.sec_QKDN_AA	Authentication and authorization in QKD networks using quantum safe cryptography	Recommendation	Drafting	[477]
ISO/IEC	CD 23837-1	Security requirements, test and evaluation methods for QKD – Part 1: Requirements	Standard	Drafting	[478]
	CD 23837-2	Security requirements, test and evaluation methods for QKD – Part 2: Evaluation and testing methods	Standard	Drafting	[479]
IETF	draft-irtf-qirg-prin..	Architectural principles for a Qinternet	Internet-draft	2021	[480]
	draft-irtf-qirg-qua..	Applications and use cases for the Qinternet	Internet-draft	2021	[481]
IEEE	P1913	Software-defined quantum communication	Standard	Drafting	[482]
CSA	N/A	Introduction to QKD	Research artifact	2015	[483]

information and communications technology (ICT). In 2017, a study period project was launched in ISO/IEC JTC 1/SC 27 targeting the security requirements, test and evaluation methods of QKD. This project has reached fruition in 2019, based on which a new work item was approved and initiated to develop two-part standards, specifying both the security requirements of QKD [478], as well as the security evaluation and testing methods [479]. Both parts are under development at the time of writing. The standard [478] aims for identifying the potential attacks from the perspective of theoretical model violation, and for characterizing the overall technical requirements, while the standard [479] will provide support for validating the conformity of the security requirements based on the expected security assurance requirements.

D. IETF

The IETF Quantum Internet Research Group (QIRG) was established in 2018 to promote the research on Internet-scale quantum communications. The Internet-draft [480] introduces some of the basic architectural principles of the Qinternet, and outlines the vision of fundamentally enhancing the Internet technology by enabling ultimately secure quantum communications between any two points in the world. As a further advance, the Internet-draft [481] gives an overview of promising applications to be supported by the Qinternet.

E. IEEE

In 2016, IEEE launched a working group to develop a new standard for software-defined quantum communication [482]. This standard intends to specify a software-defined quantum communication protocol for supporting the configuration of quantum-enabled endpoints in a communication network. Such a protocol resides at the application layer of the common Transmission Control Protocol (TCP)/IP model, which will facilitate future integration with the SDN and OpenFlow concepts. The standard [482] will also define some commands for quantum device configuration to enable the control of the transmission, reception, and operation of quantum states. The main objective is to manage the parameters that describe the preparation, measurement, and readout of quantum states.

F. CSA

In 2014, the CSA Quantum-Safe Security Working Group (QSSWG) was launched to identify quantum-safe methods for protecting data across networks in the industrial sector. The goal of this working group is to provide support for the quantum-safe cryptography community in their efforts to protect sensitive data. QKD is one of the salient quantum-safe methods considered by this working group [483].

VIII. On the Road to the Qinternet: Application Scenarios

The QKD network forms a stepping stone on the road to the Qinternet, which plays an essential role in providing long-term security for numerous applications. In this section, we discuss some promising application scenarios relying on QKD networks.

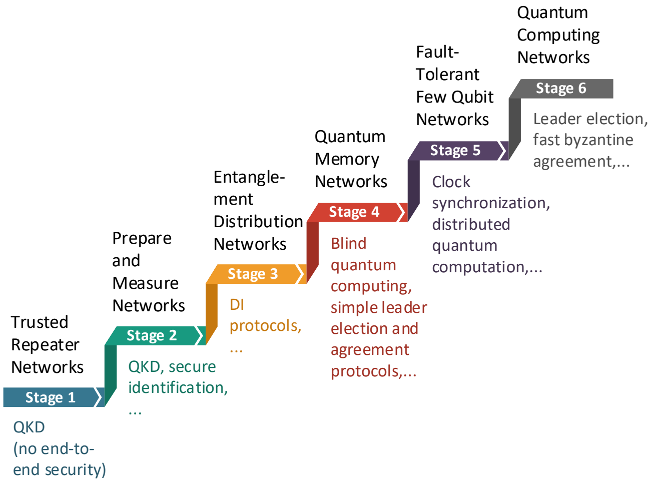

Trusted Repeater Networks
Stage 1
QKD (no end-to-end security)
Prepare and Measure Networks
Stage 2
QKD, secure identification, ...
Entangle-ment Distribution Networks
Stage 3
DI protocols, ...
Quantum Memory Networks
Stage 4
Blind quantum computing, simple leader election and agreement protocols,...
Fault-Tolerant Few Qubit Networks
Stage 5
Clock synchronization, distributed quantum computation,...
Quantum Computing Networks
Stage 6
Leader election, fast byzantine agreement,...

Fig. 32. Stages in the development of a Qinternet [50].

A. First Stage of the Qinternet

The QKD networks relying on trusted relays have evolved from the lab to preliminary real-world applications. It is important to note that these networks only constitute the first stage of the Qinternet [50], as portrayed in Fig. 32. The first stage differs significantly from the evolutionary stages, which cannot achieve the end-to-end transmission of quantum states owing to the absence of quantum repeaters. This stage may incorporate some useful evolutionary components for later stages. QKD networks reaching this stage can be upgraded by replacing some trusted relays with untrusted relays relying on MDI-QKD protocols [430], [436]. Finally, a QKD network relying on quantum repeaters would reach the second stage of the Qinternet featured in Fig. 32. The higher stages include all the functionalities of the previous stages, hence the QKD network can also be regarded as a subset of the future Qinternet.

B. QKD Applications in ICT Systems

Similar to the applications of classic key distribution algorithms routinely employed in ICT systems, QKD can be used in conjunction with well-established protocols to build high-security ICT systems. Following the classic TCP/IP model, these typical protocols are attached to different layers (i.e., link, Internet, transport, and application layers from bottom to top), as illustrated in Fig. 33. By contrast, no universal network stack is available for the Qinternet at the time of writing, which still requires further specifications. Based on the group specification ETSI GS QKD 002 [451], several integration possibilities of QKD into the different layers of ICT systems are described as follows.

1) Link Layer: QKD may be utilized to provide secret keys for the point-to-point protocol (PPP) of [486] and for the IEEE 802.1 media access control security (MACsec) [487]. The PPP is widely used for connecting a pair of nodes over a point-to-point link in the operational computer network. The encryption control protocol (ECP) of [488] is in charge of configuring and enabling the encryption functionality in PPP, while the key agreement may rely on QKD. The IEEE 802.1 MACsec is capable of supporting a connectionless service, which offers data confidentiality, integrity, and authenticity for authorized devices connecting to a local area network or interconnecting local area networks. Explicitly, the MACsec key agreement protocol may be replaced by QKD. Additionally, a point-to-point QKD link that connects a pair of QKD devices can be integrated with a link encryptor for creating a QKD-based link encryptor, which can use the symmetric secret keys generated by QKD in symmetric-key cryptosystems for encrypting the tele-traffic on communication links.

2) *Internet Layer:* QKD may also be readily used as a part of the Internet Protocol Security (IPsec) [489]. The IPsec is a network protocol suite that authenticates and encrypts the IP packets of data for securing communications over an IP network, which is commonly adopted in VPNs. In the IPsec protocol suite, Internet Key Exchange (IKE) [490] is one of the pivotal protocols utilized for establishing a security association. Conventionally, IKE employs a Diffie-Hellman key exchange protocol for setting up a shared session's secret keys. By introducing QKD, IKE may conveniently invoke the shared secret keys derived from QKD for IPsec payload encryption [491].

3) *Transport Layer:* QKD may also be seamlessly integrated with the transport layer security (TLS) protocol of [492] and its predecessor, namely the secure sockets layer (SSL) protocol [493]. The TLS and SSL are popular cryptographic protocols capable of providing end-to-end security for secure communications over a computer network. Before a client and a server can start communicating across a network using the TLS/SSL protocol, they must securely exchange or agree upon a secret key used for encrypting their data. Typically the conventional key exchange/agreement approaches (e.g., RSA and Diffie-Hellman) are utilized in TLS/SSL. In contrast to the conventional classical-domain approaches, QKD holds the promise of supplying the secret keys in a more secure fashion in the future. Hence, QKD may be used in TLS/SSL for enhancing the security of message authentication and encryption.

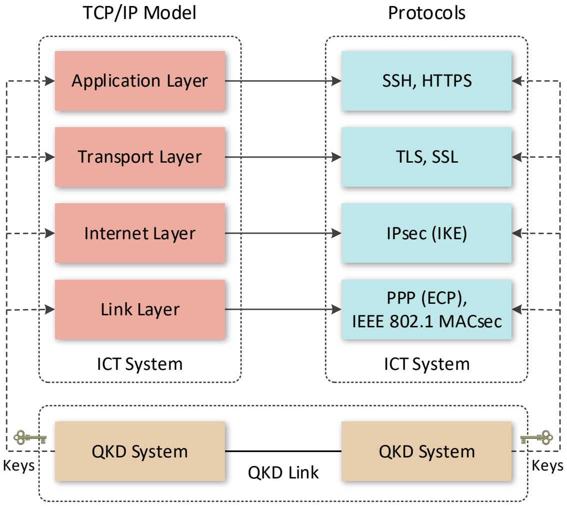


Fig. 33. Application of QKD in ICT systems following the TCP/IP model.

4) *Application Layer:* Numerous applications can use the secret keys generated by QKD for user authentication, message authentication, and service (e.g., voice-only telephone communication and video conference) encryption. Moreover, QKD may also be readily utilized in conjunction with the Diffie-Hellman protocol within secure shell (SSH) sessions for high-security service deployment [433].

C. *Application Areas*

By amalgamating QKD networks and the existing ICT systems, a variety of QKD-protected applications have emerged in diverse many areas. For example, a QKD network is capable of securing the critical links of financial institutions and government agencies. Furthermore, a QKD link has been deployed in sporting events such as the 2010 FIFA World Cup [169]. Some typical application areas of QKD networks are depicted in Fig. 34 and described in the following paragraphs.

1) *Finance and Banking:* The financial industry, especially the banking industry, handles a significant amount of highly sensitive and valuable data, such as transactions, client data and proprietary information, and so on. QKD enables financial and banking institutions to protect their data for ultimate and future-proof security. In 2004, the first QKD-secured bank transfer took place between the headquarters of an Austrian bank and the Vienna City Hall [494], where secret keys were distributed on demand between the two sites via a QKD system. In [495], a scenario of using QKD within IPsec for securing the critical financial transactions in Switzerland was described and analyzed. The financial institutions in Switzerland have also employed commercial QKD systems for securing their networks for disaster recovery. Based on the existing QKD networks, many Chinese banks have implemented QKD-secured data transfer as well as the online banking and transactions for enterprise users [46], [185]. Considering that authentication in online banking systems is potentially vulnerable to attacks such as phishing, QKD can be adopted to enhance the standard authentication in online banking systems [496]. At the time of writing, the Dutch bank is preparing to use MDI-QKD for providing ultra-secure connections.

2) *Governments and Defense:* Of all entities, governments and defense agencies have the longest-lasting data security requirements, stretching for decades in the case of official secrets. QKD can offer long-term data security for governments and defense agencies to guarantee their data sovereignty. Generally, a dedicated security system (e.g., VPN) is utilized in a government or defense agency to provide a high level of data confidentiality, integrity, and authenticity for their communications systems. In 2007, the Swiss government successfully applied QKD for securing a dedicated line used to count the ballots of national elections [497]. In [498], a QKD-based voting scheme protected against

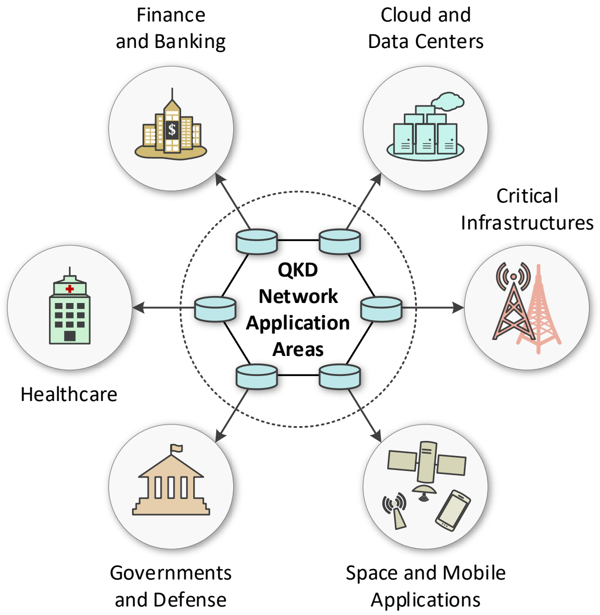


Fig. 34. Various application areas of QKD networks.

man-in-the-middle attacks has been presented. Furthermore, a QKD metropolitan network constructed in Jinan [30], [46], [153] has been used by numerous government employees to protect their secrets. Similarly, a government QKD network is being implemented to secure intra-governmental communications in the Australian capital Canberra. Finally, several studies have reported on the application of QKD for enhancing the security of VPNs [499], [500].

3) Cloud and Data Centers: Huge amounts of highly confidential data are stored in the cloud and data centers. As more and more organizations use the cloud and data centers to backup, store, and recover data, ensuring data privacy and security has become of paramount importance. Given that conventional security solutions will soon become vulnerable to the threats posed by quantum computing, QKD has the potential of increasing the security of cloud data protection and data center interconnection. In the Netherlands, a QKD link has been demonstrated to secure the data transfer between the Siemens data centers in The Hague and Zoetermeer [501], while KPN has implemented end-to-end QKD in its network between the KPN data centers in The Hague and Rotterdam [502]. In China, the Beijing-Shanghai QKD network [46], [181] has been used for securing the data center backup between Beijing and Shanghai. In the sector of corporate cloud security applications, several companies such as Acronis and Alibaba are also applying quantum-safe encryption to cloud data protection [503]. With respect to the application of QKD for cloud computing, a series of problems have been addressed, covering access control [504], authentication [505], data and privacy security [506], cloud containers [507], as well as cloud storage and data dynamics [508].

4) Critical Infrastructures: A critical national infrastructure supports the essential services that underpin society, which contains a number of sectors, such as energy, transport, and telecom. The threats (e.g., malicious data tampering and service outages) inflicted upon the critical infrastructures may cause economic damage as well as disruption to both corporate and national services. As a remedy to these threats, QKD holds the potential of providing long-term protection and forward secrecy for the critical infrastructures. The application of QKD networks for protecting the energy grid is being investigated by several institutions, such as the State Grid Corp of China as well as the Oak Ridge and Los Alamos National Labs, with the objective of ensuring safe and stable operation of the entire energy grid. Meanwhile, some telecom operators and service providers (e.g., Telefónica, China Telecom, and British Telecom) around the world are studying the feasibility of integrating QKD systems with the existing fiber infrastructures for securing data transfer across their telecoms networks. Moreover, QKD can be readily utilized for enhancing the security of aeronautical telecommunication networks [509]. An architecture of network-centric quantum communications has been applied for the protection of critical infrastructures, as detailed in [198], whereas the application of QKD for multi-source data security protection of the smart grid has been discussed in [510].

5) Healthcare: Healthcare organizations also require highly reliable networks for the transmission of sensitive information, such as patient records, including names, addresses, dates of birth, social security records, and clinical records. However, without protection, the transmission of sensitive information across networks is at risk from cyber-attacks. Such cyber-attacks may affect patients (e.g., threatening their personal information and health) and cause significant financial and credit losses for healthcare organizations. In the near future era of quantum computing, QKD can be used by healthcare organizations for protecting their data in both the current and future security landscape. To protect the sensitive data relevant to human genomes and health throughout its lifetime, a storage system based on QKD has been presented in [511], which has exceptional storage longevity. As a further application of QKD for offering both storage and access security concerning personal health records in a cloud environment has been investigated in [512]. In 2020, Toshiba and ToMMo reported on the successful demonstration of real-time transmission of genome sequence data secured by QKD [513], validating the practical applications of QKD not only in the fields of genomic research and but also in genomic medicine.

6) Space and Mobile Applications: Space and mobile applications that enable multiple users to seamlessly access networks can also benefit from the ultimate future-proof security provided by QKD. Accordingly, the application of QKD is promising to cover the entire globe, including both fiber as well as wireless terrestrial and satellite networks. With respect to space communications, QKD can be adopted for securing access to a satellite, as well as for communications between ground stations, and for satellite-to-satellite communications [514]. In this regard, a series of projects dedicated to space-based quantum communications have been announced in [196]. Moreover, an intercontinental video conference was held between China and Austria [48], relying on the combination of a satellite-based QKD network with fiber-based QKD metropolitan networks. As a further development, the application of QKD for securing smartphones in a multiuser mobile network has been implemented by harnessing the Tokyo QKD network [206], [511], [515]. The integration of QKD into wireless networks has been analyzed in [516], whereas a QKD system using optical wireless communication links for telephone networks has been studied in [517]. In particular, a commercial QKD-enhanced mobile phone has been developed by QuantumCTek in collaboration with ZTE [518], while China Telecom and QuantumCTek are jointly promoting the development of quantum encrypted phone calls relying on a special SIM card and smartphone app [519]. From the perspective of mobile network infrastructures, an experiment demonstrating the feasibility of QKD-secured inter-domain fifth generation (5G) service orchestration has been performed [520], while a field trial of dynamic QKD networking relying on the Bristol city 5GUK test network has been reported on in [127]. In [521], QKD-assisted 5G network slicing has been demonstrated. Moreover, a QKD network testbed is being developed in Eindhoven to provide quantum encryption as a service on demand for maintaining ultimate end-to-end security, which will have connections both to optical access networks and to 5G testbeds [138].

IX. Future Research Directions

This survey paves the way for the interdisciplinary cross-community dialogue on architecting the Qinternet, and reveals that QKD networks have a huge potential in terms of providing future-proof security for compelling applications and open interesting new perspectives. In this section, we discuss a range of open topics on QKD networks and beyond for future research, as illustrated at a glance in Fig. 35.

A. *QKD Network Itself*

In addition to the above subjects, there are numerous open challenges in the research and popularization of QKD networks, some of which are outlined as follows.

1) Network Coding: Network coding [522] has been widely analyzed in the context of classical networks, but a range of specific problems should be addressed to enable network coding to be exploited in QKD networks. The reliance on the trusted relays in QKD networks can be alleviated with the aid of network coding [299], which can assist in multicasting secret keys from multiple transmitters to multiple receivers [523]. This would pave the way for realistic public multi-user QKD systems [524]. In particular, a novel network coding paradigm, termed as quantum network coding, has been proposed in [525], but most studies still only focus on its theoretical aspects [526]–[530]. A particularly promising area of research is to conceive solutions for all low trust-levels of the relays, such as the trusted relays seen in Fig. 7, as well as for different quantum memory requirements in supporting the evolutionary development of the Qinternet.

2) Performance Enhancement: To provide forward secrecy and long-term protection for more and more users across the future Qinternet, the performance of QKD networks has to be enhanced. Extending the distance and increasing the secret-key rate of QKD networks would require the invention of new QKD protocols and devices. Notably, the TF-QKD [107] and PM-QKD [108] protocols hold the promise of overcoming the rate-distance limit of the existing point-to-point QKD protocols, whereas chip-based QKD combined with integrated photonic devices enables the large-scale practical deployment of QKD [329]. Both the recently invented QKD protocols and devices need further research for facilitating their implementation in practical QKD networks. On the theoretical front, the mathematical models of QKD networks also require further investigations in order to accurately describe and evaluate the performance of practical QKD networks having heterogeneous topologies and QKD protocols [531], [532]. Specifically, a sophisticated QKD network that supports the reconfiguration of devices to support diverse QKD protocols will potentially improve the agility and flexibility as well as compatibility of QKD networks [533]. Moreover, the integration of QKD with existing optical networks requires performance enhancements to facilitate the roll-out of QKD networks [436], while the family of satellite-constellation based QKD networks also has to be further explored for constructing global QKD networks.

3) Testing and Verification: The main characteristics of practical QKD networks have been reported by the QKD device vendors and network operators themselves. However, hitherto no official testing and verification schemes specific to QKD networks have been devised. Walenta *et al.* [426] described a suite of alternative options to enable QKD network

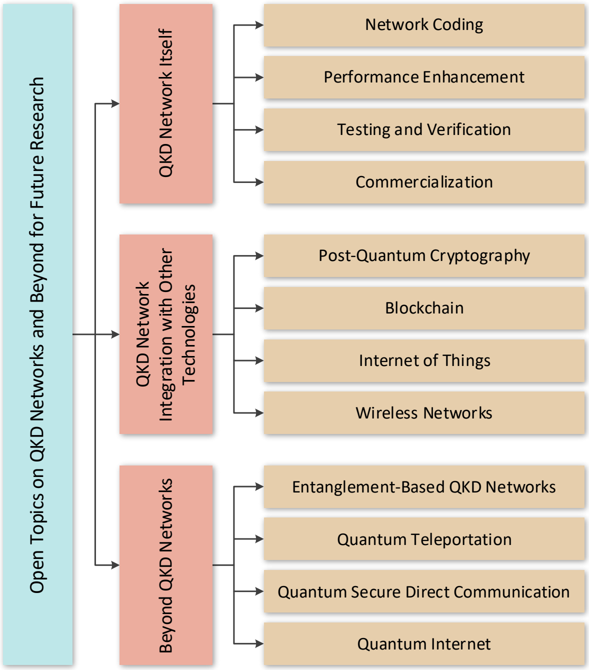


Fig. 35. Open topics on QKD networks and beyond for future research.

devices to be compliant with well-established security certification standards. The group specification ETSI GS QKD 011 [455] has outlined the measurement methods to be used for various parameters of the individual components in QKD systems. Naturally, guaranteeing the validity and impartiality of testing and verification for QKD networks is a vitally important issue. Hence widely ratified uniform testing and verification standards, instruments, and platforms have to be developed for different QKD networks. Ideally, an independent evaluation facility should be established for conducting tests on QKD networks under different conditions and validate the functionalities claimed by the network providers.

4) Commercialization: At the time of writing, a variety of commercial QKD devices are available and many practical QKD networks have been deployed. Nonetheless, the establishment and commercialization of QKD networks using commercial QKD devices still face countless obstacles. Battelle [534] has compared custom-built and commercial QKD systems in a controlled laboratory environment, with the objective of characterizing the performance attained in real-world metropolitan and long-haul environments. The family of handheld mobile QKD devices [535] still requires further research for commercialization. Moreover, the implementation security of QKD networks is one of the major obstacles in the way of wide-spread commercialization, since an attacker might maliciously use the imperfections of the QKD network to paralyze it. Thus, sophisticated countermeasures should be continuously invented and updated to guard against the implementation loopholes in order to widely roll out secure QKD networks in commercial public environments.

B. QKD Network Integration with Other Technologies

We briefly mention here some of the research topics on QKD network integration with other advanced technologies, which are of particular interest to the multidisciplinary research and engineering communities.

1) Post-Quantum Cryptography: Besides QKD networks, post-quantum cryptography is another potential approach to provide quantum-safe security [14]–[19], which relies on algorithms that have been proven to be safe against known quantum attacks. Given that the post-quantum algorithms are implemented entirely in software, post-quantum cryptography has the advantage of being compatible with existing security platforms. In reality, QKD currently cannot replicate all the functions of conventional cryptosystems. The post-quantum cryptography and QKD solutions constitute a pair of parallel research directions, neither of which has yet found widespread application in practice. In the immediate future, post-quantum cryptography is expected to be integrated with QKD [27], [536] for constructing an intrinsically amalgamated security platform for quantum-safe cryptosystems.

2) Blockchain: A blockchain constitutes a distributed and public ledger platform, which promotes reaching a consensus in a large decentralized network of parties who do not trust each other. Blockchain ledgers may consist of almost anything of value, such as identities, loans, land titles, and logistics manifests. One of the most prominent applications of blockchain is cryptocurrency, e.g., Bitcoin [537]. Although blockchain is traditionally considered secure, it is vulnerable to attacks from quantum computers [538]. Several studies have focused on post-quantum blockchain solutions [539]–[541] conceived for securing the blockchain with the aid of post-quantum cryptography. On the other hand, QKD is a promising technique of tackling the special challenges facing blockchain in the quantum era. The feasibility of establishing a quantum-safe blockchain platform based on QKD for providing authentication has been demonstrated in an urban QKD network [542]. Furthermore, a framework of quantum-secured permissioned blockchain relying on adopting a QKD-based digital signature scheme has been presented in [543]. Therefore, how to integrate QKD networks with blockchain to build a highly secure blockchain platform has become an inspirational research topic.

3) Internet of Things: The Internet of Things (IoT) is constituted by a giant network of connected things or objects, in which all physical objects are connected to the classical Internet and exchange data through network devices or routers. The IoT will become an integral part of our daily lives in the near future. However, many serious concerns have been raised about its security and privacy risks. Indeed, a highly robust cryptosystem is required for IoT. The post-quantum IoT concept has been envisioned by incorporating post-quantum cryptography into the IoT for securing IoT systems against the impending known attacks by quantum computing, which has become an active area in IoT research [544]–[551]. By contrast, the quantum IoT combining quantum cryptography (especially QKD) with the IoT requires more research attention, given that it is in its infancy [552]–[555]. The integration of QKD networks with IoT provides a solid foundation for securing the IoT in the quantum world.

4) Wireless Networks: To date, most practical QKD networks have used wired links (i.e., optical fibers) and nodes at fixed physical locations. In addition to quantum-assisted wireless communications that exploit the computing power offered by quantum computing to improve the performance of wireless systems [556], some preliminary studies suggested that QKD is capable of providing a high level of security for users and services in next-generation wireless networks [127], [138], [520], [557]–[559]. Inspired by the progress in the field of free-space QKD and mobile terminals, such as quantum-aided satellites [75] and quantum-aided drones [560]–[562], wireless/mobile QKD has become a valuable research direction. For example, the feasibility of wireless QKD in indoor environments has been studied by the authors of [563]. Additionally, the feasibility of QKD operating in the Terahertz regime over short distances has also been explored [564]. In reality, QKD is capable of replacing classical key negotiation algorithms (e.g., Diffie-Hellman algorithm [10]) used in wireless scenarios such as IoT and mobile. Both offline and online secret-key generation using QKD are possible for wireless networks. The former option has been reported in [518], [519]. More concretely, a microSD can access the QKD network offline through a secret-key charger and be installed in the mobile phone or IoT device. Then the secret keys in the microSD can be used for securing wireless communications. On the other hand, online secret-key generation demands further research on QKD over wireless channels, since it is still in its infancy.

C. *Beyond QKD Networks*

Beyond practical QKD networks, we turn our attention to future quantum networks that have not as yet been rolled out in practice and require further cutting-edge research.

1) Entanglement-Based QKD Networks: Entanglement is one of the most extraordinary features in the quantum world [565], with many applications in the field of quantum information science, such as QKD and quantum teleportation [566]. Entanglement-based QKD has bright prospects for future applications, since it has the potential of providing DI security potentially leading to a global quantum repeater based QKD network. At the time of writing, only a handful of entanglement-based QKD experiments have been carried out, as exemplified by optical fiber [567], free space [568], and satellite [324] based studies. Moreover, entanglement distribution in optical networks has been studied theoretically in [569] and experimentally demonstrated in [570]. The feasibility of entanglement-based metropolitan QKD networks has been confirmed by the field trial of [165]. Despite the technical advances in entanglement-based networks [571]–[573], further long-term efforts are required for a fully entanglement-based QKD network to reach a commercial level of maturity for practical services. The essential hardware such as quantum processors and quantum memory must be further developed in support of fully entanglement-based QKD networks.

2) Quantum Teleportation: Quantum teleportation [566] enables unknown quantum states to be faithfully transferred between distant nodes over long distances in a network. Long-distance quantum teleportation underlies the realization of global quantum communications and large-scale quantum networks [37], [574]. The experiments based on long-distance quantum teleportation through both optical fiber and free space have been reviewed in [575]. Quantum teleportation has also been demonstrated both in the context of metropolitan networks [576], [577] and quantum satellites [578]. Although a number of technologies have been developed for quantum teleportation implementations in quantum networks [135], [575], [579], the future progress in real-world applications of reliable long-distance quantum teleportation is required.

3) Quantum Secure Direct Communication: In addition to QKD and quantum teleportation, quantum secure direct communication (QSDC) [580], [581] is another extremely promising branch of quantum communication, in which secret messages are transmitted directly over a quantum channel without key distribution. The secure direct nature of QSDC makes it an important cryptographic primitive for constructing the protocols of quantum direct secret sharing [582], [583], quantum signature [584], and quantum dialogue [585], [586]. Numerous promising QSDC protocols have been proposed [580], [587]–[590], some of which have also been experimentally implemented [591] and demonstrated in QSDC networks [592]. To elaborate a little further, apart from its ultimate security, the convincing benefit of QSDC is that it is a truly quantum-domain protocol.

4) Quantum Internet: QKD has many applications over the classical Internet [593], [594]. In order to accomplish some tasks that are impossible by using purely classical information within the classical Internet, a vision of the Qinternet [51] has been presented, which can interconnect quantum information processors through quantum channels for supporting radical applications that are out of reach for the classical Internet. A technical roadmap for developing the full-blown Qinternet has been proposed in [50], where the initial developmental stage is the construction of QKD networks. In recent years, the Qinternet has attracted more and more research attention [55], [68], [406], [408], [530], [595]–[600]. Given that the Qinternet is still in its infancy and it is difficult to predict all its applications, substantial further research is required for making the Qinternet a reality. Suffice to say however that before large-scale quantum computers become available, the Qinternet would allow us to construct parallel quantum computers linked up by it.

X. Design Guidelines and a Brief Summary

A. *Trade-Offs in QKD Networks*

As a communication network capable of providing secret keys as a service, QKD networks also have some characteristics reminiscent of those of classical communication networks, such as modulation, transmission, detection, and post-processing. Accordingly, it has to comply with the basic requirements of flexible expansion, cost efficiency and

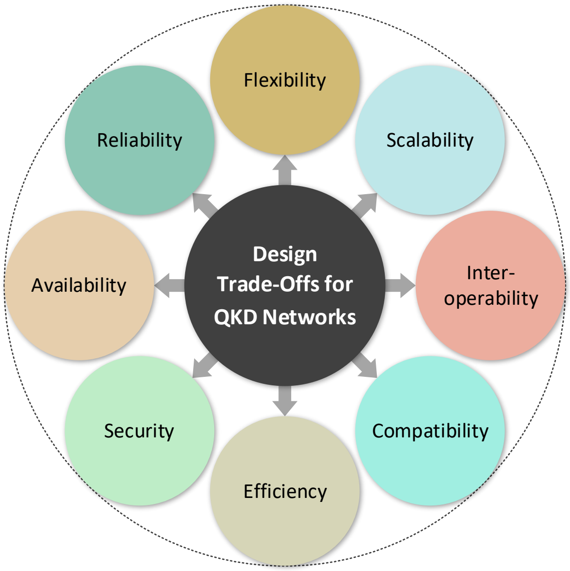


Fig. 36. Design trade-offs for QKD networks.

component compatibility. However, the services provided by QKD networks differ from those of classical communication networks in that they provide random secret keys rather than conveying classical messages. As a result, QKD networks also have to meet many secret key generation requirements for maintaining a high security level, in support of cryptographic applications. As shown in Fig. 36, the holistic design of QKD networks has to take the following fundamental requirements into consideration.

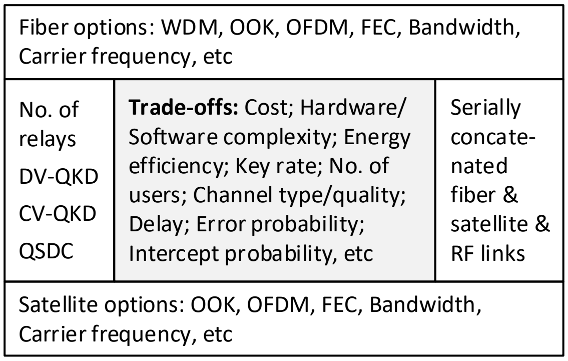
- *Availability:* The QKD network relies on an adaptive API [222] that can deliver the requested secret keys to multiple users. It also has to use the secret keys produced to provide a security guarantee anywhere and anytime for various ICT applications in numerous fields [451].
- *Reliability:* The QKD network has to support protection and restoration schemes [414], [416] that are robust to node or link failures, where prompt and accurate fault localization and recovery should be provided to ensure service continuity without eroding the user experience. Moreover, it has to maintain long-term stability [45], [180] so that the secret keys can be produced reliably.
- *Flexibility:* The QKD network has to be flexible enough to fulfil the diverse requirements of users [204]–[207], [601], [602], in terms of offering differentiated QoS [212] and flexible charging policies. It also has to be capable of supporting flexible control and management of the entire network, for example by using SDN techniques [126], [127], [163].
- *Scalability:* The QKD network is required to support smooth network expansion, upgrade, and reconfiguration [168], [241] according to the needs of its growing user population. It also has to have the capability of supporting diverse network topologies, such as the ring [47], [155], star [143], [148], [150], [158] and mesh [127], [157] structures of short-range, metropolitan and long-haul QKD networks.
- *Security:* The QKD network is expected to adopt QKD protocols having strict security proofs [28], [33], [452], and support efficient countermeasures against quantum hacking attacks [31], whilst complying with the relevant security standards and certifications.
- *Efficiency:* The QKD network has to support efficient end-to-end QKD-based connections [603], physical-layer resource scheduling [377], and secret-key assignment [200] according to diverse user requirements and network loads. Specifically, it is expected to have a high secret-key throughput and low latency to fulfil the demanding security requirements of users.
- *Compatibility:* Ideally, it should support the co-fiber transmission of the quantum and classical signals [47], [127], [128], [178], [182] in order to reduce costs. The pervasive legacy networks can provide abundant fiber resources for QKD networks, hence integrating QKD with legacy networks is one of the top priorities in facilitating the deployment and increasing the popularity of QKD. The long-term evolution of a QKD network should also be able to accommodate hitherto unknown new cryptographic functions and quantum technologies, while supporting backwards compatibility with the existing infrastructure.
- *Interoperability:* The QKD network must be able to accommodate multi-vendor QKD devices and networking devices [43], [44]. Specifically, it should be capable of achieving interoperability with heterogeneous devices developed by different vendors. With the evolution of QKD protocols and devices, a large-scale QKD network will consist of multi-protocol QKD systems in the future, where various QKD protocols may be used in different QKD systems. Hence, it is highly desirable for QKD networks to achieve interoperability of different QKD protocols.

B. *Design Guidelines*

All stages of the Qinternet's evolution introduced in Section VIII are subject to the generic trade-offs briefly touched upon in Section X-A. Against this generic backdrop, here we provide a few design guidelines for the first stage of the Qinternet's roadmap seen in Fig. 32, namely for the family of QKD networks without quantum repeaters by considering the cost, distance, key rate, channel type and quality, system complexity and the number of users, for example. It is plausible that the designer has to strike a trade-off among these typically conflicting metrics, as portrayed at a glance in Fig. 37.

The designer has to start from collecting as many of the basic metrics and constraints listed in the central core of Fig. 37 as possible and then follow an iterative design procedure reminiscent of the following steps.

1) Using the costing guidelines of QKD networks, narrow down the design options of Fig. 37.
2) The evolution of optical OFDM systems was documented in [604] and these guidelines may be used for designing the optical quantum links.
3) The broad design guidelines of the associated forward error correction (FEC) schemes may be inferred from [605].
4) It is vitally important to harmonize the bit error rate (BER) of the quantum link and of the classical link to avoid that the high BER of one of them results in an outage of the



<table>
<tr><td colspan="3">Fiber options: WDM, OOK, OFDM, FEC, Bandwidth, Carrier frequency, etc</td></tr>
<tr><td>No. of relays
DV-QKD
CV-QKD
QSDC</td><td><b>Trade-offs:</b> Cost; Hardware/ Software complexity; Energy efficiency; Key rate; No. of users; Channel type/quality; Delay; Error probability; Intercept probability, etc</td><td>Serially concate-nated fiber & satellite & RF links</td></tr>
<tr><td colspan="3">Satellite options: OOK, OFDM, FEC, Bandwidth, Carrier frequency, etc</td></tr>
</table>

Fig. 37. Design guidelines for QKD networks without quantum repeaters.

entire system.

5) Given the key rate vs. distance trade-off, it is plausible that this directly affects the cost and the number of relays. To elaborate a little further, given a certain source-destination distance, we can harness more relays for reducing the propagation distance and hence increase the key rate, but only at an increased cost and relaying delay. Indeed, a whole host of similarly intricate trade-offs may be inferred by carefully scrutinizing Fig. 37, which are left for you to explore valued colleague.

C. Summary

The QKD networks are capable of providing long-term data protection and future-proof security for numerous applications, but they have numerous open problems as well. This survey provides a comprehensive overview of the past achievements complemented by a broad research outlook on QKD networks. We commenced by a rudimentary introduction of the QKD mechanism, its implementation options, and protocols. Then, we categorized the QKD network implementation options and reviewed the development of QKD network implementations, covering short-range, metropolitan, and long-haul QKD networks. Subsequently, we described the general QKD network architecture, its elements, as well as its interfaces and protocols. Furthermore, we conducted an in-depth survey of the diverse enabling techniques both in the physical and network layers. Moreover, we outlined the associated standardization efforts as well as the application scenarios. Finally, we rounded off the paper by discussing a suite of promising future research directions on QKD networks, which constitute the initial stage of developing the Qinternet of the future. We believe that QKD networks will attract more and more attention from both academia and industry. A number of academic and engineering efforts across the fields of physics, computer science, security, and communications will be required to progress the all-round development of QKD networks. Our hope is that both researchers and practitioners might find intellectual stimulation in consulting this treatise – please join this multi-disciplinary research effort valued colleague.

References

[1] T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, and J. L. O'Brien, "Quantum computers," *Nature*, vol. 464, no. 7285, pp. 45–53, Mar. 2010.

[2] S. Debnath, N. M. Linke, C. Figgatt, K. A. Landsman, K. Wright, and C. Monroe, "Demonstration of a small programmable quantum computer with atomic qubits," *Nature*, vol. 536, no. 7614, pp. 63–66, Aug. 2016.

[3] B. Lekitsch, S. Weidt, A. G. Fowler, K. Mølmer, S. J. Devitt, C. Wunderlich, and W. K. Hensinger, "Blueprint for a microwave trapped ion quantum computer," *Sci. Adv.*, vol. 3, no. 2, Feb. 2017, Art. no. e1601540.

[4] L. R. Schreiber and H. Bluhm, "Toward a silicon-based quantum computer," *Science*, vol. 359, no. 6374, pp. 393–394, Jan. 2018.

[5] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. S. L. Brandao, D. A. Buell, B. Burkett, Y. Chen, Z. Chen, B. Chiaro, R. Collins, W. Courtney, A. Dunsworth, E. Farhi, B. Foxen, A. Fowler, C. Gidney, M. Giustina, R. Graff, K. Guerin, S. Habegger, M. P. Harrigan, M. J. Hartmann, A. Ho, M. Hoffmann, T. Huang, T. S. Humble, S. V. Isakov, E. Jeffrey, Z. Jiang, D. Kafri, K. Kechedzhi, J. Kelly, P. V. Klimov, S. Knysh, A. Korotkov, F. Kostritsa, D. Landhuis, M. Lindmark, E. Lucero, D. Lyakh, S. Mandrà, J. R. McClean, M. McEwen, A. Megrant, X. Mi, K. Michielsen, M. Mohseni, J. Mutus, O. Naaman, M. Neeley, C. Neill, M. Y. Niu, E. Ostby, A. Petukhov, J. C. Platt, C. Quintana, E. G. Rieffel, P. Roushan, N. C. Rubin, D. Sank, K. J. Satzinger, V. Smelyanskiy, K. J. Sung, M. D. Trevithick, A. Vainsencher, B. Villalonga, T. White, Z. J. Yao, P. Yeh, A. Zalcman, H. Neven, and J. M. Martinis, "Quantum supremacy using a programmable superconducting processor," *Nature*, vol. 574, no. 7779, pp. 505–510, Oct. 2019.

[6] H.-S. Zhong, H. Wang, Y.-H. Deng, M.-C. Chen, L.-C. Peng, Y.-H. Luo, J. Qin, D. Wu, X. Ding, Y. Hu, P. Hu, X.-Y. Yang, W.-J. Zhang, H. Li, Y. Li, X. Jiang, L. Gan, G. Yang, L. You, Z. Wang, L. Li, N.-L. Liu, C.-Y. Lu, and J.-W. Pan, "Quantum computational advantage using photons," *Science*, vol. 370, no. 6523, pp. 1460–1463, Dec. 2020.

[7] M. Gong, S. Wang, C. Zha, M.-C. Chen, H.-L. Huang, Y. Wu, Q. Zhu, Y. Zhao, S. Li, S. Guo, H. Qian, Y. Ye, F. Chen, C. Ying, J. Yu, D. Fan, D. Wu, H. Su, H. Deng, H. Rong, K. Zhang, S. Cao, J. Lin, Y. Xu, L. Sun, C. Guo, N. Li, F. Liang, V. M. Bastidas, K. Nemoto, W. J. Munro, Y.-H. Huo, C.-Y. Lu, C.-Z. Peng, X. Zhu, and J.-W. Pan, "Quantum walks on a programmable two-dimensional 62-qubit superconducting processor," *Science*, vol. 372, no. 6545, pp. 948–952, May 2021.

[8] "Quantum Safe Cryptography and Security," ETSI White Paper No. 8, June 2015 [Online]. Available: https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf.

[9] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[10] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, Nov. 1976.

[11] V. S. Miller, "Use of elliptic curves in cryptography," in *Proc. Conf. Theory Appl. Crypt. Tech.*, Santa Barbara, CA, USA, Aug. 1985, pp. 417–426.

[12] N. Koblitz, "Elliptic curve cryptosystems," *Math. Comput.*, vol. 48, no. 177, pp. 203–209, Jan. 1987.

[13] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. 35th Annu. Symp. Found. Comput. Sci.*, Santa Fe, NM, USA, Nov. 1994, pp. 124–134.

[14] D. J. Bernstein, J. Buchmann, and E. Dahmen, *Post-Quantum Cryptography*, Berlin, Heidelberg: Springer, 2009.

[15] D. J. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*, vol. 549, no. 7671, pp. 188–194, Sept. 2017.

[16] "The State of Post-Quantum Cryptography," CSA Quantum-Safe Security Working Group, May 2018 [Online]. Available: https://cloudsecurityalliance.org/artifacts/the-state-of-post-quantum-cryptography/.

[17] N. Sendrier, "Code-based cryptography: State of the art and perspectives," *IEEE Secur. Priv.*, vol. 15, no. 4, pp. 44–50, Aug. 2017.

[18] D. Butin, "Hash-based signatures: State of play," *IEEE Secur. Priv.*, vol. 15, no. 4, pp. 37–43, Aug. 2017.

[19] H. Nejatollahi, N. Dutt, S. Ray, F. Regazzoni, I. Banerjee, and R. Cammarota, "Post-quantum lattice-based cryptography implementations: A survey," *ACM Comput. Surv.*, vol. 51, no. 6, Feb. 2019, Art. no. 129.

[20] J. Ding and A. Petzoldt, "Current state of multivariate cryptography," *IEEE Secur. Priv.*, vol. 15, no. 4, pp. 28–36, Aug. 2017.

[21] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput. Syst. Signal Process.*, Bangalore, India, Jan. 1984, pp. 175–179.

[22] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145–195, Mar. 2002.

[23] J. Buchmann, J. Braun, D. Demirel, and M. Geihs, "Quantum cryptography: A view from classical cryptography," *Quantum Sci. Technol.*, vol. 2, no. 2, May 2017, Art. no. 020502.

[24] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in quantum cryptography," *Adv. Opt. Photonics*, vol. 12, no. 4, pp. 1012–1236, Dec. 2020.

[25] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, Oct. 1982.

[26] M. J. W. Hall, "Information exclusion principle for complementary observables," *Phys. Rev. Lett.*, vol. 74, no. 17, pp. 3307–3311, Apr. 1995.

[27] L.-J. Wang, K.-Y. Zhang, J.-Y. Wang, J. Cheng, Y.-H. Yang, S.-B. Tang, D. Yan, Y.-L. Tang, Z. Liu, Y. Yu, Q. Zhang, and J.-W. Pan, "Experimental authentication of quantum key distribution with

post-quantum cryptography," *npj Quantum Inf.*, vol. 7, May 2021, Art. no. 67.

[28] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, no. 3, pp. 1301–1350, Sept. 2009.

[29] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," *npj Quantum Inf.*, vol. 2, Nov. 2016, Art. no. 16025.

[30] Q. Zhang, F. Xu, Y.-A. Chen, C.-Z. Peng, and J.-W. Pan, "Large scale quantum key distribution: Challenges and solutions [Invited]," *Opt. Express*, vol. 26, no. 18, pp. 24260–24273, Sept. 2018.

[31] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, "Secure quantum key distribution with realistic devices," *Rev. Mod. Phys.*, vol. 92, no. 2, May 2020, Art. no. 025002.

[32] H.-K. Lo and H. F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," *Science*, vol. 283, no. 5410, pp. 2050–2056, Mar. 1999.

[33] H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nature Photon.*, vol. 8, no. 8, pp. 595–604, Aug. 2014.

[34] G. S. Vernam, "Cipher printing telegraph systems for secret wire and radio telegraphic communications," *Trans. Am. Inst. Electr. Eng.*, vol. XLV, pp. 295–301, Jan. 1926.

[35] C. E. Shannon, "Communication theory of secrecy systems," *The Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[36] "Advanced Encryption Standard (AES)," FIPS PUB 197, Nov. 2001.

[37] N. Gisin and R. Thew, "Quantum communication," *Nature Photon.*, vol. 1, no. 3, pp. 165–171, Mar. 2007.

[38] ID Quantique [Online]. Available: https://www.idquantique.com.

[39] QuantumCTek [Online]. Available: http://www.quantum-info.com/English/.

[40] Toshiba QKD System [Online]. Available: https://www.toshiba.eu/pages/eu/Cambridge-Research-Laboratory/toshiba-qkd-system.

[41] J. Qiu, "Quantum communications leap out of the lab," *Nature*, vol. 508, no. 7497, pp. 441–442, Apr. 2014.

[42] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, "Current status of the DARPA quantum network," *Proc. SPIE, Quantum Inf. Comput. III*, vol. 5815, pp. 138–149, May 2005.

[43] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden, and A. Zeilinger, "The SECOQC quantum key distribution network in Vienna," *New J. Phys.*, vol. 11, no. 7, July 2009, Art. no. 075001.

[44] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger, "Field test of quantum key distribution in the Tokyo QKD network," *Opt. Express*, vol. 19, no. 11, pp. 10387–10409, May 2011.

[45] D. Stucki, M. Legré, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, P. Monbaron, L. Monat, J.-B. Page, D. Perroud, G. Ribordy, A. Rochas, S. Robyr, J. Tavares, R. Thew, P. Trinkler, S. Ventura, R. Voirol, N. Walenta, and H. Zbinden, "Long-term performance of the SwissQuantum quantum key distribution network in a field environment," *New J. Phys.*, vol. 13, no. 12, Dec. 2011, Art. no. 123001.

[46] Y.-A. Chen, "Large-scale quantum network: From intra-city to inter-city to global," in *Proc. 8th Int. Conf. Quantum Crypt.*, Shanghai, China, Aug. 2018.

[47] J. F. Dynes, A. Wonfor, W. W.-S. Tam, A. W. Sharpe, R. Takahashi, M. Lucamarini, A. Plews, Z. L. Yuan, A. R. Dixon, J. Cho, Y. Tanizawa, J.-P. Elbers, H. Greißer, I. H. White, R. V. Penty, and A. J. Shields, "Cambridge quantum network," *npj Quantum Inf.*, vol. 5, Nov. 2019, Art. no. 101.

[48] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, F.-Z. Li, J.-F. Wang, Y.-M. Huang, L. Deng, T. Xi, L. Ma, T. Hu, L. Li, N.-L. Liu, F. Koidl, P. Wang, Y.-A. Chen, X.-B. Wang, M. Steindorfer, G. Kirchner, C.-Y. Lu, R. Shu, R. Ursin, T. Scheidl, C.-Z. Peng, J.-Y. Wang, A. Zeilinger, and J.-W. Pan, "Satellite-relayed intercontinental quantum network," *Phys. Rev. Lett.*, vol. 120, no. 3, Jan. 2018, Art. no. 030501.

[49] Y.-A. Chen, Q. Zhang, T.-Y. Chen, W.-Q. Cai, S.-K. Liao, J. Zhang, K. Chen, J. Yin, J.-G. Ren, Z. Chen, S.-L. Han, Q. Yu, K. Liang, F. Zhou, X. Yuan, M.-S. Zhao, T.-Y. Wang, X. Jiang, L. Zhang, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, C.-Y. Lu, R. Shu, J.-Y. Wang, L. Li, N.-L. Liu, F. Xu, X.-B. Wang, C.-Z. Peng, and J.-W. Pan, "An integrated space-to-ground quantum communication network over 4,600 kilometres," *Nature*, vol. 589, no. 7841, pp. 214–219, Jan. 2021.

[50] S. Wehner, D. Elkouss, and R. Hanson, "Quantum internet: A vision for the road ahead," *Science*, vol. 362, no. 6412, Oct. 2018, Art. no. eaam9288.

[51] H. J. Kimble, "The quantum internet," *Nature*, vol. 453, no. 7198, pp. 1023–1030, June 2008.

[52] R. Alléaume, C. Branciard, J. Bouda, T. Debuisschert, M. Dianati, N. Gisin, M. Godfrey, P. Grangier, T. Länger, N. Lütkenhaus, C. Monyk, P. Painchault, M. Peev, A. Poppe, T. Pornin, J. Rarity, R. Renner, G. Ribordy, M. Riguidel, L. Salvail, A. Shields, H. Weinfurter, and A. Zeilinger, "Using quantum key distribution for cryptographic purposes: A survey," *Theor. Comput. Sci.*, vol. 560, pp. 62–81, Dec. 2014.

[53] E. Diamanti and A. Leverrier, "Distributing secret keys with quantum continuous variables: Principle, security and implementations," *Entropy*, vol. 17, no. 9, pp. 6072–6092, Aug. 2015.

[54] M. Sasaki, "Quantum networks: Where should we be heading?," *Quantum Sci. Technol.*, vol. 2, no. 2, Apr. 2017, Art. no. 020501.

[55] W. Dür, R. Lamprecht, and S. Heusler, "Towards a quantum internet," *Eur. J. Phys.*, vol. 38, no. 4, May 2017, Art. no. 043001.

[56] A. Shenoy-Hejamadi, A. Pathak, and S. Radhakrishna, "Quantum cryptography: Key distribution and beyond," *Quanta*, vol. 6, no. 1, pp. 1–47, June 2017.

[57] F. Laudenbach, C. Pacher, C.-H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel, "Continuous-variable quantum key distribution with Gaussian modulation–The theory of practical implementations," *Adv. Quantum Technol.*, vol. 1, no. 1, June 2018, Art. no. 1800011.

[58] L. Gyongyosi, L. Bacsardi, and S. Imre, "A survey on quantum key distribution," *Infocommun. J.*, vol. XI, no. 2, pp. 14–21, June 2019.

[59] W. Kozlowski and S. Wehner, "Towards large-scale quantum networks," in *Proc. 6th Annu. ACM Int. Conf. Nanoscale Comput. Commun.*, Dublin, Ireland, Sept. 2019, Art. no. 3.

[60] N. Hosseinidehaj, Z. Babar, R. Malaney, S. X. Ng, and L. Hanzo, "Satellite-based continuous-variable quantum communications: State-of-the-art and a predictive outlook," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 881–919, 1st Quart., 2019.

[61] F. Cavaliere, E. Prati, L. Poti, I. Muhammad, and T. Catuogno, "Secure quantum communication technologies and systems: From labs to markets," *Quantum Rep.*, vol. 2, no. 1, pp. 80–106, Jan. 2020.

[62] M. Mehic, M. Niemiec, S. Rass, J. Ma, M. Peev, A. Aguado, V. Martin, S. Schauer, A. Poppe, C. Pacher, and M. Voznak, "Quantum key distribution: A networking perspective," *ACM Comput. Surv.*, vol. 53, no. 5, Sept. 2020, Art. no. 96.

[63] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *IEEE Access*, vol. 4, pp. 614–626, Mar. 2016.

[64] J. Zhang, S. Rajendran, Z. Sun, R. Woods, and L. Hanzo, "Physical layer security for the Internet of Things: Authentication and key generation," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 92–98, Oct. 2019.

[65] "Overview on networks supporting quantum key distribution," Recommendation ITU-T Y.3800, Oct. 2019.

[66] "Quantum key distribution (QKD); Device and communication channel parameters for QKD deployment," ETSI GS QKD 012 V1.1.1, Feb. 2019.

[67] L. Gyongyosi, S. Imre, and H. V. Nguyen, "A survey on quantum channel capacities," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 2, pp. 1149–1205, 2nd Quart., 2018.

[68] A. S. Cacciapuoti, M. Caleffi, R. V. Meter, and L. Hanzo, "When entanglement meets classical communications: Quantum teleportation for the quantum internet," *IEEE Trans. Commun.*, vol. 68, no. 6, pp.

3808–3833, June 2020.

[69] J. F. Dynes, W. W.-S. Tam, A. Plews, B. Fröhlich, A. W. Sharpe, M. Lucamarini, Z. Yuan, C. Radig, A. Straw, T. Edwards, and A. J. Shields, "Ultra-high bandwidth quantum secured data transmission," *Sci. Rep.*, vol. 6, Oct. 2016, Art. no. 35149.

[70] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, "Secure quantum key distribution over 421 km of optical fiber," *Phys. Rev. Lett.*, vol. 121, no. 19, Nov. 2018, Art. no. 190502.

[71] X.-T. Fang, P. Zeng, H. Liu, M. Zou, W. Wu, Y.-L. Tang, Y.-J. Sheng, Y. Xiang, W. Zhang, H. Li, Z. Wang, L. You, M.-J. Li, H. Chen, Y.-A. Chen, Q. Zhang, C.-Z. Peng, X. Ma, T.-Y. Chen, and J.-W. Pan, "Implementation of quantum key distribution surpassing the linear rate-transmittance bound," *Nature Photon.*, vol. 14, no. 7, pp. 422–425, July 2020.

[72] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W. Zhang, X.-L. Hu, J.-Y. Guan, Z.-W. Yu, H. Xu, J. Lin, M.-J. Li, H. Chen, H. Li, L. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, "Sending-or-not-sending with independent lasers: Secure twin-field quantum key distribution over 509 km," *Phys. Rev. Lett.*, vol. 124, no. 7, Feb. 2020, Art. no. 070501.

[73] M. Pittaluga, M. Minder, M. Lucamarini, M. Sanzaro, R. I. Woodward, M.-J. Li, Z. Yuan, and A. J. Shields, "600-km repeater-like quantum communications with dual-band stabilization," *Nature Photon.*, vol. 15, no. 7, pp. 530–535, July 2021.

[74] S. Nauerth, F. Moll, M. Rau, C. Fuchs, J. Horwath, S. Frick, and H. Weinfurter, "Air-to-ground quantum communication," *Nature Photon.*, vol. 7, no. 5, pp. 382–386, May 2013.

[75] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, F.-Z. Li, X.-W. Chen, L.-H. Sun, J.-J. Jia, J.-C. Wu, X.-J. Jiang, J.-F. Wang, Y.-M. Huang, Q. Wang, Y.-L. Zhou, L. Deng, T. Xi, L. Ma, T. Hu, Q. Zhang, Y.-A. Chen, N.-L. Liu, X.-B. Wang, Z.-C. Zhu, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, no. 7670, pp. 43–47, Sept. 2017.

[76] S.-K. Liao, H.-L. Yong, C. Liu, G.-L. Shentu, D.-D. Li, J. Lin, H. Dai, S.-Q. Zhao, B. Li, J.-Y. Guan, W. Chen, Y.-H. Gong, Y. Li, Z.-H. Lin, G.-S. Pan, J. S. Pelc, M. M. Fejer, W.-Z. Zhang, W.-Y. Liu, J. Yin, J.-G. Ren, X.-B. Wang, Q. Zhang, C.-Z. Peng, and J.-W. Pan, "Long-distance free-space quantum key distribution in daylight towards inter-satellite communication," *Nature Photon.*, vol. 11, no. 8, pp. 509–513, Aug. 2017.

[77] L. Ji, J. Gao, A.-L. Yang, Z. Feng, X.-F. Lin, Z.-G. Li, and X.-M. Jin, "Towards quantum communications in free-space seawater," *Opt. Express*, vol. 25, no. 17, pp. 19795–19806, Aug. 2017.

[78] F. Bouchard, A. Sit, F. Hufnagel, A. Abbas, Y. Zhang, K. Heshami, R. Fickler, C. Marquardt, G. Leuchs, R. W. Boyd, and E. Karimi, "Quantum cryptography with twisted photons through an outdoor underwater channel," *Opt. Express*, vol. 26, no. 17, pp. 22563–22573, Aug. 2018.

[79] S. Zhao, W. Li, Y. Shen, Y. Yu, X. Han, H. Zeng, M. Cai, T. Qian, S. Wang, Z. Wang, Y. Xiao, and Y. Gu, "Experimental investigation of quantum key distribution over a water channel," *Appl. Opt.*, vol. 58, no. 14, pp. 3902–3907, May 2019.

[80] M. Lanzagorta and J. Uhlmann, "Assessing feasibility of secure quantum communications involving underwater assets," *IEEE J. Ocean. Eng.*, vol. 45, no. 3, pp. 1138–1147, July 2020.

[81] Y. Cao, Y.-H. Li, K.-X. Yang, Y.-F. Jiang, S.-L. Li, X.-L. Hu, M. Abulizi, C.-L. Li, W. Zhang, Q.-C. Sun, W.-Y. Liu, X. Jiang, S.-K. Liao, J.-G. Ren, H. Li, L. You, Z. Wang, J. Yin, C.-Y. Lu, X.-B. Wang, Q. Zhang, C.-Z. Peng, and J.-W. Pan, "Long-distance free-space measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 125, no. 26, Dec. 2020, Art. no. 260503.

[82] C.-Q. Hu, Z.-Q. Yan, J. Gao, Z.-M. Li, H. Zhou, J.-P. Dou, and X.-M. Jin, "Decoy-state quantum key distribution over a long-distance high-loss air-water channel," *Phys. Rev. Applied*, vol. 15, no. 2, Feb. 2021, Art. no. 024060.

[83] I. Khan, B. Heim, A. Neuzner, and C. Marquardt, "Satellite-based QKD," *Opt. Photon. News*, vol. 29, no. 2, pp. 26–33, Feb. 2018.

[84] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, "Experimental quantum key distribution with decoy states," *Phys. Rev. Lett.*, vol. 96, no. 7, Feb. 2006, Art. no. 070502.

[85] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, "Provably secure and practical quantum key distribution over 307 km of optical fibre," *Nature Photon.*, vol. 9, no. 3, pp. 163–168, Mar. 2015.

[86] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, and J.-W. Pan, "Measurement-device-independent quantum key distribution over a 404 km optical fiber," *Phys. Rev. Lett.*, vol. 117, no. 19, Nov. 2016, Art. no. 190501.

[87] B. Fröhlich, M. Lucamarini, J. F. Dynes, L. C. Comandar, W. W.-S. Tam, A. Plews, A. W. Sharpe, Z. Yuan, and A. J. Shields, "Long-distance quantum key distribution secure against coherent attacks," *Optica*, vol. 4, no. 1, pp. 163–167, Jan. 2017.

[88] B. Qi, L.-L. Huang, L. Qian, and H.-K. Lo, "Experimental study on the Gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers," *Phys. Rev. A*, vol. 76, no. 5, Nov. 2007, Art. no. 052323.

[89] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, "Experimental demonstration of long-distance continuous-variable quantum key distribution," *Nature Photon.*, vol. 7, no. 5, pp. 378–381, May 2013.

[90] D. Huang, P. Huang, D. Lin, and G. Zeng, "Long-distance continuous-variable quantum key distribution by controlling excess noise," *Sci. Rep.*, vol. 6, Jan. 2016, Art. no. 19201.

[91] Y. Zhang, Z. Li, Z. Chen, C. Weedbrook, Y. Zhao, X. Wang, Y. Huang, C. Xu, X. Zhang, Z. Wang, M. Li, X. Zhang, Z. Zheng, B. Chu, X. Gao, N. Meng, W. Cai, Z. Wang, G. Wang, S. Yu, and H. Guo, "Continuous-variable QKD over 50 km commercial fiber," *Quantum Sci. Technol.*, vol. 4, no. 3, May 2019, Art. no. 035006.

[92] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Phys. Rev. Lett.*, vol. 88, no. 5, Jan. 2002, Art. no. 057902.

[93] K. Inoue, E. Waks, and Y. Yamamoto, "Differential phase shift quantum key distribution," *Phys. Rev. Lett.*, vol. 89, no. 3, June 2002, Art. no. 037902.

[94] W.-Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," *Phys. Rev. Lett.*, vol. 91, no. 5, Aug. 2003, Art. no. 057901.

[95] X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," *Phys. Rev. Lett.*, vol. 94, no. 23, June 2005, Art. no. 230503.

[96] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Phys. Rev. Lett.*, vol. 94, no. 23, June 2005, Art. no. 230504.

[97] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations," *Phys. Rev. Lett.*, vol. 92, no. 5, Feb. 2004, Art. no. 057901.

[98] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, "Fast and simple one-way quantum key distribution," *Appl. Phys. Lett.*, vol. 87, no. 19, Nov. 2005, Art. no. 194108.

[99] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, no. 6, pp. 661–663, Aug. 1991.

[100] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem," *Phys. Rev. Lett.*, vol. 68, no. 5, pp. 557–559, Feb. 1992.

[101] J. Zhang, M. A. Itzler, H. Zbinden, and J.-W. Pan, "Advances in InGaAs/InP single-photon detector systems for quantum communication," *Light Sci. Appl.*, vol. 4, no. 5, May 2015, Art. no. e286.

[102] Y. Zhang, Z. Chen, S. Pirandola, X. Wang, C. Zhou, B. Chu, Y. Zhao, B. Xu, S. Yu, and H. Guo, "Long-distance continuous-variable quantum key distribution over 202.81 km of fiber," *Phys. Rev. Lett.*, vol. 125, no. 1, July 2020, Art. no. 010502.

[103] R. Valivarthi, S. Etcheverry, J. Aldama, F. Zwiehoff, and V. Pruneri, "Plug-and-play continuous-variable quantum key distribution for metropolitan networks," *Opt. Express*, vol. 28, no. 10, pp. 14547–14559, May 2020.

[104] U. L. Andersen, J. S. Neergaard-Nielsen, P. van Loock, and A. Furusawa, "Hybrid discrete- and continuous-variable quantum information," *Nature Phys.*, vol. 11, no. 9, pp. 713–719, Sept. 2015.

[105] I. B. Djordjevic, "Hybrid DV-CV QKD outperforming existing QKD protocols in terms of secret-key rate and achievable distance," in *Proc. 21st Int. Conf. Transparent Optical Networks*, Angers, France, July 2019, Art. no. We.C5.5.

[106] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 108, no. 13, Mar. 2012, Art. no. 130503.

[107] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate-distance limit of quantum key distribution without quantum repeaters," *Nature*, vol. 557, no. 7705, pp. 400–403, May 2018.

[108] X. Ma, P. Zeng, and H. Zhou, "Phase-matching quantum key distribution," *Phys. Rev. X*, vol. 8, no. 3, Aug. 2018, Art. no. 031043.

[109] C. Pacher, A. Abidin, T. Lorünser, M. Peev, R. Ursin, A. Zeilinger, and J.-Å. Larsson, "Attacks on quantum key distribution protocols that employ non-ITS authentication," *Quantum Inf. Process.*, vol. 15, no. 1, pp. 327–362, Jan. 2016.

[110] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, "Limitations on practical quantum cryptography," *Phys. Rev. Lett.*, vol. 85, no. 6, pp. 1330–1333, Aug. 2000.

[111] N. Lütkenhaus, "Security against individual attacks for realistic quantum key distribution," *Phys. Rev. A*, vol. 61, no. 5, May 2000, Art. no. 052304.

[112] XT Quantech [Online]. Available: http://www.xtquantech.com/en/.

[113] K. Tamaki, H.-K. Lo, C.-H. F. Fung, and B. Qi, "Phase encoding schemes for measurement-device-independent quantum key distribution with basis-dependent flaw," *Phys. Rev. A*, vol. 85, no. 4, Apr. 2012, Art. no. 042307.

[114] X. Ma and M. Razavi, "Alternative schemes for measurement-device-independent quantum key distribution," *Phys. Rev. A*, vol. 86, no. 6, Dec. 2012, Art. no. 062319.

[115] F. Xu, M. Curty, B. Qi, and H.-K. Lo, "Measurement-device-independent quantum cryptography," *IEEE J. Sel. Top. Quantum Electron.*, vol. 21, no. 3, May/June 2015, Art no. 6601111.

[116] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, "High-rate measurement-device-independent quantum cryptography," *Nature Photon.*, vol. 9, no. 6, pp. 397–402, June 2015.

[117] H.-X. Ma, P. Huang, D.-Y. Bai, T. Wang, S.-Y. Wang, W.-S. Bao, and G.-H. Zeng, "Long-distance continuous-variable measurement-device-independent quantum key distribution with discrete modulation," *Phys. Rev. A*, vol. 99, no. 2, Feb. 2019, Art. no. 022322.

[118] D. Pan, S. X. Ng, D. Ruan, L. Yin, G. Long, and L. Hanzo, "Simultaneous two-way classical communication and measurement-device-independent quantum key distribution with coherent states," *Phys. Rev. A*, vol. 101, no. 1, Jan. 2020, Art. no. 012343.

[119] W. Wang, F. Xu, and H.-K. Lo, "Asymmetric protocols for scalable high-rate measurement-device-independent quantum key distribution networks," *Phys. Rev. X*, vol. 9, no. 4, Oct. 2019, Art. no. 041012.

[120] H. Liu, W. Wang, K. Wei, X.-T. Fang, L. Li, N.-L. Liu, H. Liang, S.-J. Zhang, W. Zhang, H. Li, L. You, Z. Wang, H.-K. Lo, T.-Y. Chen, F. Xu, and J.-W. Pan, "Experimental demonstration of high-rate measurement-device-independent quantum key distribution over asymmetric channels," *Phys. Rev. Lett.*, vol. 122, no. 16, Apr. 2019, Art. no. 160501.

[121] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, "Device-independent quantum key distribution secure against collective attacks," *New. J. Phys.*, vol. 11, no. 4, Apr. 2009, Art. no. 045021.

[122] K. Marshall and C. Weedbrook, "Device-independent quantum cryptography for continuous variables," *Phys. Rev. A*, vol. 90, no. 4, Oct. 2014, Art. no. 042311.

[123] J. Xin, X.-M. Lu, X. Li, and G. Li, "One-sided device-independent quantum key distribution for two independent parties," *Opt. Express*, vol. 28, no. 8, pp. 11439–11450, Apr. 2020.

[124] G. Murta, S. B. van Dam, J. Ribeiro, R. Hanson, and S. Wehner, "Towards a realization of device-independent quantum key distribution," *Quantum Sci. Technol.*, vol. 4, no. 3, July 2019, Art. no. 035011.

[125] M. Lucamarini, K. A. Patel, J. F. Dynes, B. Fröhlich, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Efficient decoy-state quantum key distribution with quantified security," *Opt. Express*, vol. 21, no. 21, pp. 24550–24565, Oct. 2013.

[126] V. Martin, A. Aguado, D. Lopez, M. Peev, V. Lopez, A. Pastor, A. Poppe, H. Brunner, S. Bettelli, F. Fung, D. Hillerkuss, L. Comandar, and D. Wang, "The Madrid SDN-QKD network," in *Proc. 8th Int. Conf. Quantum Crypt.*, Shanghai, China, Aug. 2018.

[127] R. S. Tessinari, A. Bravalheri, E. Hugues-Salas, R. Collins, D. Aktas, R. S. Guimaraes, O. Alia, J. Rarity, G. T. Kanellos, R. Nejabati, and D. Simeonidou, "Field trial of dynamic DV-QKD networking in the SDN-controlled fully-meshed optical metro network of the Bristol city 5GUK test network," in *Proc. Eur. Conf. Opt. Commun.*, Dublin, Ireland, Sept. 2019.

[128] A. Wonfor, C. White, A. Bahrami, J. Pearse, G. Duan, A. Straw, T. Edwards, T. Spiller, R. Penty, and A. Lord, "Field trial of multi-node, coherent-one-way quantum key distribution with encrypted 5x100G DWDM transmission system," in *Proc. Eur. Conf. Opt. Commun.*, Dublin, Ireland, Sept. 2019.

[129] T.-Y. Chen, X. Jiang, S.-B. Tang, L. Zhou, X. Yuan, H. Zhou, J. Wang, Y. Liu, L.-K. Chen, W.-Y. Liu, H.-F. Zhang, K. Cui, H. Liang, X.-G. Li, Y. Mao, L.-J. Wang, S.-B. Feng, Q. Chen, Q. Zhang, L. Li, N.-L. Liu, C.-Z. Peng, X. Ma, Y. Zhao, and J.-W. Pan, "Implementation of a 46-node quantum metropolitan area network," *npj Quantum Inf.*, vol. 7, Sept. 2021, Art. no. 134.

[130] B. Fröhlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, Z. Yuan, and A. J. Shields, "A quantum access network," *Nature*, vol. 501, no. 7465, pp. 69–72, Sept. 2013.

[131] X. Tang, A. Wonfor, R. Kumar, R. V. Penty, and I. H. White, "Quantum-safe metro network with low-latency reconfigurable quantum key distribution," *J. Lightwave Technol.*, vol. 36, no. 22, pp. 5230–5236, Nov. 2018.

[132] Y.-L. Tang, H.-L. Yin, Q. Zhao, H. Liu, X.-X. Sun, M.-Q. Huang, W.-J. Zhang, S.-J. Chen, L. Zhang, L.-X. You, Z. Wang, Y. Liu, C.-Y. Lu, X. Jiang, X. Ma, Q. Zhang, T.-Y. Chen, and J.-W. Pan, "Measurement-device-independent quantum key distribution over untrustful metropolitan network," *Phys. Rev. X*, vol. 6, no. 1, Mar. 2016, Art. no. 011024.

[133] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, "Quantum repeaters: The role of imperfect local operations in quantum communication," *Phys. Rev. Lett.*, vol. 81, no. 26, pp. 5932–5935, Dec. 1998.

[134] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, "Quantum repeaters based on atomic ensembles and linear optics," *Rev. Mod. Phys.*, vol. 83, no. 1, pp. 33–80, Mar. 2011.

[135] R. V. Meter and J. Touch, "Designing quantum repeater networks," *IEEE Commun. Mag.*, vol. 51, no. 8, pp. 64–71, Aug. 2013.

[136] P. D. Townsend, "Quantum cryptography on multiuser optical fibre networks," *Nature*, vol. 385, no. 6611, pp. 47–49, Jan. 1997.

[137] I. Choi, R. J. Young, and P. D. Townsend, "Quantum information to the home," *New J. Phys.*, vol. 13, no. 6, June 2011, Art. no. 063039.

[138] T. R. Raddo, S. Rommel, V. Land, C. Okonkwo, and I. T. Monroy, "Quantum data encryption as a service on demand: Eindhoven QKD network testbed," in *Proc. 21st Int. Conf. Transparent Optical Networks*, Angers, France, July 2019, Art. no. We.B5.2.

[139] X. Tang, L. Ma, A. Mink, A. Nakassis, H. Xu, B. Hershman, J. Bienfang, D. Su, R. F. Boisvert, C. Clark, and C. Williams, "Demonstration of an active quantum key distribution network," *Proc. SPIE, Quantum Commun. Quantum Imag. IV*, vol. 6305, Aug. 2006, Art. no. 630506.

[140] L. Ma, A. Mink, H. Xu, O. Slattery, and X. Tang, "Experimental demonstration of an active quantum key distribution network with over gbps clock synchronization," *IEEE Commun. Lett.*, vol. 11, no. 12, pp. 1019–1021, Dec. 2007.

[141] L. Ma, X. Tang, O. Slattery, and A. Battou, "A testbed for quantum communication and quantum networks," *Proc. SPIE, Quantum Inf. Sci. Sens. Comput. XI*, vol. 10984, May 2019, Art. no. 1098407.

[142] C. Elliott, "Building the quantum network," *New J. Phys.*, vol. 4, no. 1, July 2002, Art. no. 46.

[143] W. Chen, Z.-F. Han, T. Zhang, H. Wen, Z.-Q. Yin, F.-X. Xu, Q.-L. Wu, Y. Liu, Y. Zhang, X.-F. Mo, Y.-Z. Gui, G. Wei, and G.-C. Guo, "Field experiment on a "star type" metropolitan quantum key distribution network," *IEEE Photon. Technol. Lett.*, vol. 21, no. 9, pp. 575–577, May 2009.

[144] M. Dianati and R. Alléaume, "Architecture of the Secoqc quantum key distribution network," in *Proc. 1st Int. Conf. Quantum, Nano, and Micro Technol.*, Guadeloupe, Jan. 2007.

[145] R. Alléaume, J. Bouda, C. Branciard, T. Debuisschert, M. Dianati, N. Gisin, M. Godfrey, P. Grangier, T. Länger, A. Leverrier, N. Lütkenhaus, P. Painchault, M. Peev, A. Poppe, T. Pornin, J. Rarity, R. Renner, G. Ribordy, M. Riguidel, L. Salvail, A. Shields, H. Weinfurter, and A. Zeilinger, "SECOQC white paper on quantum key distribution and cryptography," arXiv: quant-ph/0701168, 2007.

[146] A. Poppe, M. Peev, and O. Maurhart, "Outline of the SECOQC quantum-key-distribution network in Vienna," *Int. J. Quantum Inf.*, vol. 6, no. 2, pp. 209–218, Apr. 2008.

[147] T.-Y. Chen, H. Liang, Y. Liu, W.-Q. Cai, L. Ju, W.-Y. Liu, J. Wang, H. Yin, K. Chen, Z.-B. Chen, C.-Z. Peng, and J.-W. Pan, "Field test of a practical secure communication network with decoy-state quantum cryptography," *Opt. Express*, vol. 17, no. 8, pp. 6540–6549, Apr. 2009.

[148] A. Mirza and F. Petruccione, “Realizing long-term quantum cryptography,” *J. Opt. Soc. Am. B*, vol. 27, no. 6, pp. A185–A188, June 2010.

[149] F. Xu, W. Chen, S. Wang, Z. Yin, Y. Zhang, Y. Liu, Z. Zhou, Y. Zhao, H. Li, D. Liu, Z. Han, and G. Guo, “Field experiment on a robust hierarchical metropolitan quantum cryptography network,” *Chin. Sci. Bull.*, vol. 54, no. 17, pp. 2991–2997, Sept. 2009.

[150] T.-Y. Chen, J. Wang, H. Liang, W.-Y. Liu, Y. Liu, X. Jiang, Y. Wang, X. Wan, W.-Q. Cai, L. Ju, L.-K. Chen, L.-J. Wang, Y. Gao, K. Chen, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan, “Metropolitan all-pass and inter-city quantum communication network,” *Opt. Express*, vol. 18, no. 26, pp. 27217–27225, Dec. 2010.

[151] D. Lancho, J. Martinez, D. Elkouss, M. Soto, and V. Martin, “QKD in standard optical telecommunications networks,” in *Proc. Int. Conf. Quantum Commun. Quantum Netw.*, Naples, Italy, Oct. 2009, pp. 142–149.

[152] S. Wang, W. Chen, Z.-Q. Yin, Y. Zhang, T. Zhang, H.-W. Li, F.-X. Xu, Z. Zhou, Y. Yang, D.-J. Huang, L.-J. Zhang, F.-Y. Li, D. Liu, Y.-G. Wang, G.-C. Guo, and Z.-F. Han, “Field test of wavelength-saving quantum key distribution network,” *Opt. Lett.*, vol. 35, no. 14, pp. 2454–2456, July 2010.

[153] Q. Zhang, “Quantum network in China,” in *Proc. Updating Quantum Crypt. Commun.*, Tokyo, Japan, Sept. 2015.

[154] A. Morrow, D. Hayford, and M. Legré, “Battelle QKD test bed,” in *Proc. IEEE Conf. Technol. Homeland Security*, Waltham, MA, USA, Nov. 2012, pp. 162–166.

[155] N. Walenta, D. Caselunghe, S. Chuard, M. Domergue, M. Hagerman, R. Hart, D. Hayford, R. Houlmann, M. Legré, T. McCandlish, L. Monat, A. Morrow, G. Ribordy, D. Stucki, M. Tourville, P. Trinkler, and R. Wolterman, “Towards a North American QKD backbone with certifiable security,” in *Proc. 5th Int. Conf. Quantum Crypt.*, Tokyo, Japan, Sept. 2015.

[156] A. Ciurana, J. Martínez-Mateo, M. Peev, A. Poppe, N. Walenta, H. Zbinden, and V. Martín, “Quantum metropolitan optical network based on wavelength division multiplexing,” *Opt. Express*, vol. 22, no. 2, pp. 1576–1593, Jan. 2014.

[157] D. Huang, P. Huang, H. Li, T. Wang, Y. Zhou, and G. Zeng, “Field demonstration of a continuous-variable quantum key distribution network,” *Opt. Lett.*, vol. 41, no. 15, pp. 3511–3514, Aug. 2016.

[158] O. I. Bannik, V. V. Chistyakov, L. R. Gilyazov, K. S. Melnik, A. B. Vasiliev, N. M. Arslanov, A. A. Gaidash, A. V. Kozubov, V. I. Egorov, S. A. Kozlov, A. V. Gleim, and S. A. Moiseev, “Multinode subcarrier wave quantum communication network,” in *Proc. 7th Int. Conf. Quantum Crypt.*, Cambridge, UK, Sept. 2017.

[159] T. Kim and S. Kwak, “Development of quantum technologies at SK Telecom,” *AAPPS Bull.*, vol. 26, no. 6, pp. 2–9, Dec. 2016.

[160] T. Kim, “Status of QKD system deployment and Ion Trap development at SK Telecom,” in *Proc. Relativistic Quantum Inf. North*, Kyoto, Japan, July 2017.

[161] E. O. Kiktenko, N. O. Pozhar, A. V. Duplinskiy, A. A. Kanapin, A. S. Sokolov, S. S. Vorobey, A. V. Miller, V. E. Ustimchik, M. N. Anufriev, A. T. Trushechkin, R. R. Yunusov, V. L. Kurochkin, Y. V. Kurochkin, and A. K. Fedorov, “Demonstration of a quantum key distribution network in urban fibre-optic communication lines,” *Quantum Electron.*, vol. 47, no. 9, pp. 798–802, Sept. 2017.

[162] Wuhan Launches World-Leading Quantum Network [Online]. Available: http://www.chinadaily.com.cn/china/2017-11/01/content_33968959.htm.

[163] A. Aguado, V. López, D. López, M. Peev, A. Poppe, A. Pastor, J. Folgueira, and V. Martín, “The engineering of software-defined quantum key distribution networks,” *IEEE Commun. Mag.*, vol. 57, no. 7, pp. 20–26, July 2019.

[164] A. Aguado, V. López, J. P. Brito, A. Pastor, D. R. López, and V. Martin, “Enabling quantum key distribution networks via software-defined networking,” in *Proc. Int. Conf. Optical Network Design and Modelling*, Castelldefels, Barcelona, Spain, May 2020.

[165] S. K. Joshi, D. Aktas, S. Wengerowsky, M. Lončarić, S. P. Neumann, B. Liu, T. Scheidl, G. C. Lorenzo, Ž. Samec, L. Kling, A. Qiu, M. Razavi, M. Stipčević, J. G. Rarity, and R. Ursin, “A trusted node-free eight-user metropolitan quantum communication network,” *Sci. Adv.*, vol. 6, no. 36, Sept. 2020, Art. no. eaba0959.

[166] X.-F. Mo, B. Zhu, Z.-F. Han, Y.-Z. Gui, and G.-C. Guo, “Faraday-Michelson system for quantum cryptography,” *Opt. Lett.*, vol. 30, no. 19, pp. 2632–2634, Oct. 2005.

[167] R. J. Runser, T. E. Chapuran, P. Toliver, M. S. Goodman, R. J. Hughes, C. G. Peterson, K. McCabe, J. E. Nordholt, K. Tyagi, P. Hiskett, and N. Dallmann, “Quantum key distribution for reconfigurable optical networks,” in *Proc. Opt. Fiber Commun. Conf.*, Anaheim, CA, USA, Mar. 2006, Art. no. OFL1.

[168] T. E. Chapuran, P. Toliver, N. A. Peters, J. Jackel, M. S. Goodman, R. J. Runser, S. R. McNown, N. Dallmann, R. J. Hughes, K. P. McCabe, J. E. Nordholt, C. G. Peterson, K. T. Tyagi, L. Mercer, and H. Dardy, “Optical networking for quantum key distribution and quantum communications,” *New J. Phys.*, vol. 11, no. 10, Oct. 2009, Art. no. 105001.

[169] A. Mirza and F. Petruccione, “Recent findings from the quantum network in Durban,” *AIP Conf. Proc.*, vol. 1363, no. 1, pp. 35–38, Oct. 2011.

[170] P. Jouguet, S. Kunz-Jacques, T. Debuisschert, S. Fossier, E. Diamanti, R. Alléaume, R. Tualle-Brouri, P. Grangier, A. Leverrier, P. Pache, and P. Painchault, “Field test of classical symmetric encryption with continuous variables quantum key distribution,” *Opt. Express*, vol. 20, no. 13, pp. 14030–14041, June 2012.

[171] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, “Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks,” *Phys. Rev. Lett.*, vol. 111, no. 13, Sept. 2013, Art. no. 130501.

[172] K. Shimizu, T. Honjo, M. Fujiwara, T. Ito, K. Tamaki, S. Miki, T. Yamashita, H. Terai, Z. Wang, and M. Sasaki, “Performance of long-distance quantum key distribution over 90-km optical links installed in a field environment of Tokyo metropolitan area,” *J. Lightwave Technol.*, vol. 32, no. 1, pp. 141–151, Jan. 2014.

[173] Y.-L. Tang, H.-L. Yin, S.-J. Chen, Y. Liu, W.-J. Zhang, X. Jiang, L. Zhang, J. Wang, L.-X. You, J.-Y. Guan, D.-X. Yang, Z. Wang, H. Liang, Z. Zhang, N. Zhou, X. Ma, T.-Y. Chen, Q. Zhang, and J.-W. Pan, “Field test of measurement-device-independent quantum key distribution,” *IEEE J. Sel. Top. Quantum Electron.*, vol. 21, no. 3, May/June 2015, Art. no. 6600407.

[174] A. R. Dixon, J. F. Dynes, M. Lucamarini, B. Fröhlich, A. W. Sharpe, A. Plews, S. Tam, Z. L. Yuan, Y. Tanizawa, H. Sato, S. Kawamura, M. Fujiwara, M. Sasaki, and A. J. Shields, “High speed prototype quantum key distribution system and long term field trial,” *Opt. Express*, vol. 23, no. 6, pp. 7583–7592, Mar. 2015.

[175] D. Bunandar, A. Lentine, C. Lee, H. Cai, C. M. Long, N. Boynton, N. Martinez, C. DeRose, C. Chen, M. Grein, D. Trotter, A. Starbuck, A. Pomerene, S. Hamilton, F. N. C. Wong, R. Camacho, P. Davids, J. Urayama, and D. Englund, “Metropolitan quantum key distribution with silicon photonics,” *Phys. Rev. X*, vol. 8, no. 2, Apr. 2018, Art. no. 021009.

[176] D. Bacco, I. Vagniluca, B. D. Lio, N. Biagi, A. D. Frera, D. Calonico, C. Toninelli, F. S. Cataliotti, M. Bellini, L. K. Oxenløwe, and A. Zavatta, “Field trial of a three-state quantum key distribution scheme in the Florence metropolitan area,” *EPJ Quantum Technol.*, vol. 6, Oct. 2019, Art. no. 5.

[177] T. Zhang, X.-F. Mo, Z.-F. Han, and G.-C. Guo, “Extensible router for a quantum key distribution network,” *Phys. Lett. A*, vol. 372, no. 22, pp. 3957–3962, May 2008.

[178] V. Martin, A. Aguado, P. Salas, A. L. Sanz, J. P. Brito, D. R. Lopez, V. Lopez, A. Pastor, J. Folgueira, H. H. Brunner, S. Bettelli, F. Fung, L. C. Comandar, D. Wang, A. Poppe, and M. Peev, “The Madrid quantum network: A quantum-classical integrated infrastructure,” in *Proc. OSA Adv. Photon. Cong.*, Burlingame, CA, USA, July 2019, Art. no. QtW3E.5.

[179] F. Grosshans, G. V. Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, “Quantum key distribution using gaussian-modulated coherent states,” *Nature*, vol. 421, no. 6920, pp. 238–241, Jan. 2003.

[180] S. Wang, W. Chen, Z.-Q. Yin, H.-W. Li, D.-Y. He, Y.-H. Li, Z. Zhou, X.-T. Song, F.-Y. Li, D. Wang, H. Chen, Y.-G. Han, J.-Z. Huang, J.-F. Guo, P.-L. Hao, M. Li, C.-M. Zhang, D. Liu, W.-Y. Liang, C.-H. Miao, P. Wu, G.-C. Guo, and Z.-F. Han, “Field and long-term demonstration of a wide area quantum key distribution network,” *Opt. Express*, vol. 22, no. 18, pp. 21739–21756, Sept. 2014.

[181] Q. Zhang, F. Xu, L. Li, N.-L. Liu, and J.-W. Pan, “Quantum information research in China,” *Quantum Sci. Technol.*, vol. 4, no. 4, Nov. 2019, Art. no. 040503.

[182] Y. Mao, B.-X. Wang, C. Zhao, G. Wang, R. Wang, H. Wang, F. Zhou, J. Nie, Q. Chen, Y. Zhao, Q. Zhang, J. Zhang, T.-Y. Chen, and J.-W. Pan, “Integrating quantum key distribution with classical communications in backbone fiber network,” *Opt. Express*, vol. 26, no. 5, pp. 6010–6020, Mar. 2018.

[183] New Quantum Communication Landline Connecting East, Central China

Put into Service [Online]. Available: http://www.globaltimes.cn/content/1127200.shtml.

[184] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W.-J. Zhang, Z.-Y. Han, S.-Z. Ma, X.-L. Hu, Y.-H. Li, H. Liu, F. Zhou, H.-F. Jiang, T.-Y. Chen, H. Li, L.-X. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, "Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas," *Nature Photon.*, vol. 15, no. 8, pp. 570–575, Aug. 2021.

[185] H. Qin, "Towards large-scale quantum key distribution network and its applications," in *Proc. ITU Workshop on Quantum Information Technology (QIT) for Networks*, Shanghai, China, June 2019.

[186] Quantum Network from Boston to Washington DC in the Works [Online]. Available: https://quantumxc.com/media-coverage/quantum-network-from-boston-to-washington-dc-in-the-works/.

[187] Building a Globe-Spanning Quantum Internet [Online]. Available: https://www.theverge.com/2014/11/18/7214483/quantum-networks-expand-across-three-continents.

[188] Quantum Communications Hub Annual Report 2018-2019 [Online]. Available: https://www.quantumcommshub.net/wp-content/uploads/2020/09/FINAL-for-web_Quantum-Hub_report_condensed_2019.pdf.

[189] P. Knight and I. Walmsley, "UK national quantum technology programme," *Quantum Sci. Technol.*, vol. 4, no. 4, Oct. 2019, Art. no. 040502.

[190] OpenQKD [Online]. Available: https://openqkd.eu/.

[191] 7 Thousand km of Quantum Networks to be Stretched in Russia by the End of 2024 [Online]. Available: https://ict.moscow/en/news/7000-km-of-quantum-networks-to-be-stretched-in-russia-by-the-end-of-2024/.

[192] A. K. Fedorov, A. V. Akimov, J. D. Biamonte, A. V. Kavokin, F. Y. Khalili, E. O. Kiktenko, N. N. Kolachevsky, Y. V. Kurochkin, A. I. Lvovsky, A. N. Rubtsov, G. V. Shlyapnikov, S. S. Straupe, A. V. Ustinov, and A. M. Zheltikov, "Quantum technologies in Russia," *Quantum Sci. Technol.*, vol. 4, no. 4, Oct. 2019, Art. no. 040501.

[193] N. Walenta and L. Oesterling, "Quantum networks: Photons hold key to data security," *Photon. Spectra*, vol. 50, no. 5, pp. 40–44, May 2016.

[194] Toshiba to Lead Joint R&D Project Commissioned by Japan's MIC to Develop Global Quantum Cryptography Communications Network [Online]. Available: https://www.global.toshiba/ww/technology/corporate/rdc/rd/topics/20/2007-02.html.

[195] Y. Yamamoto, M. Sasaki, and H. Takesue, "Quantum information science and technology in Japan," *Quantum Sci. Technol.*, vol. 4, no. 2, Feb. 2019, Art. no. 020502.

[196] R. Bedington, J. M. Arrazola, and A. Ling, "Progress in satellite quantum key distribution," *npj Quantum Inf.*, vol. 3, Aug. 2017, Art. no. 30.

[197] Governments Ally for Federated Quantum Encryption Satellite Network [Online]. Available: https://spacenews.com/governments-ally-for-federated-quantum-encryption-satellite-network/.

[198] R. J. Hughes, J. E. Nordholt, K. P. McCabe, R. T. Newell, C. G. Peterson, and R. D. Somma, "Network-centric quantum communications with application to critical infrastructure protection," arXiv: 1305.0305, 2013.

[199] A. Aguado, V. Martin, D. Lopez, M. Peev, J. Martinez-Mateo, J. L. Rosales, F. de la Iglesia, M. Gomez, E. Hugues-Salas, A. Lord, R. Nejabati, and D. Simeonidou, "Quantum-aware software defined networks," in *Proc. 6th Int. Conf. Quantum Crypt.*, Washington, DC, USA, Sept. 2016.

[200] Y. Cao, Y. Zhao, R. Lin, X. Yu, J. Zhang, and J. Chen, "Multi-tenant secret-key assignment over quantum key distribution networks," *Opt. Express*, vol. 27, no. 3, pp. 2544–2561, Feb. 2019.

[201] Y. Cao, Y. Zhao, J. Wang, X. Yu, Z. Ma, and J. Zhang, "SDQaaS: Software defined networking for quantum key distribution as a service," *Opt. Express*, vol. 27, no. 5, pp. 6892–6909, Mar. 2019.

[202] Y. Cao, Y. Zhao, X. Yu, and J. Zhang, "Multi-tenant provisioning over software defined networking enabled metropolitan area quantum key distribution networks," *J. Opt. Soc. Am. B*, vol. 36, no. 3, pp. B31–B40, Mar. 2019.

[203] W. Maeda, A. Tanaka, S. Takahashi, A. Tajima, and A. Tomita, "Technologies for quantum key distribution networks integrated with optical communication networks," *IEEE J. Sel. Top. Quantum Electron.*, vol. 15, no. 6, pp. 1591–1601, Nov./Dec. 2009.

[204] Y. Cao, Y. Zhao, C. Colman-Meixner, X. Yu, and J. Zhang, "Key on demand (KoD) for software-defined optical networks secured by quantum key distribution (QKD)," *Opt. Express*, vol. 25, no. 22, pp. 26453–26467, Oct. 2017.

[205] Y. Cao, Y. Zhao, X. Yu, and Y. Wu, "Resource assignment strategy in optical networks integrated with quantum key distribution," *J. Opt. Commun. Netw.*, vol. 9, no. 11, pp. 995–1004, Nov. 2017.

[206] A. Tajima, T. Kondoh, T. Ochi, M. Fujiwara, K. Yoshino, H. Iizuka, T. Sakamoto, A. Tomita, E. Shimamura, S. Asami, and M. Sasaki, "Quantum key distribution network for multiple applications," *Quantum Sci. Technol.*, vol. 2, no. 3, July 2017, Art. no. 034003.

[207] Y. Zhao, Y. Cao, W. Wang, H. Wang, X. Yu, J. Zhang, M. Tornatore, Y. Wu, and B. Mukherjee, "Resource allocation in optical networks secured by quantum key distribution," *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 130–137, Aug. 2018.

[208] Y. Cao, Y. Zhao, J. Wang, X. Yu, Z. Ma, and J. Zhang, "KaaS: Key as a service over quantum key distribution integrated optical networks," *IEEE Commun. Mag.*, vol. 57, no. 5, pp. 152–159, May 2019.

[209] Y. Tanizawa, R. Takahashi, H. Sato, and A. R. Dixon, "An approach to integrate quantum key distribution technology into standard secure communication applications," in *Proc. 9th Int. Conf. Ubiquitous and Future Networks*, Milan, Italy, July 2017, pp. 880–886.

[210] A. Aguado, E. Hugues-Salas, P. A. Haigh, J. Marhuenda, A. B. Price, P. Sibson, J. E. Kennard, C. Erven, J. G. Rarity, M. G. Thompson, A. Lord, R. Nejabati, and D. Simeonidou, "Secure NFV orchestration over an SDN-controlled optical network with time-shared quantum key distribution resources," *J. Lightwave Technol.*, vol. 35, no. 8, pp. 1357–1362, Apr. 2017.

[211] K. Dong, Y. Zhao, X. Yu, A. Nag, and J. Zhang, "Auxiliary graph based routing, wavelength, and time-slot assignment in metro quantum optical networks with a novel node structure," *Opt. Express*, vol. 28, no. 5, pp. 5936–5952, Mar. 2020.

[212] M. Mehic, P. Fazio, S. Rass, O. Maurhart, M. Peev, A. Poppe, J. Rozhon, M. Niemiec, and M. Voznak, "A novel approach to quality-of-service provisioning in trusted relay quantum key distribution networks," *IEEE/ACM Trans. Netw.*, vol. 28, no. 1, pp. 168–181, Feb. 2020.

[213] "Quantum key distribution (QKD); Components and internal interfaces," ETSI GR QKD 003 V2.1.1, Mar. 2018.

[214] D. Levi, P. Meyer, and B. Stewart, "Simple network management protocol (SNMP) applications," IETF RFC 3413, Dec. 2002.

[215] D. Harrington and J. Schoenwaelder, "Transport subsystem for the simple network management protocol (SNMP)," IETF RFC 5590, June 2009.

[216] Common Object Request Broker Architecture [Online]. Available: https://www.omg.org/spec/CORBA/.

[217] "Quantum key distribution (QKD); Control interface for software defined networks," ETSI GS QKD 015 V1.1.1, Mar. 2021.

[218] "Quantum key distribution networks - Software defined networking control," Recommendation ITU-T Y.3805, Dec. 2021.

[219] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "OpenFlow: Enabling innovation in campus networks," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 38, no. 2, pp. 69–74, Mar. 2008.

[220] R. Enns, M. Bjorklund, J. Schoenwaelder, and A. Bierman, "Network configuration protocol (NETCONF)," IETF RFC 6241, June 2011.

[221] "Quantum key distribution (QKD); Application interface," ETSI GS QKD 004 V2.1.1, Aug. 2020.

[222] "Quantum key distribution (QKD); Protocol and data format of REST-based key delivery API," ETSI GS QKD 014 V1.1.1, Feb. 2019.

[223] P. D. Townsend, "Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelength-division multiplexing," *Electron. Lett.*, vol. 33, no. 3, pp. 188–190, Jan. 1997.

[224] A. Bahrami, A. Lord, and T. P. Spiller, "Quantum key distribution integration with optical dense wavelength division multiplexing: A review," *IET Quantum Commun.*, vol. 1, no. 1, pp. 9–15, July 2020.

[225] R. J. Runser, T. Chapuran, P. Toliver, N. A. Peters, M. S. Goodman, J. T. Kosloski, N. Nweke, S. R. McNown, R. J. Hughes, D. Rosenberg, C. G. Peterson, K. P. McCabe, J. E. Nordholt, K. Tyagi, P. A. Hiskett, and N. Dallmann, "Progress toward quantum communications networks: Opportunities and challenges," *Proc. SPIE, Optoelectronic Integrated Circuits IX*, vol. 6476, Feb. 2007, Art. no. 64760I.

[226] H. Rohde, S. Smolorz, A. Poppe, and H. Huebel, "Quantum key distribution integrated into commercial WDM systems," in *Proc. Opt. Fiber Commun. Conf.*, San Diego, CA, USA, Feb. 2008, Art. no. OTuP1.

[227] G. B. Xavier, G. V. de Faria, G. P. Temporão, and J. P. von der Weid, "Scattering effects on QKD employing simultaneous classical and quantum channels in telecom optical fibers in the C-band," *AIP Conf. Proc.*, vol. 1110, no. 1, pp. 327–330, Apr. 2009.

[228] B. Qi, W. Zhu, L. Qian, and H.-K. Lo, "Feasibility of quantum key distribution through a dense wavelength division multiplexing network," *New J. Phys.*, vol. 12, no. 10, Oct. 2010, Art. no. 103042.

[229] H. Kawahara, A. Medhipour, and K. Inoue, "Effect of spontaneous Raman scattering on quantum channel wavelength-multiplexed with classical channel," *Opt. Commun.*, vol. 284, no. 2, pp. 691–696, Jan. 2011.

[230] T. F. da Silva, G. B. Xavier, G. P. Temporão, and J. P. von der Weid, "Impact of Raman scattered noise from multiple telecom channels on fiber-optic quantum key distribution systems," *J. Lightwave Technol.*, vol. 32, no. 13, pp. 2332–2339, July 2014.

[231] B. Fröhlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, S. W.-B. Tam, Z. Yuan, and A. J. Shields, "Quantum secured gigabit optical access networks," *Sci. Rep.*, vol. 5, Dec. 2015, Art. no. 18121.

[232] Y. Sun, Y. Lu, J. Niu, and Y. Ji, "Reduction of FWM noise in WDM-based QKD systems using interleaved and unequally spaced channels," *Chin. Opt. Lett.*, vol. 14, no. 6, June 2016, Art. no. 060602.

[233] J.-N. Niu, Y.-M. Sun, C. Cai, and Y.-F. Ji, "Optimized channel allocation scheme for jointly reducing four-wave mixing and Raman scattering in the DWDM-QKD system," *Appl. Opt.*, vol. 57, no. 27, pp. 7987–7996, Sept. 2018.

[234] P. Toliver, R. J. Runser, T. E. Chapuran, S. McNown, M. S. Goodman, J. Jackel, R. J. Hughes, C. G. Peterson, K. McCabe, J. E. Nordholt, K. Tyagi, P. Hiskett, and N. Dallman, "Impact of spontaneous anti-Stokes Raman scattering on QKD+DWDM networking," in *Proc. 17th Annu. Meeting IEEE Lasers and Electro-Optics Soc.*, Rio Grande, Puerto Rico, Nov. 2004, pp. 491–492.

[235] N. I. Nweke, P. Toliver, R. J. Runser, S. R. McNown, J. B. Khurgin, T. E. Chapuran, M. S. Goodman, R. J. Hughes, C. G. Peterson, K. McCabe, J. E. Nordholt, K. Tyagi, P. Hiskett, and N. Dallmann, "Experimental characterization of the separation between wavelength-multiplexed quantum and classical communication channels," *Appl. Phys. Lett.*, vol. 87, no. 17, Oct. 2005, Art. no. 174103.

[236] R. J. Runser, T. E. Chapuran, P. Toliver, M. S. Goodman, J. Jackel, N. Nweke, S. R. McNown, R. J. Hughes, C. G. Peterson, K. McCabe, J. E. Nordholt, K. Tyagi, P. Hiskett, and N. Dallmann, "Demonstration of 1.3 μm quantum key distribution (QKD) compatibility with 1.5 μm metropolitan wavelength division multiplexed (WDM) systems," in *Proc. Opt. Fiber Commun. Conf.*, Anaheim, CA, USA, Mar. 2005, Art. no. OWI2.

[237] N. I. Nweke, R. J. Runser, S. R. McNown, J. B. Khurgin, T. E. Chapuran, P. Toliver, M. S. Goodman, J. Jackel, R. J. Hughes, C. G. Peterson, and J. E. Nordholt, "EDFA bypass and filtering architecture enabling QKD+WDM coexistence on mid-span amplified links," in *Proc. Conf. Lasers and Electro-Optics*, Long Beach, CA, USA, May 2006, Art. no. CWQ7.

[238] S. Aleksic, F. Hipp, D. Winkler, A. Poppe, B. Schrenk, and G. Franzl, "Perspectives and limitations of QKD integration in metropolitan area networks," *Opt. Express*, vol. 23, no. 8, pp. 10359–10373, Apr. 2015.

[239] L.-J. Wang, K.-H. Zou, W. Sun, Y. Mao, Y.-X. Zhu, H.-L. Yin, Q. Chen, Y. Zhao, F. Zhang, T.-Y. Chen, and J.-W. Pan, "Long-distance copropagation of quantum key distribution and terabit classical optical data channels," *Phys. Rev. A*, vol. 95, no. 1, Jan. 2017, Art. no. 012301.

[240] T. J. Xia, D. Z. Chen, G. A. Wellbrock, A. Zavriyev, A. C. Beal, and K. M. Lee, "In-band quantum key distribution (QKD) on fiber populated by high-speed classical data channels," in *Proc. Opt. Fiber Commun. Conf.*, Anaheim, CA, USA, Mar. 2006, Art. no. OTuJ7.

[241] N. A. Peters, P. Toliver, T. E. Chapuran, R. J. Runser, S. R. McNown, C. G. Peterson, D. Rosenberg, N. Dallmann, R. J. Hughes, K. P. McCabe, J. E. Nordholt, and K. T. Tyagi, "Dense wavelength multiplexing of 1550 nm QKD with strong classical channels in reconfigurable networking environments," *New J. Phys.*, vol. 11, no. 4, Apr. 2009, Art. no. 045012.

[242] P. Eraerds, N. Walenta, M. Legré, N. Gisin, and H. Zbinden, "Quantum key distribution and 1 Gbps data encryption over a single fibre," *New J. Phys.*, vol. 12, no. 6, June 2010, Art. no. 063027.

[243] I. Choi, R. J. Young, and P. D. Townsend, "Quantum key distribution on a 10Gb/s WDM-PON," *Opt. Express*, vol. 18, no. 9, pp. 9600–9612, Apr. 2010.

[244] K. A. Patel, J. F. Dynes, M. Lucamarini, I. Choi, A. W. Sharpe, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks," *Appl. Phys. Lett.*, vol. 104, no. 5, Feb. 2014, Art. no. 051123.

[245] R. Kumar, H. Qin, and R. Alléaume, "Coexistence of continuous variable QKD with intense DWDM classical channels," *New J. Phys.*, vol. 17, no. 4, Apr. 2015, Art. no. 043027.

[246] F. Karinou, L. Comandar, H. H. Brunner, D. Hillerkuss, F. Fung, S. Bettelli, S. Mikroulis, D. Wang, Q. Yi, M. Kuschnerov, C. Xie, A. Poppe, and M. Peev, "Experimental evaluation of the impairments on a QKD system in a 20-channel WDM co-existence scheme," in *Proc. IEEE Photon. Soc. Summer Top. Meeting Ser.*, San Juan, Puerto Rico, July 2017, pp. 145–146.

[247] T. A. Eriksson, T. Hirano, M. Ono, M. Fujiwara, R. Namiki, K. Yoshino, A. Tajima, M. Takeoka, and M. Sasaki, "Coexistence of continuous variable quantum key distribution and 7×12.5 Gbit/s classical channels," in *Proc. IEEE Photon. Soc. Summer Top. Meeting Ser.*, Waikoloa Village, HI, USA, July 2018, pp. 71–72.

[248] T. A. Eriksson, T. Hirano, G. Rademacher, B. J. Puttnam, R. S. Luís, M. Fujiwara, R. Namiki, Y. Awaji, M. Takeoka, N. Wada, and M. Sasaki, "Joint propagation of continuous variable quantum key distribution and 18 × 24.5 Gbaud PM-16QAM channels," in *Proc. Eur. Conf. Opt. Commun.*, Rome, Italy, Sept. 2018.

[249] F. Karinou, H. H. Brunner, C.-H. F. Fung, L. C. Comandar, S. Bettelli, D. Hillerkuss, M. Kuschnerov, S. Mikroulis, D. Wang, C. Xie, M. Peev, and A. Poppe, "Toward the integration of CV quantum key distribution in deployed optical networks," *IEEE Photon. Technol. Lett.*, vol. 30, no. 7, pp. 650–653, Apr. 2018.

[250] T. A. Eriksson, T. Hirano, B. J. Puttnam, G. Rademacher, R. S. Luís, M. Fujiwara, R. Namiki, Y. Awaji, M. Takeoka, N. Wada, and M. Sasaki, "Wavelength division multiplexing of continuous variable quantum key distribution and 18.3 Tbit/s data channels," *Commun. Phys.*, vol. 2, Jan. 2019, Art. no. 9.

[251] R. Valivarthi, P. Umesh, C. John, K. A. Owen, V. B. Verma, S. W. Nam, D. Oblak, Q. Zhou, and W. Tittel, "Measurement-device-independent quantum key distribution coexisting with classical communication," *Quantum Sci. Technol.*, vol. 4, no. 4, July 2019, Art. no. 045002.

[252] D. Milovančev, N. Vokić, F. Laudenbach, C. Pacher, H. Hübel, and B. Schrenk, "Spectrally-shaped continuous-variable QKD operating at 500 MHz over an optical pipe lit by 11 DWDM channels," in *Proc. Opt. Fiber Commun. Conf.*, San Diego, CA, USA, Mar. 2020, Art. no. T3D.4.

[253] K. A. Patel, J. F. Dynes, I. Choi, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Coexistence of high-bit-rate quantum key distribution and data on optical fiber," *Phys. Rev. X*, vol. 2, no. 4, Nov. 2012, Art. no. 041010.

[254] D. Huang, D. Lin, C. Wang, W. Liu, S. Fang, J. Peng, P. Huang, and G. Zeng, "Continuous-variable quantum key distribution with 1 Mbps secure key rate," *Opt. Express*, vol. 23, no. 13, pp. 17511–17519, June 2015.

[255] L.-J. Wang, L.-K. Chen, L. Ju, M.-L. Xu, Y. Zhao, K. Chen, Z.-B. Chen, T.-Y. Chen, and J.-W. Pan, "Experimental multiplexing of quantum key distribution with classical optical communication," *Appl. Phys. Lett.*, vol. 106, no. 8, Feb. 2015, Art. no. 081108.

[256] S. Kleis, J. Steinmayer, R. H. Derksen, and C. G. Schaeffer, "Experimental investigation of heterodyne quantum key distribution in the S-band embedded in a commercial DWDM system," in *Proc. Opt. Fiber Commun. Conf.*, San Diego, CA, USA, Mar. 2019, Art. no. Th1J.3.

[257] K. Yoshino, M. Fujiwara, A. Tanaka, S. Takahashi, Y. Nambu, A. Tomita, S. Miki, T. Yamashita, Z. Wang, M. Sasaki, and A. Tajima, "High-speed wavelength-division multiplexing quantum key distribution system," *Opt. Lett.*, vol. 37, no. 2, pp. 223–225, Jan. 2012.

[258] K. Yoshino, T. Ochi, M. Fujiwara, M. Sasaki, and A. Tajima, "Maintenance-free operation of WDM quantum key distribution system through a field fiber over 30 days," *Opt. Express*, vol. 21, no. 25, pp. 31395–31401, Dec. 2013.

[259] T. A. Eriksson, R. S. Luís, B. J. Puttnam, G. Rademacher, M. Fujiwara, Y. Awaji, H. Furukawa, N. Wada, M. Takeoka, and M. Sasaki, "Wavelength division multiplexing of 194 continuous variable quantum key distribution channels," *J. Lightwave Technol.*, vol. 38, no. 8, pp. 2214–2218, Apr. 2020.

[260] A. Tanaka, M. Fujiwara, S. W. Nam, Y. Nambu, S. Takahashi, W. Maeda, K. Yoshino, S. Miki, B. Baek, Z. Wang, A. Tajima, M. Sasaki, and A. Tomita, "Ultra fast quantum key distribution over a 97 km installed telecom fiber with wavelength division multiplexing clock synchronization," *Opt. Express*, vol. 16, no. 15, pp. 11354–11360, July 2008.

[261] I. Choi, Y. R. Zhou, J. F. Dynes, Z. Yuan, A. Klar, A. Sharpe, A. Plews, M. Lucamarini, C. Radig, J. Neubert, H. Griesser, M. Eiselt, C. Chunnilall, G. Lepert, A. Sinclair, J.-P. Elbers, A. Lord, and A. Shields, "Field trial of a

quantum secured 10Gb/s DWDM transmission system over a single installed fiber," *Opt. Express*, vol. 22, no. 19, pp. 23121–23128, Sept. 2014.

[262] S. Bahrani, M. Razavi, and J. A. Salehi, "Orthogonal frequency-division multiplexed quantum key distribution," *J. Lightwave Technol.*, vol. 33, no. 23, pp. 4687–4698, Dec. 2015.

[263] N. Yu, Z. Dong, J. Wang, Z. Wei, and Z. Zhang, "Impact of spontaneous Raman scattering on quantum channel wavelength-multiplexed with classical channel in time domain," *Chin. Opt. Lett.*, vol. 12, no. 10, Oct. 2014, Art. no. 102703.

[264] A. Ortigosa-Blanch and J. Capmany, "Subcarrier multiplexing optical quantum key distribution," *Phys. Rev. A*, vol. 73, no. 2, Feb. 2006, Art. no. 024305.

[265] J. Capmany and C. R. Fernandez-Pousa, "Analysis of passive optical networks for subcarrier multiplexed quantum key distribution," *IEEE Trans. Microwave Theory Tech.*, vol. 58, no. 11, pp. 3220–3228, Nov. 2010.

[266] J. Mora, W. Amaya, A. Ruiz-Alba, A. Martinez, D. Calvo, V. García-Muñoz, and J. Capmany, "Simultaneous transmission of 20x2 WDM/SCM-QKD and 4 bidirectional classical channels over a PON," *Opt. Express*, vol. 20, no. 15, pp. 16358–16365, July 2012.

[267] A. Ruiz-Alba, J. Mora, W. Amava, A. Martínez, V. García-Muñoz, D. Calvo, and J. Capmany, "Microwave photonics parallel quantum key distribution," *IEEE Photon. J.*, vol. 4, no. 3, pp. 931–942, June 2012.

[268] M. Ureña, I. Gasulla, F. J. Fraile, and J. Capmany, "Modeling optical fiber space division multiplexed quantum key distribution systems," *Opt. Express*, vol. 27, no. 5, pp. 7047–7063, Mar. 2019.

[269] C. Cai, Y. Sun, and Y. Ji, "Intercore spontaneous Raman scattering impact on quantum key distribution in multicore fiber," *New J. Phys.*, vol. 22, no. 8, Aug. 2020, Art. no. 083020.

[270] G. B. Xavier and G. Lima, "Quantum information processing with space-division multiplexing optical fibres," *Commun. Phys.*, vol. 3, Jan. 2020, Art. no. 9.

[271] C. Cai, Y. Sun, and Y. Ji, "Simultaneous long-distance transmission of discrete-variable quantum key distribution and classical optical communication," *IEEE Trans. Commun.*, vol. 69, no. 5, pp. 3222–3234, May 2021.

[272] W. Kong, Y. Sun, C. Cai, and Y. Ji, "Impact of classical modulation signals on quantum key distribution over multicore fiber," *J. Lightwave Technol.*, vol. 39, no. 13, pp. 4341–4350, July 2021.

[273] J. F. Dynes, S. J. Kindness, S. W.-B. Tam, A. Plews, A. W. Sharpe, M. Lucamarini, B. Fröhlich, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Quantum key distribution over multicore fiber," *Opt. Express*, vol. 24, no. 8, pp. 8081–8087, Apr. 2016.

[274] R. Lin, A. Udalcovs, O. Ozolins, X. Pang, L. Gan, L. Shen, M. Tang, S. Fu, S. Popov, C. Yang, W. Tong, D. Liu, T. F. da Silva, G. B. Xavier, and J. Chen, "Telecom compatibility validation of quantum key distribution co-existing with 112 Gbps/λ/core data transmission in non-trench and trench-assistant multicore fibers," in *Proc. Eur. Conf. Opt. Commun.*, Rome, Italy, Sept. 2018.

[275] E. Hugues-Salas, R. Wang, G. T. Kanellos, R. Nejabati, and D. Simeonidou, "Co-existence of 9.6 Tb/s classical channels and a quantum key distribution (QKD) channel over a 7-core multicore optical fibre," in *Proc. IEEE British and Irish Conf. Opt. Photon.*, London, UK, Dec. 2018.

[276] T. A. Eriksson, B. J. Puttnam, G. Rademacher, R. S. Luís, M. Fujiwara, M. Takeoka, Y. Awaji, M. Sasaki, and N. Wada, "Crosstalk impact on continuous variable quantum key distribution in multicore fiber transmission," *IEEE Photon. Technol. Lett.*, vol. 31, no. 6, pp. 467–470, Mar. 2019.

[277] C. Cai, Y. Sun, Y. Zhang, P. Zhang, J. Niu, and Y. Ji, "Experimental wavelength-space division multiplexing of quantum key distribution with classical optical communication over multicore fiber," *Opt. Express*, vol. 27, no. 4, pp. 5125–5135, Feb. 2019.

[278] D. Bacco, B. D. Lio, D. Cozzolino, F. D. Ros, X. Guo, Y. Ding, Y. Sasaki, K. Aikawa, S. Miki, H. Terai, T. Yamashita, J. S. Neergaard-Nielsen, M. Galili, K. Rottwitt, U. L. Andersen, T. Morioka, and L. K. Oxenløwe, "Boosting the secret key rate in a shared quantum and classical fibre communication system," *Commun. Phys.*, vol. 2, Nov. 2019, Art. no. 140.

[279] R. Lin, A. Udalcovs, O. Ozolins, X. Pang, L. Gan, M. Tang, S. Fu, S. Popov, T. F. da Silva, G. B. Xavier, and J. Chen, "Telecommunication compatibility evaluation for co-existing quantum key distribution in homogenous multicore fiber," *IEEE Access*, vol. 8, pp. 78836–78846, May 2020.

[280] E. Hugues-Salas, O. Alia, R. Wang, K. Rajkumar, G. T. Kanellos, R. Nejabati, and D. Simeonidou, "11.2 Tb/s classical channel coexistence with DV-QKD over a 7-core multicore fiber," *J. Lightwave Technol.*, vol. 38, no. 18, pp. 5064–5070, Sept. 2020.

[281] B.-X. Wang, Y. Mao, L. Shen, L. Zhang, X.-B. Lan, D. Ge, Y. Gao, J. Li, Y.-L. Tang, S.-B. Tang, J. Zhang, T.-Y. Chen, and J.-W. Pan, "Long-distance transmission of quantum key distribution coexisting with classical optical communication over a weakly-coupled few-mode fiber," *Opt. Express*, vol. 28, no. 9, pp. 12558–12565, Apr. 2020.

[282] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, "Long-distance quantum communication with atomic ensembles and linear optics," *Nature*, vol. 414, no. 6862, pp. 413–418, Nov. 2001.

[283] W. J. Munro, K. Azuma, K. Tamaki, and K. Nemoto, "Inside quantum repeaters," *IEEE J. Sel. Top. Quantum Electron.*, vol. 21, no. 3, May/June 2015, Art. no. 6400813.

[284] W. J. Munro, A. M. Stephens, S. J. Devitt, K. A. Harrison, and K. Nemoto, "Quantum communication without the necessity of quantum memories," *Nature Photon.*, vol. 6, no. 11, pp. 777–781, Nov. 2012.

[285] K. Azuma, K. Tamaki, and H.-K. Lo, "All-photonic quantum repeaters," *Nature Commun.*, vol. 6, Apr. 2015, Art. no. 6787.

[286] R. Van Meter, T. D. Ladd, W. J. Munro, and K. Nemoto, "System design for a long-line quantum repeater," *IEEE/ACM Trans. Netw.*, vol. 17, no. 3, pp. 1002–1013, June 2009.

[287] Y. Hasegawa, R. Ikuta, N. Matsuda, K. Tamaki, H.-K. Lo, T. Yamamoto, K. Azuma, and N. Imoto, "Experimental time-reversed adaptive Bell measurement towards all-photonic quantum repeaters," *Nature Commun.*, vol. 10, Jan. 2019, Art. no. 378.

[288] Z.-D. Li, R. Zhang, X.-F. Yin, L.-Z. Liu, Y. Hu, Y.-Q. Fang, Y.-Y. Fei, X. Jiang, J. Zhang, L. Li, N.-L. Liu, F. Xu, Y.-A. Chen, and J.-W. Pan, "Experimental quantum repeater without quantum memory," *Nature Photon.*, vol. 13, no. 9, pp. 644–648, Sept. 2019.

[289] S. Kumar, N. Lauk, and C. Simon, "Towards long-distance quantum networks with superconducting processors and optical links," *Quantum Sci. Technol.*, vol. 4, no. 4, July 2019, Art. no. 045003.

[290] S. Pirandola, "End-to-end capacities of a quantum communication network," *Commun. Phys.*, vol. 2, May 2019, Art. no. 51.

[291] M. Takeoka, S. Guha, and M. M. Wilde, "Fundamental rate-loss tradeoff for optical quantum key distribution," *Nature Commun.*, vol. 5, Oct. 2014, Art. no. 5235.

[292] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, "Fundamental limits of repeaterless quantum communications," *Nature Commun.*, vol. 8, Apr. 2017, Art. no. 15043.

[293] M. Minder, M. Pittaluga, G. L. Roberts, M. Lucamarini, J. F. Dynes, Z. L. Yuan, and A. J. Shields, "Experimental quantum key distribution beyond the repeaterless secret key capacity," *Nature Photon.*, vol. 13, no. 5, pp. 334–338, May 2019.

[294] S. Wang, D.-Y. He, Z.-Q. Yin, F.-Y. Lu, C.-H. Cui, W. Chen, Z. Zhou, G.-C. Guo, and Z.-F. Han, "Beating the fundamental rate-distance limit in a proof-of-principle quantum key distribution system," *Phys. Rev. X*, vol. 9, no. 2, June 2019, Art. no. 021046.

[295] Y. Liu, Z.-W. Yu, W. Zhang, J.-Y. Guan, J.-P. Chen, C. Zhang, X.-L. Hu, H. Li, C. Jiang, J. Lin, T.-Y. Chen, L. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, "Experimental twin-field quantum key distribution through sending or not sending," *Phys. Rev. Lett.*, vol. 123, no. 10, Sept. 2019, Art. no. 100505.

[296] X. Zhong, J. Hu, M. Curty, L. Qian, and H.-K. Lo, "Proof-of-principle experimental demonstration of twin-field type quantum key distribution," *Phys. Rev. Lett.*, vol. 123, no. 10, Sept. 2019, Art. no. 100506.

[297] "Quantum key distribution networks - Key management," Recommendation ITU-T Y.3803, Dec. 2020.

[298] W. Stacey, R. Annabestani, X. Ma, and N. Lütkenhaus, "Security of quantum key distribution using a simplified trusted relay," *Phys. Rev. A*, vol. 91, no. 1, Jan. 2015, Art. no. 012338.

[299] D. Elkouss, J. Martinez-Mateo, A. Ciurana, and V. Martin, "Secure optical networks based on quantum key distribution and weakly trusted repeaters," *J. Opt. Commun. Netw.*, vol. 5, no. 4, pp. 316–328, Apr. 2013.

[300] X. Zou, X. Yu, Y. Zhao, A. Nag, and J. Zhang, "Collaborative routing in partially-trusted relay based quantum key distribution optical networks," in *Proc. Opt. Fiber Commun. Conf.*, San Diego, CA, USA, Mar. 2020, Art. no. M3K.4.

[301] H.-K. Lo, W. Wang, and F. Xu, "Scalable measurement-device-independent quantum key distribution networks with untrusted relays," in *Proc. Opt. Fiber Commun. Conf.*, San Diego,

CA, USA, Mar. 2020, Art. no. M1E.2.

[302] M. Razavi, N. L. Piparo, C. Panayi, and D. E. Bruschi, "Architectural considerations in hybrid quantum-classical networks," in *Proc. Iran Workshop on Commun. Inf. Theory*, Tehran, Iran, May 2013.

[303] N. L. Piparo and M. Razavi, "Long-distance trust-free quantum key distribution," *IEEE J. Sel. Top. Quantum Electron.*, vol. 21, no. 3, May/June 2015, Art. no. 6600508.

[304] B. Mukherjee, I. Tomkos, M. Tornatore, P. Winzer, and Y. Zhao, *Springer Handbook of Optical Networks*. Springer International Publishing, 2020.

[305] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *J. Cryptol.*, vol. 5, no. 1, pp. 3–28, Jan. 1992.

[306] W. T. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons, "Practical free-space quantum key distribution over 1 km," *Phys. Rev. Lett.*, vol. 81, no. 15, pp. 3283–3286, Oct. 1998.

[307] W. T. Buttler, R. J. Hughes, S. K. Lamoreaux, G. L. Morgan, J. E. Nordholt, and C. G. Peterson, "Daylight quantum key distribution over 1.6 km," *Phys. Rev. Lett.*, vol. 84, no. 24, pp. 5652–5655, June 2000.

[308] J. G. Rarity, P. M. Gorman, and P. R. Tapster, "Secure key exchange over 1.9 km free-space range using quantum cryptography," *Electron. Lett.*, vol. 37, no. 8, pp. 512–514, Apr. 2001.

[309] R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson, "Practical free-space quantum key distribution over 10 km in daylight and at night," *New J. Phys.*, vol. 4, no. 1, July 2002, Art. no. 43.

[310] C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster, and J. G. Rarity, "A step towards global key distribution," *Nature*, vol. 419, no. 6906, pp. 450, Oct. 2002.

[311] C.-Z. Peng, T. Yang, X.-H. Bao, J. Zhang, X.-M. Jin, F.-Y. Feng, B. Yang, J. Yang, J. Yin, Q. Zhang, N. Li, B.-L. Tian, and J.-W. Pan, "Experimental free-space distribution of entangled photon pairs over 13 km: Towards satellite-based global quantum communication," *Phys. Rev. Lett.*, vol. 94, no. 15, Apr. 2005, Art. no. 150501.

[312] K. J. Resch, M. Lindenthal, B. Blauensteiner, H. R. Böhm, A. Fedrizzi, C. Kurtsiefer, A. Poppe, T. Schmitt-Manderbach, M. Taraba, R. Ursin, P. Walther, H. Weier, H. Weinfurter, and A. Zeilinger, "Distributing entanglement and single photons through an intra-city, free-space quantum channel," *Opt. Express*, vol. 13, no. 1, pp. 202–209, Jan. 2005.

[313] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km," *Phys. Rev. Lett.*, vol. 98, no. 1, Jan. 2007, Art. no. 010504.

[314] L. Moli-Sanchez, A. Rodriguez-Alonso, and G. Seco-Granados, "Performance analysis of quantum cryptography protocols in optical earth-satellite and intersatellite links," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 9, pp. 1582–1590, Dec. 2009.

[315] J.-P. Bourgoin, E. Meyer-Scott, B. L. Higgins, B. Helou, C. Erven, H. Hübel, B. Kumar, D. Hudson, I. D'Souza, R. Girard, R. Laflamme, and T. Jennewein, "A comprehensive design and performance analysis of low Earth orbit satellite quantum communication," *New J. Phys.*, vol. 15, no. 2, Feb. 2013, Art. no. 023006.

[316] J.-Y. Wang, B. Yang, S.-K. Liao, L. Zhang, Q. Shen, X.-F. Hu, J.-C. Wu, S.-J. Yang, H. Jiang, Y.-L. Tang, B. Zhong, H. Liang, W.-Y. Liu, Y.-H. Hu, Y.-M. Huang, B. Qi, J.-G. Ren, G.-S. Pan, J. Yin, J.-J. Jia, Y.-A. Chen, K. Chen, C.-Z. Peng, and J.-W. Pan, "Direct and full-scale experimental verifications towards ground-satellite quantum key distribution," *Nature Photon.*, vol. 7, no. 5, pp. 387–393, May 2013.

[317] G. Vallone, D. Bacco, D. Dequal, S. Gaiarin, V. Luceri, G. Bianco, and P. Villoresi, "Experimental satellite quantum communications," *Phys. Rev. Lett.*, vol. 115, no. 4, July 2015, Art. no. 040502.

[318] F. Steinlechner, P. Trojek, M. Jofre, H. Weier, D. Perez, T. Jennewein, R. Ursin, J. Rarity, M. W. Mitchell, J. P. Torres, H. Weinfurter, and V. Pruneri, "A high-brightness source of polarization-entangled photons optimized for applications in free space," *Opt. Express*, vol. 20, no. 9, pp. 9640–9649, Apr. 2012.

[319] G. Vest, M. Rau, L. Fuchs, G. Corrielli, H. Weier, S. Nauerth, A. Crespi, R. Osellame, and H. Weinfurter, "Design and evaluation of a handheld quantum key distribution sender module," *IEEE J. Sel. Top. Quantum Electron.*, vol. 21, no. 3, May/June 2015, Art. no. 6600607.

[320] I. Capraro, A. Tomaello, A. Dall'Arche, F. Gerlin, R. Ursin, G. Vallone, and P. Villoresi, "Impact of turbulence in long range quantum and classical communications," *Phys. Rev. Lett.*, vol. 109, no. 20, Nov. 2012, Art. no. 200502.

[321] D. P. Naughton, R. Bedington, S. Barraclough, T. Islam, D. Griffin, B. Smith, J. Kurtz, A. S. Alenin, I. J. Vaughn, A. Ramana, I. Dimitrijevic, Z. S. Tang, C. Kurtsiefer, A. Ling, and R. Boyce, "Design considerations for an optical link supporting intersatellite quantum key distribution," *Opt. Eng.*, vol. 58, no. 1, Jan. 2019, Art. no. 016106.

[322] Y. C. Tan, R. Chandrasekara, C. Cheng, and A. Ling, "Silicon avalanche photodiode operation and lifetime analysis for small satellites," *Opt. Express*, vol. 21, no. 14, pp. 16946–16954, July 2013.

[323] E. Anisimova, B. L. Higgins, J. Bourgoin, M. Cranmer, E. Choi, D. Hudson, L. P. Piche, A. Scott, V. Makarov, and T. Jennewein, "Mitigating radiation damage of single photon detectors for space applications," *EPJ Quantum Technol.*, vol. 4, May 2017, Art. no. 10.

[324] J. Yin, Y.-H. Li, S.-K. Liao, M. Yang, Y. Cao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, S.-L. Li, R. Shu, Y.-M. Huang, L. Deng, L. Li, Q. Zhang, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, X.-B. Wang, F. Xu, J.-Y. Wang, C.-Z. Peng, A. K. Ekert, and J.-W. Pan, "Entanglement-based secure quantum cryptography over 1,120 kilometres," *Nature*, vol. 582, no. 7813, pp. 501–505, June 2020.

[325] H. Takenaka, A. Carrasco-Casado, M. Fujiwara, M. Kitamura, M. Sasaki, and M. Toyoshima, "Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite," *Nature Photon.*, vol. 11, no. 8, pp. 502–508, Aug. 2017.

[326] J. A. Grieve, R. Bedington, Z. Tang, R. C. Chandrasekara, and A. Ling, "SpooQySats: CubeSats to demonstrate quantum key distribution technologies," *Acta Astronautica*, vol. 151, pp. 103–106, Oct. 2018.

[327] T. Vergoossen, S. Loarte, R. Bedington, H. Kuiper, and A. Ling, "Modelling of satellite constellations for trusted node QKD networks," *Acta Astronautica*, vol. 173, pp. 164–171, Aug. 2020.

[328] D. Huang, Y. Zhao, T. Yang, S. Rahman, X. Yu, X. He, and J. Zhang, "Quantum key distribution over double-layer quantum satellite networks," *IEEE Access*, vol. 8, pp. 16087–16098, Jan. 2020.

[329] P. Sibson, C. Erven, M. Godfrey, S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, H. Terai, M. G. Tanner, C. M. Natarajan, R. H. Hadfield, J. L. O'Brien, and M. G. Thompson, "Chip-based quantum key distribution," *Nature Commun.*, vol. 8, Feb. 2017, Art. no. 13984.

[330] A. Himeno, K. Kato, and T. Miya, "Silica-based planar lightwave circuits," *IEEE J. Sel. Top. Quantum Electron.*, vol. 4, no. 6, pp. 913–924, Nov./Dec. 1998.

[331] H. Takesue, E. Diamanti, T. Honjo, C. Langrock, M. M. Fejer, K. Inoue, and Y. Yamamoto, "Differential phase shift quantum key distribution experiment over 105 km fibre," *New J. Phys.*, vol. 7, no. 1, Nov. 2005, Art. no. 232.

[332] E. Diamanti, H. Takesue, C. Langrock, M. M. Fejer, and Y. Yamamoto, "100 km differential phase shift quantum key distribution experiment with low jitter up-conversion detectors," *Opt. Express*, vol. 14, no. 26, pp. 13073–13082, Dec. 2006.

[333] H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, "Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors," *Nature Photon.*, vol. 1, no. 6, pp. 343–348, June 2007.

[334] Y. Nambu, K. Yoshino, and A. Tomita, "Quantum encoder and decoder for practical quantum key distribution using a planar lightwave circuit," *J. Mod. Opt.*, vol. 55, no. 12, pp. 1953–1970, July 2008.

[335] J. L. Duligall, M. S. Godfrey, K. A. Harrison, W. J. Munro, and J. G. Rarity, "Low cost and compact quantum key distribution," *New J. Phys.*, vol. 8, no. 10, Oct. 2006, Art. no. 249.

[336] P. Zhang, K. Aungskunsiri, E. Martín-López, J. Wabnig, M. Lobino, R. W. Nock, J. Munns, D. Bonneau, P. Jiang, H. W. Li, A. Laing, J. G. Rarity, A. O. Niskanen, M. G. Thompson, and J. L. O'Brien, "Reference-frame-independent quantum-key-distribution server with a telecom tether for an on-chip client," *Phys. Rev. Lett.*, vol. 112, no. 13, Apr. 2014, Art. no. 130501.

[337] A. E.-J. Lim, J. Song, Q. Fang, C. Li, X. Tu, N. Duan, K. K. Chen, R. P.-C. Tern, and T.-Y. Liow, "Review of silicon photonics foundry efforts," *IEEE J. Sel. Top. Quantum Electron.*, vol. 20, no. 4, July/Aug. 2014, Art. no. 8300112.

[338] C. Ma, W. D. Sacher, Z. Tang, J. C. Mikkelsen, Y. Yang, F. Xu, T. Thiessen, H.-K. Lo, and J. K. S. Poon, "Silicon photonic transmitter for polarization-encoded quantum key distribution," *Optica*, vol. 3, no. 11, pp. 1274–1278, Nov. 2016.

[339] P. Sibson, J. E. Kennard, S. Stanisic, C. Erven, J. L. O'Brien, and M. G. Thompson, "Integrated silicon photonics for high-speed quantum key

distribution," *Optica*, vol. 4, no. 2, pp. 172–177, Feb. 2017.

[340] D. Bacco, Y. Ding, K. Dalgaard, K. Rottwitt, and L. K. Oxenløwe, "Space division multiplexing chip-to-chip quantum key distribution," *Sci. Rep.*, vol. 7, Sept. 2017, Art. no. 12459.

[341] Y. Ding, D. Bacco, K. Dalgaard, X. Cai, X. Zhou, K. Rottwitt, and L. K. Oxenløwe, "High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits," *npj Quantum Inf.*, vol. 3, June 2017, Art. no. 25.

[342] M. Ziebell, M. Persechino, N. Harris, C. Galland, D. Marris-Morini, L. Vivien, E. Diamanti, and P. Grangier, "Towards on-chip continuous-variable quantum key distribution," in *Proc. Eur. Quantum Electron. Conf.*, Munich, Germany, June 2015, Art. no. JSV_4_2.

[343] G. Zhang, J. Y. Haw, H. Cai, F. Xu, S. M. Assad, J. F. Fitzsimons, X. Zhou, Y. Zhang, S. Yu, J. Wu, W. Ser, L. C. Kwek, and A. Q. Liu, "An integrated silicon photonic chip platform for continuous-variable quantum key distribution," *Nature Photon.*, vol. 13, no. 12, pp. 839–842, Dec. 2019.

[344] Y. Shen, L. Cao, X. Wang, J. Zou, W. Luo, Y. Wang, H. Cai, B. Dong, X. Luo, W. Fan, L. C. Kwek, and A. Liu, "On-chip continuous-variable quantum key distribution (CV-QKD) and homodyne detection," in *Proc. Opt. Fiber Commun. Conf.*, San Diego, CA, USA, Mar. 2020, Art. no. W2A.53.

[345] H. Cai, C. M. Long, C. T. DeRose, N. Boynton, J. Urayama, R. Camacho, A. Pomerene, A. L. Starbuck, D. C. Trotter, P. S. Davids, and A. L. Lentine, "Silicon photonic transceiver circuit for high-speed polarization-based discrete variable quantum key distribution," *Opt. Express*, vol. 25, no. 11, pp. 12282–12294, May 2017.

[346] W. Geng, C. Zhang, Y. Zheng, J. He, C. Zhou, and Y. Kong, "Stable quantum key distribution using a silicon photonic transceiver," *Opt. Express*, vol. 27, no. 20, pp. 29045–29054, Sept. 2019.

[347] C.-Y. Wang, J. Gao, Z.-Q. Jiao, L.-F. Qiao, R.-J. Ren, Z. Feng, Y. Chen, Z.-Q. Yan, Y. Wang, H. Tang, and X.-M. Jin, "Integrated measurement server for measurement-device-independent quantum key distribution network," *Opt. Express*, vol. 27, no. 5, pp. 5982–5989, Mar. 2019.

[348] H. Semenenko, P. Sibson, A. Hart, M. G. Thompson, J. G. Rarity, and C. Erven, "Chip-based measurement-device-independent quantum key distribution," *Optica*, vol. 7, no. 3, pp. 238–242, Mar. 2020.

[349] K. Wei, W. Li, H. Tan, Y. Li, H. Min, W.-J. Zhang, H. Li, L. You, Z. Wang, X. Jiang, T.-Y. Chen, S.-K. Liao, C.-Z. Peng, F. Xu, and J.-W. Pan, "High-speed measurement-device-independent quantum key distribution with integrated silicon photonics," *Phys. Rev. X*, vol. 10, no. 3, Aug. 2020, Art. no. 031030.

[350] A. Orieux and E. Diamanti, "Recent advances on integrated quantum communications," *J. Opt.*, vol. 18, no. 8, July 2016, Art. no. 083002.

[351] Q.-Y. Zhang, P. Xu, and S.-N. Zhu, "Quantum photonic network on chip," *Chin. Phys. B*, vol. 27, no. 5, Apr. 2018, Art. no. 054207.

[352] C. Lee, Z. Zhang, G. R. Steinbrecher, H. Zhou, J. Mower, T. Zhong, L. Wang, X. Hu, R. D. Horansky, V. B. Verma, A. E. Lita, R. P. Mirin, F. Marsili, M. D. Shaw, S. W. Nam, G. W. Wornell, F. N. C. Wong, J. H. Shapiro, and D. Englund, "Entanglement-based quantum communication secured by nonlocal dispersion cancellation," *Phys. Rev. A*, vol. 90, no. 6, Dec. 2014, Art. no. 062331.

[353] J. Nunn, L. J. Wright, C. Söller, L. Zhang, I. A. Walmsley, and B. J. Smith, "Large-alphabet time-frequency entangled quantum key distribution by means of time-to-frequency conversion," *Opt. Express*, vol. 21, no. 13, pp. 15959–15973, July 2013.

[354] M. Mafu, A. Dudley, S. Goyal, D. Giovannini, M. McLaren, M. J. Padgett, T. Konrad, F. Petruccione, N. Lütkenhaus, and A. Forbes, "Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases," *Phys. Rev. A*, vol. 88, no. 3, Sept. 2013, Art. no. 032305.

[355] T. K. Paraïso, T. Roger, D. G. Marangon, I. D. Marco, M. Sanzaro, R. I. Woodward, J. F. Dynes, Z. Yuan, and A. J. Shields, "A photonic integrated quantum secure communication system," *Nature Photon.*, vol. 15, no. 11, pp. 850–856, Nov. 2021.

[356] D. Kreutz, F. M. V. Ramos, P. E. Veríssimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: A comprehensive survey," *Proc. IEEE*, vol. 103, no. 1, pp. 14–76, Jan. 2015.

[357] D. B. Rawat and S. R. Reddy, "Software defined networking architecture, security and energy efficiency: A survey," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 325–346, 1st Quart., 2017.

[358] T. S. Humble and R. J. Sadlier, "Software-defined quantum communication systems," *Proc. SPIE, Quantum Commun. Quantum Imag. XI*, vol. 8875, Sept. 2013, Art. no. 88750R.

[359] V. R. Dasari, R. J. Sadlier, R. Prout, B. P. Williams, and T. S. Humble, "Programmable multi-node quantum network design and simulation," *Proc. SPIE, Quantum Inf. Comput. IX*, vol. 9873, May 2016, Art. no. 98730B.

[360] V. R. Dasari, R. J. Sadlier, B. E. Geerhart, N. A. Snow, B. P. Williams, and T. S. Humble, "Software-defined network abstractions and configuration interfaces for building programmable quantum networks," *Proc. SPIE, Advanced Photon Counting Techniques XI*, vol. 10212, May 2017, Art. no. 102120U.

[361] W. Yu, B. Zhao, and Z. Yan, "Software defined quantum key distribution network," in *Proc. 3rd IEEE Int. Conf. Comput. Commun.*, Chengdu, China, Dec. 2017, pp. 1293–1297.

[362] H. Zhang, D. Quan, C. Zhu, and Z. Li, "A quantum cryptography communication network based on software defined network," *ITM Web Conf.*, vol. 17, Feb. 2018, Art. no. 01008.

[363] T. S. Humble, R. J. Sadlier, B. P. Williams, and R. C. Prout, "Software-defined quantum network switching," *Proc. SPIE, Disruptive Technol. Inf. Sci.*, vol. 10652, May 2018, Art. no. 106520B.

[364] H. Wang, Y. Zhao, and A. Nag, "Quantum-key-distribution (QKD) networks enabled by software-defined networks (SDN)," *Appl. Sci.*, vol. 9, no. 10, May 2019, Art. no. 2081.

[365] Y. Cao, Y. Zhao, X. Yu, L. Cheng, Z. Li, G. Liu, and J. Zhang, "Experimental demonstration of end-to-end key on demand service provisioning over quantum key distribution networks with software defined networking," in *Proc. Opt. Fiber Commun. Conf.*, San Diego, CA, USA, Mar. 2019, Art. no. Th1G.4.

[366] J. Y. Cho, T. Szyrkowiec, and H. Griesser, "Quantum key distribution as a service," in *Proc. 7th Int. Conf. Quantum Crypt.*, Cambridge, UK, Sept. 2017.

[367] A. Aguado, V. Lopez, J. Martinez-Mateo, M. Peev, D. Lopez, and V. Martin, "GMPLS network control plane enabling quantum encryption in end-to-end services," in *Proc. Int. Conf. Optical Network Design and Modelling*, Budapest, Hungary, May 2017.

[368] A. Aguado, V. Lopez, J. Martinez-Mateo, M. Peev, D. Lopez, and V. Martin, "Virtual network function deployment and service automation to provide end-to-end quantum encryption," *J. Opt. Commun. Netw.*, vol. 10, no. 4, pp. 421–430, Apr. 2018.

[369] E. Hugues-Salas, F. Ntavou, Y. Ou, J. E. Kennard, C. White, D. Gkounis, K. Nikolovgenis, G. Kanellos, C. Erven, A. Lord, R. Nejabati, and D. Simeonidou, "Experimental demonstration of DDoS mitigation over a quantum key distribution (QKD) network using software defined networking (SDN)," in *Proc. Opt. Fiber Commun. Conf.*, San Diego, California, USA, Mar. 2018, Art. no. M2A.6.

[370] E. Hugues-Salas, F. Ntavou, D. Gkounis, G. T. Kanellos, R. Nejabati, and D. Simeonidou, "Monitoring and physical-layer attack mitigation in SDN-controlled quantum key distribution networks," *J. Opt. Commun. Netw.*, vol. 11, no. 2, pp. A209–A218, Feb. 2019.

[371] V. I. Egorov, V. V. Chistyakov, O. L. Sadov, A. B. Vasiliev, P. V. Fedchenkov, V. A. Grudinin, O. I. Lazo, A. E. Shevel, N. V. Buldakov, S. M. Kynev, A. V. Gleim, S. E. Khoruzhnikov, and S. A. Kozlov, "Software-defined subcarrier wave quantum networking operated by OpenFlow protocol," in *Proc. 7th Int. Conf. Quantum Crypt.*, Cambridge, UK, Sept. 2017.

[372] Y. Ou, E. Hugues-Salas, F. Ntavou, R. Wang, Y. Bi, S. Yan, G. Kanellos, R. Nejabati, and D. Simeonidou, "Field-trial of machine learning-assisted quantum key distribution (QKD) networking with SDN," in *Proc. Eur. Conf. Opt. Commun.*, Rome, Italy, Sept. 2018.

[373] V. López, A. Gomez, A. Aguado, O. Gonzalez, V. Martin, J. P. Fernandez-Palacios, and D. Lopez, "Extension of the ONF transport API to enable quantum encryption in end-to-end services," in *Proc. Eur. Conf. Opt. Commun.*, Dublin, Ireland, Sept. 2019.

[374] Q. Chen, E. Segev, E. Varma, G. Zhang, H. Ding, I. Busi, J. He, K. Sethuraman, L. Ong, N. Davis, R. Vilalta, S. Bellotti, and V. Lopez, "Functional requirements for transport API," ONF TR-527, June 2016.

[375] A. Aguado, D. R. López, A. Pastor, V. López, J. P. Brito, M. Peev, A. Poppe, and V. Martín, "Quantum cryptography networks in support of path verification in service function chains," *J. Opt. Commun. Netw.*, vol. 12, no. 4, pp. B9–B19, Apr. 2020.

[376] P. K. Tysowski, X. Ling, N. Lütkenhaus, and M. Mosca, "The engineering of a scalable multi-site communications system utilizing quantum key distribution (QKD)," *Quantum Sci. Technol.*, vol. 3, no. 2,

Jan. 2018, Art. no. 024001.

[377] Y. Cao, Y. Zhao, Y. Wu, X. Yu, and J. Zhang, "Time-scheduled quantum key distribution (QKD) over WDM networks," *J. Lightwave Technol.*, vol. 36, no. 16, pp. 3382–3395, Aug. 2018.

[378] Y. Cao, Y. Zhao, J. Wang, X. Yu, Z. Ma, and J. Zhang, "Cost-efficient quantum key distribution (QKD) over WDM networks," *J. Opt. Commun. Netw.*, vol. 11, no. 6, pp. 285–298, June 2019.

[379] Y. Zhao, Y. Cao, X. Yu, and J. Zhang, "Software defined optical networks secured by quantum key distribution (QKD)," in *Proc. IEEE/CIC Int. Conf. Commun. in China*, Qingdao, China, Oct. 2017.

[380] X. Ning, Y. Zhao, X. Yu, Y. Cao, Q. Ou, Z. Liu, X. Liao, and J. Zhang, "Soft-reservation based resource allocation in optical networks secured by quantum key distribution (QKD)," in *Proc. Asia Commun. Photon. Conf.*, Guangzhou, China, Nov. 2017, Art. no. Su2A.66.

[381] S. Bahrani, M. Razavi, and J. A. Salehi, "Wavelength assignment in hybrid quantum-classical networks," *Sci. Rep.*, vol. 8, Feb. 2018, Art. no. 3456.

[382] S. Bahrani, O. Elmabrok, G. C. Lorenzo, and M. Razavi, "Wavelength assignment in quantum access networks with hybrid wireless-fiber links," *J. Opt. Soc. Am. B*, vol. 36, no. 3, pp. B99–B108, Mar. 2019.

[383] J. Niu, Y. Sun, Y. Zhang, and Y. Ji, "Noise-suppressing channel allocation in dynamic DWDM-QKD networks using LightGBM," *Opt. Express*, vol. 27, no. 22, pp. 31741–31756, Oct. 2019.

[384] J. Niu, Y. Sun, X. Jia, and Y. Ji, "Key-size-driven wavelength resource sharing scheme for QKD and the time-varying data services," *J. Lightwave Technol.*, vol. 39, no. 9, pp. 2661–2672, May 2021.

[385] R. Wang, S. K. Joshi, G. T. Kanellos, D. Aktas, J. Rarity, R. Nejabati, and D. Simeonidou, "AI-enabled large-scale entanglement distribution quantum networks," in *Proc. Opt. Fiber Commun. Conf.*, San Francisco, CA, USA, June 2021, Art. no. Tu1I.4.

[386] C. Cai, Y. Sun, J. Niu, P. Zhang, Y. Zhang, and Y. Ji, "Multicore-fiber-based quantum-classical access network architecture with quantum signal wavelength-time division multiplexing," *J. Opt. Soc. Am. B*, vol. 37, no. 4, pp. 1047–1053, Apr. 2020.

[387] E. E. Moghaddam, H. Beyranvand, and J. A. Salehi, "Resource allocation in space division multiplexed elastic optical networks secured with quantum key distribution," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 9, pp. 2688–2700, Sept. 2021.

[388] X. Yu, S. Li, Y. Zhao, Y. Cao, A. Nag, and J. Zhang, "Routing, core and wavelength allocation in multi-core-fiber-based quantum-key-distribution-enabled optical networks," *IEEE Access*, vol. 9, pp. 99842–99852, July 2021.

[389] Y. Cao, Y. Zhao, J. Li, R. Lin, J. Zhang, and J. Chen, "Multi-tenant provisioning for quantum key distribution networks with heuristics and reinforcement learning: A comparative study," *IEEE Trans. Netw. Service Manag.*, vol. 17, no. 2, pp. 946–957, June 2020.

[390] Y. Cao, Y. Zhao, X. Yu, and J. Zhang, "Secure virtual optical network embedding over optical networks integrated with quantum key distribution," in *Proc. Asia Commun. Photon. Conf.*, Guangzhou, China, Nov. 2017, Art. no. S4C.4.

[391] X. Yu, Y. Wang, L. Lu, Y. Zhao, H. Zhang, and J. Zhang, "VON embedding in elastic optical networks (EON) integrated with quantum key distribution (QKD)," *Opt. Fiber Technol.*, vol. 63, Mar. 2021, Art. no. 102486.

[392] K. Dong, Y. Zhao, T. Yang, Y. Li, A. Nag, X. Yu, and J. Zhang, "Tree-topology-based quantum-key-relay strategy for secure multicast services," *J. Opt. Commun. Netw.*, vol. 12, no. 5, pp. 120–132, May 2020.

[393] H. Wang, Y. Zhao, M. Tornatore, X. Yu, and J. Zhang, "Dynamic secret-key provisioning in quantum-secured passive optical networks (PONs)," *Opt. Express*, vol. 29, no. 2, pp. 1578–1596, Jan. 2021.

[394] X. Cheng, Y. Sun, and Yuefeng Ji, "A QoS-supported scheme for quantum key distribution," in *Proc. Int. Conf. Advanced Intelligence and Awareness Internet*, Shenzhen, China, Oct. 2011, pp. 220–224.

[395] J. Moy, "OSPF version 2," IETF RFC 2328, Apr. 1998.

[396] M. Dianati, R. Alléaume, M. Gagnaire, and X. Shen, "Architecture and protocols of the future European quantum key distribution network," *Security Commun. Networks*, vol. 1, no. 1, pp. 57–74, Feb. 2008.

[397] C. E. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 24, no. 4, pp. 234–244, Oct. 1994.

[398] Y. Wang, Q. Li, Q. Han, and Y. Wang, "Modeling and simulation of practical quantum secure communication network," *Quantum Inf. Process.*, vol. 18, no. 9, Sept. 2019, Art. no. 278.

[399] Y. Tanizawa, R. Takahashi, and A. R. Dixon, "A routing method designed for a quantum key distribution network," in *Proc. 8th Int. Conf. Ubiquitous and Future Networks*, Vienna, Austria, July 2016, pp. 208–214.

[400] C. le Quoc, P. Bellot, and A. Demaille, "Stochastic routing in large grid-shaped quantum networks," in *Proc. IEEE Int. Conf. Research, Innovation and Vision for the Future*, Hanoi, Vietnam, Mar. 2007, pp. 166–174.

[401] H. Wen, Z. Han, Y. Zhao, G. Guo, and P. Hong, "Multiple stochastic paths scheme on partially-trusted relay quantum key distribution network," *Sci. China Ser. F-Inf. Sci.*, vol. 52, no. 1, pp. 18–22, Jan. 2009.

[402] Q. Han, L. Yu, W. Zheng, N. Cheng, and X. Niu, "A novel QKD network routing algorithm based on optical-path-switching," *J. Inf. Hiding Multimedia Signal Process.*, vol. 5, no. 1, pp. 13–19, Jan. 2014.

[403] C. Yang, H. Zhang, and J. Su, "The QKD network: Model and routing scheme," *J. Mod. Opt.*, vol. 64, no. 21, pp. 2350–2362, Aug. 2017.

[404] C. Yang, H. Zhang, and J. Su, "Quantum key distribution network: Optimal secret-key-aware routing method for trust relaying," *China Commun.*, vol. 15, no. 2, pp. 33–45, Feb. 2018.

[405] M. Mehic, O. Maurhart, S. Rass, D. Komosny, F. Rezac, and M. Voznak, "Analysis of the public channel of quantum key distribution link," *IEEE J. Quantum Electron.*, vol. 53, no. 5, Oct. 2017, Art. no. 9300408.

[406] M. Pant, H. Krovi, D. Towsley, L. Tassiulas, L. Jiang, P. Basu, D. Englund, and S. Guha, "Routing entanglement in the quantum internet," *npj Quantum Inf.*, vol. 5, Mar. 2019, Art. no. 25.

[407] M. Caleffi, "Optimal routing for quantum networks," *IEEE Access*, vol. 5, pp. 22299–22312, Oct. 2017.

[408] L. Gyongyosi and S. Imre, "Decentralized base-graph routing for the quantum internet," *Phys. Rev. A*, vol. 98, no. 2, Aug. 2018, Art. no. 022310.

[409] L. Gyongyosi and S. Imre, "Entanglement-gradient routing for quantum networks," *Sci. Rep.*, vol. 7, Oct. 2017, Art. no. 14255.

[410] D. Wu, W. Yu, B. Zhao, and C. Wu, "Quantum key distribution in large scale quantum network assisted by classical routing information," *Int. J. Theor. Phys.*, vol. 53, no. 10, pp. 3503–3511, Oct. 2014.

[411] K. Chakraborty, D. Elkouss, B. Rijsman, and S. Wehner, "Entanglement distribution in a quantum network: A multicommodity flow-based approach," *IEEE Trans. Quantum Engineering*, vol. 1, Oct. 2020, Art. no. 4101321.

[412] K. Goodenough, D. Elkouss, and S. Wehner, "Optimizing repeater schemes for the quantum internet," *Phys. Rev. A*, vol. 103, no. 3, Mar. 2021, Art. no. 032610.

[413] M. Pompili, S. L. N. Hermans, S. Baier, H. K. C. Beukers, P. C. Humphreys, R. N. Schouten, R. F. L. Vermeulen, M. J. Tiggelman, L. dos S. Martins, B. Dirkse, S. Wehner, and R. Hanson, "Realization of a multinode quantum network of remote solid-state qubits," *Science*, vol. 372, no. 6539, pp. 259–264, Apr. 2021.

[414] H. Wang, Y. Zhao, X. Yu, Z. Ma, J. Wang, A. Nag, L. Yi, and J. Zhang, "Protection schemes for key service in optical networks secured by quantum key distribution (QKD)," *J. Opt. Commun. Netw.*, vol. 11, no. 3, pp. 67–78, Mar. 2019.

[415] Y. Wang, X. Yu, J. Li, Y. Zhao, X. Zhou, S. Xie, and J. Zhang, "A novel shared backup path protection scheme in time-division-multiplexing based QKD optical networks," in *Proc. Asia Commun. Photon. Conf.*, Chengdu, China, Nov. 2019, Art. no. M4C.6.

[416] H. Wang, Y. Zhao, X. Yu, A. Nag, Z. Ma, J. Wang, L. Yan, and J. Zhang, "Resilient quantum key distribution (QKD)-integrated optical networks with secret-key recovery strategy," *IEEE Access*, vol. 7, pp. 60079–60090, May 2019.

[417] Y.-L. Tang, H.-L. Yin, X. Ma, C.-H. F. Fung, Y. Liu, H.-L. Yong, T.-Y. Chen, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan, "Source attack of decoy-state quantum key distribution using phase information," *Phys. Rev. A*, vol. 88, no. 2, Aug. 2013, Art. no. 022308.

[418] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, "Trojan-horse attacks on quantum-key-distribution systems," *Phys. Rev. A*, vol. 73, no. 2, Feb. 2006, Art. no. 022320.

[419] N. Jain, E. Anisimova, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, "Trojan-horse attacks threaten the security of practical quantum cryptography," *New J. Phys.*, vol. 16, no. 12, Dec. 2014, Art. no. 123030.

[420] N. Jain, B. Stiller, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, "Risk analysis of Trojan-horse attacks on practical quantum key distribution systems," *IEEE J. Sel. Top. Quantum Electron.*, vol. 21, no. 3, May/June 2015, Art no. 6600710.

[421] V. Makarov, “Controlling passively quenched single photon detectors by bright light,” *New J. Phys.*, vol. 11, no. 6, June 2009, Art. no. 065003.

[422] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, “Hacking commercial quantum cryptography systems by tailored bright illumination,” *Nature Photon.*, vol. 4, no. 10, pp. 686–689, Oct. 2010.

[423] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, “Full-field implementation of a perfect eavesdropper on a quantum cryptography system,” *Nature Commun.*, vol. 2, June 2011, Art. no. 349.

[424] L. Lydersen, M. K. Akhlaghi, A. H. Majedi, J. Skaar, and V. Makarov, “Controlling a superconducting nanowire single-photon detector using tailored bright illumination,” *New J. Phys.*, vol. 13, no. 11, Nov. 2011, Art. no. 113042.

[425] Y.-J. Qian, D.-Y. He, S. Wang, W. Chen, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, “Hacking the quantum key distribution system by exploiting the avalanche-transition region of single-photon detectors,” *Phys. Rev. Applied*, vol. 10, no. 6, Dec. 2018, Art. no. 064062.

[426] N. Walenta, M. Soucarros, D. Stucki, D. Caselunghe, M. Domergue, M. Hagerman, R. Hart, D. Hayford, R. Houlmann, M. Legré, T. McCandlish, J.-B. Page, M. Tourville, and R. Wolterman, “Practical aspects of security certification for commercial quantum technologies,” *Proc. SPIE, Electro-Optical and Infrared Systems: Technol. Appl. XII; and Quantum Inf. Sci. Technol.*, vol. 9648, Oct. 2015, Art. no. 96480U.

[427] L. Salvail, M. Peev, E. Diamanti, R. Alléaume, N. Lütkenhaus, and T. Länger, “Security of trusted repeater quantum key distribution networks,” *J. Comput. Security*, vol. 18, no. 1, pp. 61–87, Jan. 2010.

[428] J. Cederlof and J. Larsson, “Security aspects of the authentication used in quantum cryptography,” *IEEE Trans. Inf. Theory*, vol. 54, no. 4, pp. 1735–1741, Apr. 2008.

[429] J. Y. Cho and H. Griesser, “Secure deployment of quantum key distribution in optical communication systems,” in *Proc. Photon. Networks; 18. ITG-Symp.*, Leipzig, Germany, May 2017.

[430] Y. Cao, Y. Zhao, J. Li, R. Lin, J. Zhang, and J. Chen, “Mixed relay placement for quantum key distribution chain deployment over optical networks,” in *Proc. Eur. Conf. Opt. Commun.*, Brussels, Belgium, Dec. 2020.

[431] K.-I. Kitayama, M. Sasaki, S. Araki, M. Tsubokawa, A. Tomita, K. Inoue, K. Harasawa, Y. Nagasako, and A. Takada, “Security in photonic networks: Threats and security enhancement,” *J. Lightwave Technol.*, vol. 29, no. 21, pp. 3210–3222, Nov. 2011.

[432] S. Scott-Hayward, G. O’Callaghan, and S. Sezer, “SDN security: A survey,” in *Proc. IEEE SDN Future Netw. Services*, Trento, Italy, Nov. 2013.

[433] A. Aguado, V. Lopez, J. Martinez-Mateo, T. Szyrkowiec, A. Autenrieth, M. Peev, D. Lopez, and V. Martin, “Hybrid conventional and quantum security for software defined and virtualized networks,” *J. Opt. Commun. Netw.*, vol. 9, no. 10, pp. 819–825, Oct. 2017.

[434] F. Pederzolli, F. Faticanti, and D. Siracusa, “Optimal design of practical quantum key distribution backbones for securing core transport networks,” *Quantum Rep.*, vol. 2, no. 1, pp. 114–125, Jan. 2020.

[435] R. Alléaume, F. Roueff, E. Diamanti, and N. Lütkenhaus, “Topological optimization of quantum key distribution networks,” *New. J. Phys.*, vol. 11, no. 7, July 2009, Art. no. 075002.

[436] Y. Cao, Y. Zhao, J. Li, R. Lin, J. Zhang, and J. Chen, “Hybrid trusted/untrusted relay-based quantum key distribution over optical backbone networks,” *IEEE J. Sel. Areas Commun.*, vol. 39, no. 9, pp. 2701–2718, Sept. 2021.

[437] P. D. Townsend, S. J. D. Phoenix, K. J. Blow, and S. M. Barnett, “Design of quantum cryptography systems for passive optical networks,” *Electron. Lett.*, vol. 30, no. 22, pp. 1875–1877, Oct. 1994.

[438] S. J. D. Phoenix, S. M. Barnett, P. D. Townsend, and K. J. Blow, “Multi-user quantum cryptography on optical networks,” *J. Mod. Opt.*, vol. 42, no. 6, pp. 1155–1163, June 1995.

[439] P. D. Kumavor, A. C. Beal, S. Yelin, E. Donkor, and B. C. Wang, “Comparison of four multi-user quantum key distribution schemes over passive optical networks,” *J. Lightwave Technol.*, vol. 23, no. 1, pp. 268–276, Jan. 2005.

[440] P. D. Kumavor, A. C. Beal, E. Donkor, and B. C. Wang, “Experimental multiuser quantum key distribution network using a wavelength-addressed bus architecture,” *J. Lightwave Technol.*, vol. 24, no. 8, pp. 3103–3106, Aug. 2006.

[441] V. Fernandez, R. J. Collins, K. J. Gordon, P. D. Townsend, and G. S. Buller, “Passive optical network approach to gigahertz-clocked multiuser quantum key distribution,” *IEEE J. Quantum Electron.*, vol. 43, no. 2, pp. 130–138, Feb. 2007.

[442] S. Aleksic, D. Winkler, G. Franzl, A. Poppe, B. Schrenk, and F. Hipp, “Quantum key distribution over optical access networks,” in *Proc. 18th Eur. Conf. Netw. Opt. Commun. & 8th Conf. Opt. Cabling Infrastructure*, Graz, Austria, July 2013, pp. 11–18.

[443] J. Martinez-Mateo, A. Ciurana, and V. Martin, “Quantum key distribution based on selective post-processing in passive optical networks,” *IEEE Photon. Technol. Lett.*, vol. 26, no. 9, pp. 881–884, May 2014.

[444] K. Lim, H. Ko, C. Suh, and J.-K. K. Rhee, “Security analysis of quantum key distribution on passive optical networks,” *Opt. Express*, vol. 25, no. 10, pp. 11894–11909, May 2017.

[445] O. Elmabrok, M. Ghalaii, and M. Razavi, “Quantum-classical access networks with embedded optical wireless links,” *J. Opt. Soc. Am. B*, vol. 35, no. 3, pp. 487–499, Mar. 2018.

[446] M. Razavi, “Multiple-access quantum key distribution networks,” *IEEE Trans. Commun.*, vol. 60, no. 10, pp. 3071–3079, Oct. 2012.

[447] J. C. Garcia-Escartin and P. Chamorro-Posada, “Quantum spread spectrum multiple access,” *IEEE J. Sel. Top. Quantum Electron.*, vol. 21, no. 3, May/June 2015, Art. no. 6400107.

[448] S. Bahrani, O. Elmabrok, G. C. Lorenzo, and M. Razavi, “Finite-key effects in quantum access networks with wireless links,” in *Proc. IEEE Globecom Workshops*, Abu Dhabi, United Arab Emirates, Dec. 2018.

[449] C. Cai, Y. Sun, J. Niu, and Y. Ji, “A quantum access network suitable for internetworking optical network units,” *IEEE Access*, vol. 7, pp. 92091–92099, July 2019.

[450] P. Xue, K. Wang, and X. Wang, “Efficient multiuser quantum cryptography network based on entanglement,” *Sci. Rep.*, vol. 7, Apr. 2017, Art. no. 45928.

[451] “Quantum key distribution (QKD); Use cases,” ETSI GS QKD 002 V1.1.1, June 2010.

[452] “Quantum key distribution (QKD); Security proofs,” ETSI GS QKD 005 V1.1.1, Dec. 2010.

[453] “Quantum key distribution (QKD); Vocabulary,” ETSI GR QKD 007 V1.1.1, Dec. 2018.

[454] “Quantum key distribution (QKD); QKD module security specification,” ETSI GS QKD 008 V1.1.1, Dec. 2010.

[455] “Quantum key distribution (QKD); Component characterization: Characterizing optical components for QKD systems,” ETSI GS QKD 011 V1.1.1, May 2016.

[456] “Quantum key distribution (QKD); Implementation security: Protection against Trojan horse attacks in one-way QKD systems,” ETSI GS QKD 010, drafting.

[457] “Quantum key distribution (QKD); Characterisation of optical output of QKD transmitter modules,” ETSI GS QKD 013, drafting.

[458] “Quantum key distribution (QKD); Common criteria protection profile for QKD,” ETSI GS QKD 016, drafting.

[459] “Quantum key distribution (QKD); Network architectures,” ETSI GR QKD 017, drafting.

[460] “Quantum key distribution (QKD); Orchestration interface of software defined networks,” ETSI GS QKD 018, drafting.

[461] “Quantum key distribution (QKD); Design of QKD interfaces with authentication,” ETSI GR QKD 019, drafting.

[462] “Functional requirements for quantum key distribution networks,” Recommendation ITU-T Y.3801, Apr. 2020.

[463] “Quantum key distribution networks - Functional architecture,” Recommendation ITU-T Y.3802, Dec. 2020.

[464] “Quantum key distribution networks - Control and management,” Recommendation ITU-T Y.3804, Sept. 2020.

[465] “Quantum key distribution networks - Requirements for quality of service assurance,” Recommendation ITU-T Y.3806, Sept. 2021.

[466] “Quantum noise random number generator architecture,” Recommendation ITU-T X.1702, Nov. 2019.

[467] “Security framework for quantum key distribution networks,” Recommendation ITU-T X.1710, Oct. 2020.

[468] “Security requirements and measures for quantum key distribution networks - Key management,” Recommendation ITU-T X.1712, Oct. 2021.

[469] “Key combination and confidential key supply for quantum key distribution networks,” Recommendation ITU-T X.1714, Oct. 2020.

[470] “Quantum key distribution networks - QoS parameters,” Recommendation ITU-T Y.3807, drafting.

[471] "Framework for integration of quantum key distribution network and secure storage network," Recommendation ITU-T Y.3808, drafting.

[472] "Quantum key distribution networks - Business role-based models," Recommendation ITU-T Y.3809, drafting.

[473] "Functional architecture of QoS assurance for quantum key distribution networks," Recommendation ITU-T Y.QKDN-qos-fa, drafting.

[474] "Security requirements and designs for quantum key distribution networks - Trusted node," Recommendation ITU-T X.sec-QKDN-tn, drafting.

[475] "Security requirements for integration of QKDN and secure network infrastructures," Recommendation ITU-T X.sec_QKDN_intrq, drafting.

[476] "Security requirements and measures for quantum key distribution networks - Control and management," Recommendation ITU-T X.sec_QKDN_CM, drafting.

[477] "Authentication and authorization in QKDN using quantum safe cryptography," Recommendation ITU-T X.sec_QKDN_AA, drafting.

[478] "Security requirements, test and evaluation methods for quantum key distribution – Part 1: Requirements," ISO/IEC CD 23837-1, drafting.

[479] "Security requirements, test and evaluation methods for quantum key distribution – Part 2: Evaluation and testing methods," ISO/IEC CD 23837-2, drafting.

[480] W. Kozlowski, S. Wehner, R. V. Meter, B. Rijsman, A. S. Cacciapuoti, M. Caleffi, and S. Nagayama, "Architectural principles for a quantum internet," draft-irtf-qirg-principles-07, June 2021.

[481] C. Wang, A. Rahman, R. Li, M. Aelmans, and K. Chakraborty, "Applications and use cases for the quantum internet," draft-irtf-qirg-quantum-internet-use-cases-07, July 2021.

[482] "Software-defined quantum communication," IEEE P1913, drafting.

[483] "What is quantum key distribution?," CSA Quantum-Safe Security Working Group, Aug. 2015.

[484] T. Länger and G. Lenhart, "Standardization of quantum key distribution and the ETSI standardization initiative ISG-QKD," *New. J. Phys.*, vol. 11, no. 5, May 2009, Art. no. 055051.

[485] W. Weigel and G. Lenhart, "Standardization of quantum key distribution in ETSI," *Wirel. Pers. Commun.*, vol. 58, no. 1, pp. 145–157, May 2011.

[486] W. Simpson, "The point-to-point protocol (PPP)," IETF RFC 1661, July 1994.

[487] "IEEE standard for local and metropolitan area networks–Media access control (MAC) security," IEEE Std 802.1AE-2018, Dec. 2018.

[488] G. Meyer, "The PPP encryption control protocol (ECP)," IETF RFC 1968, June 1996.

[489] S. Kent and K. Seo, "Security architecture for the Internet protocol," IETF RFC 4301, Dec. 2005.

[490] C. Kaufman, P. Hoffman, Y. Nir, P. Eronen, and T. Kivinen, "Internet key exchange protocol version 2 (IKEv2)," IETF RFC 7296, Oct. 2014.

[491] S. Marksteiner and O. Maurhart, "A protocol for synchronizing quantum-derived keys in IPsec and its implementation," in *Proc. 9th Int. Conf. Quantum, Nano/Bio, and Micro Technologies*, Venice, Italy, Aug. 2015, pp. 35–40.

[492] E. Rescorla, "The transport layer security (TLS) protocol version 1.3," IETF RFC 8446, Aug. 2018.

[493] A. Freier, P. Karlton, and P. Kocher, "The secure sockets layer (SSL) protocol version 3.0," IETF RFC 6101, Aug. 2011.

[494] A. Poppe, A. Fedrizzi, R. Ursin, H. R. Böhm, T. Lorünser, O. Maurhardt, M. Peev, M. Suda, C. Kurtsiefer, H. Weinfurter, T. Jennewein, and A. Zeilinger, "Practical quantum key distribution with polarization entangled photons," *Opt. Express*, vol. 12, no. 16, pp. 3865–3871, Aug. 2004.

[495] S. Ghernaouti-Hélie and M. A. Sfaxi, "Guaranteeing security of financial transaction by using quantum cryptography in banking environment," in *Proc. Int. Conf. E-Business Telecommun. Netw.*, Reading, UK, Oct. 2005, pp. 268–274.

[496] A. Sharma and S. K. Lenka, "Authentication in online banking systems through quantum cryptography," *Int. J. Eng. Technol.*, vol. 5, no. 3, pp. 2696–2700, June/July 2013.

[497] Securing Data Transfer for Elections: Ethernet Encryption with Quantum Key Distribution [Online]. Available: https://marketing.idquantique.com/acton/attachment/11868/f-020f/1/-/-/-/-/Geneva%20Govt_%20DCI%20QKD%20Use%20Case.pdf.

[498] D. S. Sundar and N. Narayan, "A novel voting scheme using quantum cryptography," in *Proc. IEEE Conf. Open Systems*, Subang, Malaysia, Oct. 2014, pp. 66–71.

[499] M. Niemiec and P. Machnik, "Authentication in virtual private networks based on quantum key distribution methods," *Multimedia Tools Appl.*, vol. 75, no. 17, pp. 10691–10707, Sept. 2016.

[500] A. Aguado, V. López, J. Martinez-Mateo, M. Peev, D. López, and V. Martín, "VPN service provisioning via virtual router deployment and quantum key distribution," in *Proc. Opt. Fiber Commun. Conf.*, San Diego, California, USA, Mar. 2018, Art. no. Th2A.32.

[501] Senetas Technology in Netherlands' First Commercial Quantum Cryptography Project [Online]. Available: http://www.prweb.com/releases/2010/10/prweb4670214.htm.

[502] KPN to Implement Quantum Encrypted Connection (QKD) [Online]. Available: https://www.overons.kpn/nieuws/en/kpn-to-implement-quantum-encrypted-connection-qkd.

[503] L. Huang, H. Zhou, K. Feng, and C. Xie, "Quantum random number cloud platform," *npj Quantum Inf.*, vol. 7, July 2021, Art. no. 107.

[504] L. Zhou, Q. Wang, X. Sun, P. Kulicki, and A. Castiglione, "Quantum technique for access control in cloud computing II: Encryption and key distribution," *J. Network Comput. Appl.*, vol. 103, pp. 178–184, Feb. 2018.

[505] G. Sharma and S. Kalra, "Identity based secure authentication scheme based on quantum key distribution for cloud computing," *Peer-to-Peer Netw. Appl.*, vol. 11, no. 2, pp. 220–234, Mar. 2018.

[506] J. Han, Y. Liu, X. Sun, and L. Song, "Enhancing data and privacy security in mobile cloud computing through quantum cryptography," in *Proc. 7th IEEE Int. Conf. Software Engineering and Service Science*, Beijing, China, Aug. 2016, pp. 398–401.

[507] B. Kelley, J. J. Prevost, P. Rad, and A. Fatima, "Securing cloud containers using quantum networking channels," in *Proc. IEEE Int. Conf. Smart Cloud*, New York, NY, USA, Nov. 2016, pp. 103–111.

[508] G. Murali and R. S. Prasad, "CloudQKDP: Quantum key distribution protocol for cloud computing," in *Proc. Int. Conf. Inf. Commun. Embedded Systems*, Chennai, India, Feb. 2016.

[509] Q.-C. Le and P. Bellot, "Enhancement of AGT telecommunication security using quantum cryptography," in *Proc. Int. Conf. Research, Innovation and Vision for the Future*, Ho Chi Minh City, Vietnam, Feb. 2006, pp. 7–16.

[510] L. Wang, D. Wang, J. Gao, C. Huo, H. Bai, and J. Yuan, "Research on multi-source data security protection of smart grid based on quantum key combination," in *Proc. IEEE 4th Int. Conf. Cloud Computing and Big Data Analysis*, Chengdu, China, Apr. 2019, pp. 449–453.

[511] M. Sasaki, "Quantum key distribution and its applications," *IEEE Secur. Priv.*, vol. 16, no. 5, pp. 42–48, Sept./Oct. 2018.

[512] M. Thangapandiyan, P. M. R. Anand, and K. S. Sankaran, "Quantum key distribution and cryptography mechanisms for cloud data security," in *Proc. Int. Conf. Commun. Signal Process.*, Chennai, India, Apr. 2018, pp. 1031–1035.

[513] World-first Demonstration of Real-time Transmission of Whole-genome Sequence Data Using Quantum Cryptography [Online]. Available: https://www.global.toshiba/ww/technology/corporate/rdc/rd/topics/20/2001-01.html.

[514] J. M. P. Armengol, B. Furch, C. J. de Matos, O. Minster, L. Cacciapuoti, M. Pfennigbauer, M. Aspelmeyer, T. Jennewein, R. Ursin, T. Schmitt-Manderbach, G. Baister, J. Rarity, W. Leeb, C. Barbieri, H. Weinfurter, and A. Zeilinger, "Quantum communications at ESA: Towards a space experiment on the ISS," *Acta Astronautica*, vol. 63, no. 1–4, pp. 165–178, July/Aug. 2008.

[515] A. Tajima, T. Kondoh, T. Ochi, M. Fujiwara, K. Yoshino, H. Iizuka, T. Sakamoto, A. Tomita, S. Asami, and M. Sasaki, "Quantum key distribution network and its applications," in *Proc. IEEE Photon. Soc. Summer Top. Meeting Ser.*, Waikoloa Village, HI, USA, July 2018, pp. 69–70.

[516] T. M. T. Nguyen, M. A. Sfaxi, and S. Ghernaouti-Helie, "Integration of quantum cryptography in 802.11 networks," in *Proc. 1st Int. Conf. Availability, Reliability and Security*, Vienna, Austria, Apr. 2006.

[517] S. Suchat, W. Khunnam, and P. P. Yupapin, "Quantum key distribution via an optical wireless communication link for telephone networks," *Opt. Eng.*, vol. 46, no. 10, Oct. 2007, Art. no. 100502.

[518] QuantumCTek Security Mobile Phone [Online]. Available: http://www.quantum-info.com/English/product/ptwo/yidongjiamiyingyongchanpin/2018/0118/477.html.

[519] China Telecom Launches Quantum Encrypted Phone Calls on Smartphones in a New Pilot Programme [Online]. Available: https://www.thestar.com.my/tech/tech-news/2021/01/07/china-telecom-launches-quantum-encrypted-phone-calls-on-smartphones-in-a-new-pilot-programme.

[520] R. Wang, R. S. Tessinari, E. Hugues-Salas, A. Bravalheri, N. Uniyal, A. S. Muqaddas, R. S. Guimaraes, T. Diallo, S. Moazzeni, Q. Wang, G. T. Kanellos, R. Nejabati, and D. Simeonidou, “End-to-end quantum secured inter-domain 5G service orchestration over dynamically switched flex-grid optical networks enabled by a q-ROADM,” *J. Lightwave Technol.*, vol. 38, no. 1, pp. 139–149, Jan. 2020.

[521] P. Wright, C. White, R. C. Parker, J.-S. Pegon, M. Menchetti, J. Pearse, A. Bahrami, A. Moroz, A. Wonfor, R. V. Penty, T. P. Spiller, and A. Lord, “5G network slicing with QKD and quantum-safe security,” *J. Opt. Commun. Netw.*, vol. 13, no. 3, pp. 33–40, Mar. 2021.

[522] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, “Network information flow,” *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1204–1216, July 2000.

[523] F.-H. Xu, H. Wen, Z.-F. Han, and G.-C. Guo, “Network coding in trusted relay based quantum network,” [Online]. Available: http://individual.utoronto.ca/Tiger_Xu/Research_files/NCodingQKD.pdf.

[524] H. V. Nguyen, P. V. Trinh, A. T. Pham, Z. Babar, D. Alanis, P. Botsinis, D. Chandra, S. X. Ng, and L. Hanzo, “Network coding aided cooperative quantum key distribution over free-space optical channels,” *IEEE Access*, vol. 5, pp. 12301–12317, July 2017.

[525] M. Hayashi, K. Iwama, H. Nishimura, R. Raymond, and S. Yamashita, “Quantum network coding,” in *Proc. Annu. Symp. Theoretical Aspects Comput. Sci., Lecture Notes in Computer Science*, vol. 4393, pp. 610–621, 2007.

[526] J. Li, X.-B. Chen, G. Xu, Y.-X. Yang, and Z.-P. Li, “Perfect quantum network coding independent of classical network solutions,” *IEEE Commun. Lett.*, vol. 19, no. 3, pp. 115–118, Feb. 2015.

[527] T. Shang, J. Li, and J. Liu, “Secure quantum network coding for controlled repeater networks,” *Quantum Inf. Process.*, vol. 15, no. 7, pp. 2937–2953, Apr. 2016.

[528] T. Satoh, K. Ishizaki, S. Nagayama, and R. V. Meter, “Analysis of quantum network coding for realistic repeater networks,” *Phys. Rev. A*, vol. 93, no. 3, Mar. 2016, Art. no. 032302.

[529] T. Shang, X. Zhao, and J. Liu, “Quantum network coding based on controlled teleportation,” *IEEE Commun. Lett.*, vol. 18, no. 5, pp. 865–868, May 2014.

[530] H. V. Nguyen, Z. Babar, D. Alanis, P. Botsinis, D. Chandra, M. A. M. Izhar, S. X. Ng, and L. Hanzo, “Towards the quantum internet: Generalised quantum network coding for large-scale quantum communication networks,” *IEEE Access*, vol. 5, pp. 17288–17308, Aug. 2017.

[531] Q. Li, Y. Wang, H. Mao, J. Yao, and Q. Han, “Mathematical model and topology evaluation of quantum key distribution network,” *Opt. Express*, vol. 28, no. 7, pp. 9419–9434, Mar. 2020.

[532] Y. Wang, Q. Li, H. Mao, Q. Han, F. Huang, and H. Xu, “Topological optimization of hybrid quantum key distribution networks,” *Opt. Express*, vol. 28, no. 18, pp. 26348–26358, Aug. 2020.

[533] G. L. Roberts, M. Lucamarini, Z. L. Yuan, J. F. Dynes, L. C. Comandar, A. W. Sharpe, A. J. Shields, M. Curty, I. V. Puthoor, and E. Andersson, “Experimental measurement-device-independent quantum digital signatures,” *Nature Commun.*, vol. 8, Oct. 2017, Art. no. 1098.

[534] L. Oesterling, D. Hayford, and G. Friend, “Comparison of commercial and next generation quantum key distribution: Technologies for secure communication of information,” in *Proc. IEEE Conf. Technologies for Homeland Security*, Waltham, MA, USA, Nov. 2012.

[535] H. Chun, I. Choi, G. Faulkner, L. Clarke, B. Barber, G. George, C. Capon, A. Niskanen, J. Wabnig, D. O’Brien, and D. Bitauld, “Handheld free space quantum key distribution with dynamic motion compensation,” *Opt. Express*, vol. 25, no. 6, pp. 6784–6795, Mar. 2017.

[536] Y.-H. Yang, P.-Y. Li, S.-Z. Ma, X.-C. Qian, K.-Y. Zhang, L.-J. Wang, W.-L. Zhang, F. Zhou, S.-B. Tang, J.-Y. Wang, Y. Yu, Q. Zhang, and J.-W. Pan, “All optical metropolitan quantum key distribution network with post-quantum cryptography authentication,” *Opt. Express*, vol. 29, no. 16, pp. 25859–25867, Aug. 2021.

[537] A. Extance, “The future of cryptocurrencies: Bitcoin and beyond,” *Nature*, vol. 526, no. 7571, pp. 21–23, Oct. 2015.

[538] A. K. Fedorov, E. O. Kiktenko, and A. I. Lvovsky, “Quantum computers put blockchain security at risk,” *Nature*, vol. 563, no. 7732, pp. 465–467, Nov. 2018.

[539] Y.-L. Gao, X.-B. Chen, Y.-L. Chen, Y. Sun, X.-X. Niu, and Y.-X. Yang, “A secure cryptocurrency scheme based on post-quantum blockchain,” *IEEE Access*, vol. 6, pp. 27205–27213, June 2018.

[540] C.-Y. Li, X.-B. Chen, Y.-L. Chen, Y.-Y. Hou, and J. Li, “A new lattice-based signature scheme in post-quantum blockchain network,” *IEEE Access*, vol. 7, pp. 2026–2033, Jan. 2019.

[541] T. M. Fernández-Caramès and P. Fraga-Lamas, “Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks,” *IEEE Access*, vol. 8, pp. 21091–21116, Feb. 2020.

[542] E. O. Kiktenko, N. O. Pozhar, M. N. Anufriev, A. S. Trushechkin, R. R. Yunusov, Y. V. Kurochkin, A. I. Lvovsky, and A. K. Fedorov, “Quantum-secured blockchain,” *Quantum Sci. Technol.*, vol. 3, no. 3, May 2018, Art. no. 035004.

[543] X. Sun, M. Sopek, Q. Wang, and P. Kulicki, “Towards quantum-secured permissioned blockchain: Signature, consensus, and logic,” *Entropy*, vol. 21, no. 9, Sept. 2019, Art. no. 887.

[544] T. M. Fernández-Caramés, “From pre-quantum to post-quantum IoT security: A survey on quantum-resistant cryptosystems for the Internet of Things,” *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6457–6480, July 2020.

[545] R. Chaudhary, G. S. Aujla, N. Kumar, and S. Zeadally, “Lattice-based public key cryptosystem for Internet of Things environment: Challenges and solutions,” *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4897–4909, June 2019.

[546] S. Ebrahimi, S. Bayat-Sarmadi, and H. Mosanaei-Boorani, “Post-quantum cryptoprocessors optimized for edge and resource-constrained devices in IoT,” *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5500–5507, June 2019.

[547] C. Cheng, R. Lu, A. Petzoldt, and T. Takagi, “Securing the Internet of Things in a quantum world,” *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 116–120, Feb. 2017.

[548] Z. Liu, K. R. Choo, and J. Grossschadl, “Securing edge devices in the post-quantum Internet of Things using lattice-based cryptography,” *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 158–162, Feb. 2018.

[549] J. Lee, D. Kim, H. Lee, Y. Lee, and J. H. Cheon, “RLizard: Post-quantum key encapsulation mechanism for IoT devices,” *IEEE Access*, vol. 7, pp. 2080–2091, Jan. 2019.

[550] A. Khalid, S. McCarthy, M. O’Neill, and W. Liu, “Lattice-based cryptography for IoT in a quantum world: Are we ready?,” in *Proc. IEEE 8th Int. Workshop on Advances in Sensors and Interfaces*, Otranto, Italy, June 2019, pp. 194–199.

[551] U. Banerjee, A. Pathak, and A. P. Chandrakasan, “An energy-efficient configurable lattice cryptography processor for the quantum-secure Internet of Things,” in *Proc. IEEE Int. Solid-State Circuits Conf.*, San Francisco, CA, USA, Feb. 2019, pp. 46–48.

[552] S. K. Routray, M. K. Jha, L. Sharma, R. Nyamangoudar, A. Javali, and S. Sarkar, “Quantum cryptography for IoT: A perspective,” in *Proc. Int. Conf. IoT Appl.*, Nagapattinam, India, May 2017.

[553] A. Mavromatis, F. Ntavou, E. H. Salas, G. T. Kanellos, R. Nejabati, and D. Simeonidou, “Experimental demonstration of quantum key distribution (QKD) for energy-efficient software-defined Internet of Things,” in *Proc. Eur. Conf. Opt. Commun.*, Rome, Italy, Sept. 2018.

[554] G. T. Kanellos, F. Ntavou, A. Mavromatis, R. Wang, E. H. Salas, S. Yan, R. Nejabati, and D. Simeonidou, “Quantum key distribution: Scenarios for application and co-existence in optical metro and IoT networks,” in *Proc. Int. Photon. Optoelectron. Meeting*, Wuhan, China, Nov. 2018, Art. no. OF2A.2.

[555] M. S. Rahman and M. Hossam-E-Haider, “Quantum IoT: A quantum approach in IoT security maintenance,” in *Proc. Int. Conf. Robotics, Electrical and Signal Processing Techniques*, Dhaka, Bangladesh, Jan. 2019, pp. 269–272.

[556] L. Hanzo, H. Haas, S. Imre, D. O’Brien, M. Rupp, and L. Gyongyosi, “Wireless myths, realities, and futures: From 3G/4G to optical and quantum wireless,” *Proc. IEEE*, vol. 100, pp. 1853–1888, May 2012.

[557] B. Sujatha, S. V. Raju, and G. S. Rao, “Proficient capability of QKD in Wi-Fi network system implementation,” in *Proc. Int. Conf. Commun. Electron. Systems*, Coimbatore, India, Oct. 2016.

[558] A. Aguado, D. R. Lopez, V. Lopez, F. de la Iglesia, A. Pastor, M. Peev, W. Amaya, F. Martin, C. Abellan, and V. Martin, “Quantum technologies in support for 5G services: Ordered proof-of-transit,” in *Proc. Eur. Conf. Opt. Commun.*, Dublin, Ireland, Sept. 2019.

[559] V. Lopez, A. Pastor, D. Lopez, A. Aguado, and V. Martin, “Applying QKD to improve next-generation network infrastructures,” in *Proc. Eur. Conf. Netw. Commun.*, Valencia, Spain, June 2019, pp. 283–288.

[560] C. Q. Choi, “World’s first “quantum drone” for impenetrable air-to-ground data links takes off,” *IEEE Spectr.*, June 2019.

[561] H.-Y. Liu, X.-H. Tian, C. Gu, P. Fan, X. Ni, R. Yang, J.-N. Zhang, M. Hu, J. Guo, X. Cao, X. Hu, G. Zhao, Y.-Q. Lu, Y.-X. Gong, Z. Xie, and S.-N. Zhu, “Drone-based entanglement distribution towards mobile quantum

networks," *Natl. Sci. Rev.*, vol. 7, no. 5, pp. 921–928, May 2020.

[562] H.-Y. Liu, X.-H. Tian, C. Gu, P. Fan, X. Ni, R. Yang, J.-N. Zhang, M. Hu, J. Guo, X. Cao, X. Hu, G. Zhao, Y.-Q. Lu, Y.-X. Gong, Z. Xie, and S.-N. Zhu, "Optical-relayed entanglement distribution using drones as mobile nodes," *Phys. Rev. Lett.*, vol. 126, no. 2, Jan. 2021, Art. no. 020503.

[563] O. Elmabrok and M. Razavi, "Wireless quantum key distribution in indoor environments," *J. Opt. Soc. Am. B*, vol. 35, no. 2, pp. 197–207, Feb. 2018.

[564] C. Ottaviani, M. J. Woolley, M. Erementchouk, J. F. Federici, P. Mazumder, S. Pirandola, and C. Weedbrook, "Terahertz quantum cryptography," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 3, pp. 483–495, Mar. 2020.

[565] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, "Quantum entanglement," *Rev. Mod. Phys.*, vol. 81, no. 2, pp. 865–942, June 2009.

[566] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Phys. Rev. Lett.*, vol. 70, no. 13, pp. 1895–1899, Mar. 1993.

[567] T. Honjo, S. W. Nam, H. Takesue, Q. Zhang, H. Kamada, Y. Nishida, O. Tadanaga, M. Asobe, B. Baek, R. Hadfield, S. Miki, M. Fujiwara, M. Sasaki, Z. Wang, K. Inoue, and Y. Yamamoto, "Long-distance entanglement-based quantum key distribution over optical fiber," *Opt. Express*, vol. 16, no. 23, pp. 19118–19126, Dec. 2008.

[568] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, "Entanglement-based quantum communication over 144 km," *Nature Phys.*, vol. 3, no. 7, pp. 481–486, July 2007.

[569] A. Ciurana, V. Martin, J. Martinez-Mateo, B. Schrenk, M. Peev, and A. Poppe, "Entanglement distribution in optical networks," *IEEE J. Sel. Top. Quantum Electron.*, vol. 21, no. 3, May/June 2015, Art. no. 6400212.

[570] S. Wengerowsky, S. K. Joshi, F. Steinlechner, J. R. Zichi, S. M. Dobrovolskiy, R. van der Molen, J. W. N. Los, V. Zwiller, M. A. M. Versteegh, A. Mura, D. Calonico, M. Inguscio, H. Hübel, L. Bo, T. Scheidl, A. Zeilinger, A. Xuereb, and R. Ursin, "Entanglement distribution over a 96-km-long submarine optical fiber," *PNAS*, vol. 116, no. 14, pp. 6684–6688, Apr. 2019.

[571] M. Sasaki, M. Fujiwara, R.-B. Jin, M. Takeoka, T. S. Han, H. Endo, K.-I. Yoshino, T. Ochi, S. Asami, and A. Tajima, "Quantum photonic network: Concept, basic tools, and future issues," *IEEE J. Sel. Top. Quantum Electron.*, vol. 21, no. 3, May/June 2015, Art. no. 6400313.

[572] S. Wengerowsky, S. K. Joshi, F. Steinlechner, H. Hübel, and R. Ursin, "An entanglement-based wavelength-multiplexed quantum communication network," *Nature*, vol. 564, no. 7735, pp. 225–228, Dec. 2018.

[573] A. Pirker and W. Dür, "A quantum network stack and protocols for reliable entanglement-based networks," *New J. Phys.*, vol. 21, no. 3, Mar. 2019, Art. no. 033003.

[574] J. I. Cirac, P. Zoller, H. J. Kimble, and H. Mabuchi, "Quantum state transfer and entanglement distribution among distant nodes in a quantum network," *Phys. Rev. Lett.*, vol. 78, no. 16, pp. 3221–3224, Apr. 1997.

[575] X.-X. Xia, Q.-C. Sun, Q. Zhang, and J.-W. Pan, "Long distance quantum teleportation," *Quantum Sci. Technol.*, vol. 3, no. 1, Dec. 2017, Art. no. 014012.

[576] R. Valivarthi, M. G. Puigibert, Q. Zhou, G. H. Aguilar, V. B. Verma, F. Marsili, M. D. Shaw, S. W. Nam, D. Oblak, and W. Tittel, "Quantum teleportation across a metropolitan fibre network," *Nature Photon.*, vol. 10, no. 10, pp. 676–680, Oct. 2016.

[577] Q.-C. Sun, Y.-L. Mao, S.-J. Chen, W. Zhang, Y.-F. Jiang, Y.-B. Zhang, W.-J. Zhang, S. Miki, T. Yamashita, H. Terai, X. Jiang, T.-Y. Chen, L.-X. You, X.-F. Chen, Z. Wang, J.-Y. Fan, Q. Zhang, and J.-W. Pan, "Quantum teleportation with independent sources and prior entanglement distribution over a network," *Nature Photon.*, vol. 10, no. 10, pp. 671–675, Oct. 2016.

[578] J.-G. Ren, P. Xu, H.-L. Yong, L. Zhang, S.-K. Liao, J. Yin, W.-Y. Liu, W.-Q. Cai, M. Yang, L. Li, K.-X. Yang, X. Han, Y.-Q. Yao, J. Li, H.-Y. Wu, S. Wan, L. Liu, D.-Q. Liu, Y.-W. Kuang, Z.-P. He, P. Shang, C. Guo, R.-H. Zheng, K. Tian, Z.-C. Zhu, N.-L. Liu, C.-Y. Lu, R. Shu, Y.-A. Chen, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, "Ground-to-satellite quantum teleportation," *Nature*, vol. 549, no. 7670, pp. 70–73, Aug. 2017.

[579] R. V. Meter, "Quantum networking and internetworking," *IEEE Network*, vol. 26, no. 4, pp. 59–64, July/Aug. 2012.

[580] G. L. Long and X. S. Liu, "Theoretically efficient high-capacity quantum-key-distribution scheme," *Phys. Rev. A*, vol. 65, no. 3, Mar. 2002, Art. no. 032302.

[581] G.-L. Long, "Quantum secure direct communication: Principles, current status, perspectives," in *Proc. IEEE 85th Vehicular Technol. Conf.*, Sydney, NSW, Australia, June 2017.

[582] Z.-J. Zhang, "Multiparty quantum secret sharing of secure direct communication," *Phys. Lett. A*, vol. 342, no. 1–2, pp. 60–66, July 2005.

[583] H. Lai, J. Xiao, M. A. Orgun, L. Xue, and J. Pieprzyk, "Quantum direct secret sharing with efficient eavesdropping-check and authentication based on distributed fountain codes," *Quantum Inf. Process.*, vol. 13, no. 4, pp. 895–907, Apr. 2014.

[584] C. S. Yoon, M. S. Kang, J. I. Lim, and H. J. Yang, "Quantum signature scheme based on a quantum search algorithm," *Phys. Scr.*, vol. 90, no. 1, Dec. 2014, Art. no. 015103.

[585] G. Gao, "Two quantum dialogue protocols without information leakage," *Opt. Commun.*, vol. 283, no. 10, pp. 2288–2293, May 2010.

[586] C. Zheng and G. Long, "Quantum secure direct dialogue using Einstein-Podolsky-Rosen pairs," *Sci. China Phys. Mech. Astron.*, vol. 57, no. 7, pp. 1238–1243, July 2014.

[587] F.-G. Deng, G. L. Long, and X.-S. Liu, "Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block," *Phys. Rev. A*, vol. 68, no. 4, Oct. 2003, Art. no. 042317.

[588] F.-G. Deng and G. L. Long, "Secure direct communication with a quantum one-time pad," *Phys. Rev. A*, vol. 69, no. 5, May 2004, Art. no. 052319.

[589] D. Pan, K. Li, D. Ruan, S. X. Ng, and L. Hanzo, "Single-photon-memory two-step quantum secure direct communication relying on Einstein-Podolsky-Rosen pairs," *IEEE Access*, vol. 8, pp. 121146–121161, July 2020.

[590] Z. Sun, L. Song, Q. Huang, L. Yin, G. Long, J. Lu, and L. Hanzo, "Toward practical quantum secure direct communication: A quantum-memory-free protocol and code design," *IEEE Trans. Commun.*, vol. 68, no. 9, pp. 5778–5792, Sept. 2020.

[591] R. Qi, Z. Sun, Z. Lin, P. Niu, W. Hao, L. Song, Q. Huang, J. Gao, L. Yin, and G.-L. Long, "Implementation and security analysis of practical quantum secure direct communication," *Light: Sci. Appl.*, vol. 8, Feb. 2019, Art. no. 22.

[592] Z. Qi, Y. Li, Y. Huang, J. Feng, Y. Zheng, and X. Chen, "A 15-user quantum secure direct communication network," *Light: Sci. Appl.*, vol. 10, Sept. 2021, Art. no. 183.

[593] C.-Y. Chen, G.-J. Zeng, F.-J. Lin, Y.-H. Chou, and H.-C. Chao, "Quantum cryptography and its applications over the Internet," *IEEE Network*, vol. 29, no. 5, pp. 64–69, Sept./Oct. 2015.

[594] M. Geihs, O. Nikiforov, D. Demirel, A. Sauer, D. Butin, F. Günther, G. Alber, T. Walther, and J. Buchmann, "The status of quantum-key-distribution-based long-term secure Internet communication," *IEEE Trans. Sustainable Comput.*, vol. 6, no. 1, pp. 19–29, Jan.-Mar. 2021.

[595] K. Azuma, A. Mizutani, and H.-K. Lo, "Fundamental rate-loss trade-off for the quantum internet," *Nature Commun.*, vol. 7, Nov. 2016, Art. no. 13523.

[596] K. Azuma and G. Kato, "Aggregating quantum repeaters for the quantum internet," *Phys. Rev. A*, vol. 96, no. 3, Sept. 2017, Art. no. 032332.

[597] A. S. Cacciapuoti, M. Caleffi, F. Tafuri, F. S. Cataliotti, S. Gherardini, and G. Bianchi, "Quantum internet: Networking challenges in distributed quantum computing," *IEEE Network*, vol. 34, no. 1, pp. 137–143, Jan./Feb. 2020.

[598] M. Caleffi and A. S. Cacciapuoti, "Quantum switch for the quantum internet: Noiseless communications through noisy channels," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 3, pp. 575–588, Mar. 2020.

[599] Z. Li, K. Xue, J. Li, N. Yu, J. Liu, D. S. L. Wei, Q. Sun, and J. Lu, "Building a large-scale and wide-area quantum internet based on an OSI-alike model," *China Commun.*, vol. 18, no. 10, pp. 1–14, Oct. 2021.

[600] D. Chandra, A. S. Cacciapuoti, M. Caleffi, and L. Hanzo, "Direct quantum communications in the presence of realistic noisy entanglement," *IEEE Trans. Commun.*, Early Access, Oct. 2021, DOI: 10.1109/TCOMM.2021.3122786.

[601] H. Wang, Y. Zhao, Y. Li, X. Yu, J. Zhang, C. Liu, and Q. Shao, "A flexible key-updating method for software-defined optical networks secured by quantum key distribution," *Opt. Fiber Technol.*, vol. 45, pp. 195–200, Nov. 2018.

[602] X. Yu, X. Liu, Y. Liu, A. Nag, X. Zou, Y. Zhao, and J. Zhang,

"Multi-path-based quasi-real-time key provisioning in quantum-key-distribution enabled optical networks (QKD-ON)," *Opt. Express*, vol. 29, no. 14, pp. 21225–21239, July 2021.

[603] H. Wang, Y. Zhao, A. Nag, X. Yu, X. He, and J. Zhang, "End-to-end quantum key distribution (QKD) from metro to access networks," in *Proc. Int. Conf. Design of Reliable Communication Networks*, Milan, Itlay, Mar. 2020.

[604] X. Zhang, Z. Babar, P. Petropoulos, H. Haas, and L. Hanzo, "The evolution of optical OFDM," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 3, pp. 1430–1457, 3rd Quart., 2021.

[605] L. Hanzo, T. H. Liew, B. L. Yeap, R. Y. S. Tee, and S. X. Ng, *Turbo Coding, Turbo Equalisation and Space-Time Coding*. John Wiley & Sons Ltd, 2nd edition, 2011.

Yuan Cao received the B.Eng. degree in optoelectronic information engineering from the Nanjing University of Posts and Telecommunications, China, in 2016, and the Ph.D. degree in information and communication engineering from the Beijing University of Posts and Telecommunications, China, in 2021. From June 2018 to August 2018, he was an Academic Visitor with the KTH Royal Institute of Technology, Sweden. From June 2019 to August 2019, he was an Academic Visitor with the University of Southampton, U.K. He is currently a Lecturer with the Nanjing University of Posts and Telecommunications. His research interests include quantum communications, quantum key distribution networking, software defined networking, and optical network security.

Yongli Zhao [SM'15] received the Ph.D. degree from the Beijing University of Posts and Telecommunications in 2010. From January 2016 to January 2017, he was a Visiting Associate Professor with the University of California, Davis. He is currently a Professor with the Beijing University of Posts and Telecommunications. He has published more than 400 international journal and conference papers. His research interests include software defined optical networks, elastic optical networks, datacenter networking, machine learning in optical networks, optical network security, and quantum key distribution networking. He is a Fellow of the IET.

Qin Wang received the Ph.D. degree from the University of Science and Technology of China in 2006. From October 2006 to July 2012, she was a Post-Doctoral Researcher with the KTH Royal Institute of Technology, Technical University of Denmark, and University of Copenhagen. She is currently a Professor and the Deputy Dean of the School of Communication and Information Engineering, Nanjing University of Posts and Telecommunications. Her research interests include quantum cryptography and quantum optics.

Jie Zhang received the Ph.D. degree in electromagnetic field and microwave technology from the Beijing University of Posts and Telecommunications in 1998. He is currently a Professor and the Dean of the School of Electronic Engineering, Beijing University of Posts and Telecommunications. He has published more than 400 technical articles, authored eight books, and submitted 17 ITU-T recommendation contributions and six IETF drafts. His research interests include architecture, protocols, security, and standards for optical transport networks.

Soon Xin Ng (Michael) [S'99–M'03–SM'08] received the B.Eng. degree (First class) in electronic engineering and the Ph.D. degree in telecommunications from the University of Southampton, U.K., in 1999 and 2002, respectively. From 2003 to 2006, he was a postdoctoral research fellow working on collaborative European research projects. Since August 2006, he has been a member of academic staff in the School of Electronics and Computer Science, University of Southampton. He was the principal investigator of an EPSRC project on "Cooperative Classical and Quantum Communications Systems". He is currently a Professor of Next Generation Communications at the University of Southampton. His research interests include adaptive coded modulation, coded modulation, channel coding, space-time coding, joint source and channel coding, iterative detection, OFDM, MIMO, cooperative communications, distributed coding, quantum communications, quantum error correction codes, joint wireless-and-optical-fibre communications, game theory, artificial intelligence and machine learning. He has published over 260 papers and co-authored two John Wiley/IEEE Press books in this field.

He is a Senior Member of the IEEE, a Fellow of the Higher Education Academy in the UK, a Chartered Engineer and a Fellow of the IET. He acted as TPC/track/workshop chairs for various conferences. He serves as an editor of Quantum Engineering. He was a guest editor for the special issues in IEEE Journal on Selected Areas in Communications as well as editors in the IEEE Access and the KSII Transactions on Internet and Information Systems. He is one of the Founders and Officers of the IEEE Quantum Communications & Information Technology Emerging Technical Subcommittee (QCIT-ETC).

Lajos Hanzo (http://www-mobile.ecs.soton.ac.uk, https://en.wikipedia.org/wiki/Lajos_Hanzo) [FIEEE'04] received his Master degree and Doctorate in 1976 and 1983, respectively from the Technical University (TU) of Budapest. He was also awarded the Doctor of Sciences (DSc) degree by the University of Southampton (2004) and Honorary Doctorates by the TU of Budapest (2009) and by the University of Edinburgh (2015). He is a Foreign Member of the Hungarian Academy of Sciences and a former Editor-in-Chief of the IEEE Press. He has served several terms as Governor of both IEEE ComSoc and of VTS. He has published 2000+ contributions at IEEE Xplore, 19 Wiley-IEEE Press books and has helped the fast-track career of 123 PhD students. Over 40 of them are Professors at various stages of their careers in academia and many of them are leading scientists in the wireless industry. He is also a Fellow of the Royal Academy of Engineering (FREng), of the IET and of EURASIP. He is the recipient of the 2022 Eric Sumner Field Award.

Quantum Search Algorithms for Wireless Communications

Panagiotis Botsinis, *Member, IEEE*, Dimitrios Alanis, *Student Member, IEEE*, Zunaira Babar, Hung Viet Nguyen, *Member, IEEE*, Daryus Chandra, *Student Member, IEEE*, Soon Xin Ng, *Senior Member, IEEE*, and Lajos Hanzo, *Fellow, IEEE*

***Abstract*—Faster, ultra-reliable, low-power, and secure communications has always been high on the wireless evolutionary agenda. However, the appetite for faster, more reliable, greener, and more secure communications continues to grow. The state-of-the-art methods conceived for achieving the performance targets of the associated processes may be accompanied by an increase in computational complexity. Alternatively, a degraded performance may have to be accepted due to the lack of jointly optimized system components. In this survey we investigate the employment of quantum computing for solving problems in wireless communication systems. By exploiting the inherent parallelism of quantum computing, quantum algorithms may be invoked for approaching the optimal performance of classical wireless processes, despite their reduced number of cost-function evaluations. In this contribution we discuss the basics of quantum computing using linear algebra, before presenting the operation of the major quantum algorithms, which have been proposed in the literature for improving wireless communications systems. Furthermore, we investigate a number of optimization problems encountered both in the physical and network layer of wireless communications, while comparing their classical and quantum-assisted solutions. Finally, we state a number of open problems in wireless communications that may benefit from quantum computing.**

***Index Terms*—Algorithm design and analysis, channel estimation, localization, multiuser detection, non-orthogonal multiple access, optimization, precoding, quantum algorithms, quantum computing, routing, visible light communication, wireless communication.**

List of Abbreviations

ACO	Ant Colony Optimization
AoA	Angle of Arrival
BBHT	Boyer-Brassard-Høyer-Tapp
BER	Bit Error Rate
CDMA	Code Division Multiple Access
CF	Cost Function
CFE	Cost Function Evaluation
CIR	Channel Impulse Response
CoMP	Coordinated Multi-Point
DDCE	Decision-Directed Channel Estimation
DEA	Differential Evolution Algorithm
DH	Dürr-Høyer
DN	Destination Node
eMBB	enhanced Mobile BroadBand
EQPO	Evolutionary Quantum Pareto Optimization
FD-CHTF	Frequency Domain - CHannel Transfer Function
FFT	Fast Fourier Transform
GA	Genetic Algorithm
GNFS	General Number Field Sieve
HetNet	Heterogeneous Network
HHL	Harrow-Hassidim-Lloyd
IoT	Internet of Things
IQFT	Inverse Quantum Fourier Transform
LED	Light Emitting Diode
LLR	Log-Likelihood Ratio
LOS	Line Of Sight
LTE	Long-Term Evolution
MAP	Maximum *A posteriori* Probability
MBER	Minimum Bit Error Ratio
ML	Maximum Likelihood
MMSE	Minimum Mean Square Error
mMTC	massive Machine Type Communications
MODQO	Multi-Objective Decomposition Quantum Optimization
MPC	Multi-Path Component
MUD	Multi-User Detection
MUT	Multi-User Transmitter
NDQIO	Non-Dominated Quantum Iterative Optimization
NDQO	Non-Dominated Quantum Optmization
NOMA	Non-Orthogonal Multiple Access
NU	Network Utility
OFDMA	Orthogonal Frequency Division Multiple Access
OMA	Orthogonal Multiple Access
PDP	Power Delay Profile
PIC	Parallel Interference Cancellation
PLR	Packet Loss Ratio
PSO	Particle Swarm Optimization
QCA	Quantum Counting Algorithm
QGA	Quantum Genetic Algorithm

Manuscript received February 10, 2018; revised August 15, 2018 and October 10, 2018; accepted November 16, 2018. Date of publication November 20, 2018; date of current version May 31, 2019. This work was supported by the European Research Council under the Advanced Fellow Grant the Royal Society's Wolfson Research Merit Award and the Engineering and Physical Sciences Research Council under Grant EP/L018659/1. *(Corresponding author: Lajos Hanzo.)*

The authors are with the School of Electronics and Computer Science, University of Southampton, Southampton, SO17 1BJ, U.K. (e-mail: pb1y14@ecs.soton.ac.uk; da1d16@ecs.soton.ac.uk; zb2g10@ecs.soton.ac.uk; hvn08r@ecs.soton.ac.uk; dc2n14@ecs.soton.ac.uk; sxn@ecs.soton.ac.uk; lh@ecs.soton.ac.uk).

Digital Object Identifier 10.1109/COMST.2018.2882385

QHA	Quantum Heuristic Algorithm
QMA	Quantum Mean Algorithm
QoS	Quality of Service
QPEA	Quantum Phase Estimation Algorithm
QPSK	Quadrature Phase Shift Keying
QRWBS	Quantum Weighted Boosting Search
QSA	Quantum Search Algorithm
QSVM	Quantum Support Vector Machine
QWSA	Quantum Weighted Sum Algorithm
RN	Relay Node
RSSI	Received Signal Strength Indicator
RWBS	Repeated Weighted Boosting Search
SC-FDMA	Single-Carrier Frequency Division Multiple Access
SIC	Successive Interference Cancellation
SISO	Soft-Input Soft-Output
SN	Source Node
SNR	Signal to Noise Ratio
SVM	Support Vector Machine
TDMA	Time Division Multiple Access
TDoA	Time Difference of Arrival
ToA	Time of Arrival
TPC	Transmit Pre-Coding
URLLC	Ultra-Reliable Low-Latency Communications
UV	Utility Vector
UWB	Ultra WideBand
WSN	Wireless Sensor Network
ZF	Zero Forcing.

I. Introduction

THE NEXT generation of wireless communications promises Ultra-Reliable Low-Latency Communications (URLLC), massive Machine Type Communications (mMTC), as well as 100x increased throughput in enhanced Mobile BroadBand (eMBB) communications [1], [2]. The plethora of applications, involving the Internet of Things (IoT) and the vision of everything being connected everywhere and anytime has to be achieved [3], [4], while keeping the required resources as low as possible. For example, the transition from Orthogonal Multiple Access (OMA) to Non-Orthogonal Multiple Access (NOMA) [5] is expected to occur in the eMBB use case of 5G for increasing the system throughput. However, the complexity of the signal detection will also be increased, even if a sub-optimal detector based on for example Successive Interference Cancellation (SIC) is adopted [6]. At the same time, agile and accurate channel estimation will be required in URLLC [7], where the target end-to-end delay requirement, which includes both the transmission time as well as processing time, is on the order of a few OFDM symbols. In order to achieve this, a joint channel estimator and data detector may be employed for achieving an improved performance, albeit this tends to impose increased computational complexity. In a mobile mMTC network, the inherent problem of finding the optimal route amongst numerous nodes is again going to require intensive computations [8].

During the last few years the research community has turned its attention to quantum computing [1], [9]–[12] with the objective of amalgamating it with classical communications in order to attain certain performance targets, such as throughput, round trip delay and reliability targets at a low computational complexity. As we will discuss in more detail in this contribution, there are numerous optimization problems in wireless communications systems that may be solved at a reduced number of Cost Function Evaluations (CFEs) by employing quantum algorithms.

A. Why Quantum Computing?

The ever-reducing transistor size following Moore's law is approaching the point, where the so-called *quantum effects* [9] become prevalent in the transistors' operation [13]. This specific trend implies that quantum effects become unavoidable, hence rendering the research of quantum computation systems an urgent necessity. In fact, a quantum annealing chipset [14] is already commercially available from *D-Wave*[1] [15], [16]. Apart from the quantum annealing architecture, the so-called *gate-based architecture* [10], which relies on building computational blocks using quantum gates in a similar fashion to classical logic gates, is attracting increasing attention due to the recent advances in *quantum stabilizer codes* [17]–[22], which are capable of mitigating the *decoherence*[2] effects encountered by quantum circuits [9]. In terms of implementation, D-Wave's most recent model, namely *D-Wave 2000Q*,[3] has a total of 2000 qubits, while *IBM Q Experience*,[4] which relies on the gated-based architecture, has currently only 20 qubits in total. However, IBM has recently announced their plans[5] for delivering a 50 qubit gate-based quantum computer by 2020.

Once quantum computing becomes a commercial reality, it may be used in wireless communications systems in order to speed up specific processes due to its inherent parallelization capabilities. While a classical bit may adopt either the values 0 or 1, a quantum bit, or *qubit*, may have the values $|0\rangle$, $|1\rangle$, or any superposition of the two [9]–[11], where the notation $|\cdot\rangle$ is the ket representation [23] and it is the column vector of a quantum state. If two qubits are used, then the composite quantum state may have the values $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$ simultaneously. In general, by employing b bits in a classical register, one out of 2^b combinations is represented at any time. By contrast, in a quantum register associated with b qubits, the composite quantum state may be found in a superposition of all 2^b values *simultaneously*. Therefore, by applying a quantum operation to the quantum register would result in altering all 2^b values at the same time. This represents the parallel processing capability of quantum computing. Multiple quantum algorithms have been proposed [12], which are capable of outperforming their classical counterparts in the same categories of problems, by either requiring fewer computational steps, or by finding a better solution to the specific problem.

[1] https://www.dwavesys.com/d-wave-two-system

[2] As it will be explained in the following, decoherence may be considered as detrimental noise in quantum circuits.

[3] https://www.dwavesys.com/d-wave-two-system

[4] https://quantumexperience.ng.bluemix.net/qx/experience

[5] https://www-03.ibm.com/press/us/en/pressrelease/53374.wss

In this treatise, we will focus our attention on the employment of quantum algorithms in classical communication systems, which may be termed as *quantum-assisted communications* [1], [9]. More specifically, the employment of quantum algorithms may be capable of improving the already existing processes of classical communications, such as optimal multi-user detection, channel estimation, finding the optimal precoding matrix for the downlink of a multi-user system, or finding the optimal route in a classical wireless network. Quantum-assisted communications should be distinguished from *quantum-based communications* [1], [10], [11]. In the latter, quantum bits are transmitted and received over quantum channels. By contrast, quantum-assisted communications may be considered as a classical communication system like the mobile broadband in the Long-Term Evolution (LTE) standard, where hybrid classical and quantum processors are exchanging information at the Base Station (BS).

B. Motivation for This Contribution

There is a number of well-established surveys on quantum algorithms [24]–[27]. In [24], Williams detailed the operation of Grover's Quantum Search Algorithm (QSA) [28], [29] and discussed its applications as a "subroutine" in other quantum algorithms. Quantum walk-based search algorithms were the focus of [25], arguing that they may be used for solving search problems, such as finding out whether a list has unique entries, or determining if a group's elements are commutative with each other. In [26], efficient quantum algorithms substantially outperforming their classical counterparts were reviewed, with a focus on their employment in algebraic problems. In [27], Mosca reviewed a number of quantum algorithms, explaining their operation and their associated computational complexity. The website "Quantum Zoo" [30] has gathered a comprehensive list of quantum algorithms, briefly describing their operation.

Against this background, the main motivation of this paper is to make quantum computing and quantum algorithms accessible to communication engineers, by investigating their operation and employment in communication applications. We provide a list of optimization problems in the area of wireless communications that may be solved using a quantum computer. We review quantum algorithms that have already been used[6] for solving existing problems in classical wireless communication systems. Furthermore, we discuss both the "why" and the "how" of quantum computation. Quantum computing is still considered by the majority of communication engineers as a term closely intertwined with physics. Therefore, we assume that the reader has no background on quantum computing and we aim for ripping off this mysterious cloak from quantum computing by showing the quantum circuits employed in the quantum algorithms presented. In this study we have focused our attention on the associated algorithmic perspectives, with an emphasis on the potential performance gain as well as on the attainable complexity reduction. Indeed, we concur that also the other important practical requirements have to be taken into consideration, such as the scalability and timing requirements, the required hardware and the potential reuse of existing hardware blocks in a modem chip along with the integration between the classical and quantum parts of the solutions presented, which have not been considered in this paper.

The rest of the paper is structured as follows. In Section II we state the basic postulates of quantum mechanics and describe how quantum computing systems can be represented and simulated by classical computers. We continue by offering a brief historical perspective of quantum computing and review the operation of the most popular quantum algorithms. In Section III, we describe a number of optimization problems that appear in wireless communication systems, along with their associated classical, as well as quantum algorithms that may be employed for solving them. Finally, we state a number of open problems in Section IV and we conclude in Section V. The paper's structure is given in Fig. 1.

II. INTRODUCTION TO QUANTUM COMPUTING

A. Basics of Quantum Computing

1) The Qubit: The quantum state of a qubit may be represented using any chosen orthogonal basis. The most commonly used basis is the computational basis [9], which corresponds to the states $|0\rangle$ and $|1\rangle$. The quantum state $|q\rangle$ of a single-qubit system in the computational basis $\{|0\rangle, |1\rangle\}$ is [9]

$$|q\rangle = a|0\rangle + b|1\rangle, \tag{1}$$

where $a, b \in \mathbb{C}$ are the amplitudes of $|q\rangle$ on the computational basis and we have $|a|^2+|b|^2 = 1$. When $a = 0$, we have $b = 1$ and hence

$$|q\rangle = |1\rangle, \tag{2}$$

which corresponds to the classical bit value 1. Similarly, if $a = 1$, then $b = 0$ and

$$|q\rangle = |0\rangle, \tag{3}$$

which again is a classical bit value. However, if we choose $a = b = 1/\sqrt{2}$, then we have

$$|q\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle. \tag{4}$$

The quantum state in (4) seems to exhibit a symmetry with respect to the orthogonal states $|0\rangle$ and $|1\rangle$, not favoring one over the other. This state is widely used in most of the quantum algorithms that we will investigate.

2) Geometrical Representation: Assuming only real-valued amplitudes for a quantum state $a, b \in \mathbb{R}$, the resultant 2-D geometrical representation of a qubit's state is shown in Fig. 2, since its state may be written as in

$$|q\rangle = \cos(\theta)|0\rangle + \sin(\theta)|1\rangle. \tag{5}$$

In the general case, the amplitudes of the quantum states are complex-valued, therefore the state of a qubit is represented

[6] Since a universal quantum computer does not exist at the time of writing, the operation of the quantum algorithms has been demonstrated with simulations on classical super-computers. Please note that the practical creation of the discussed quantum algorithms is out of the scope of this paper. Here we assume that a universal quantum computer exists and that the discussed quantum algorithms are available.

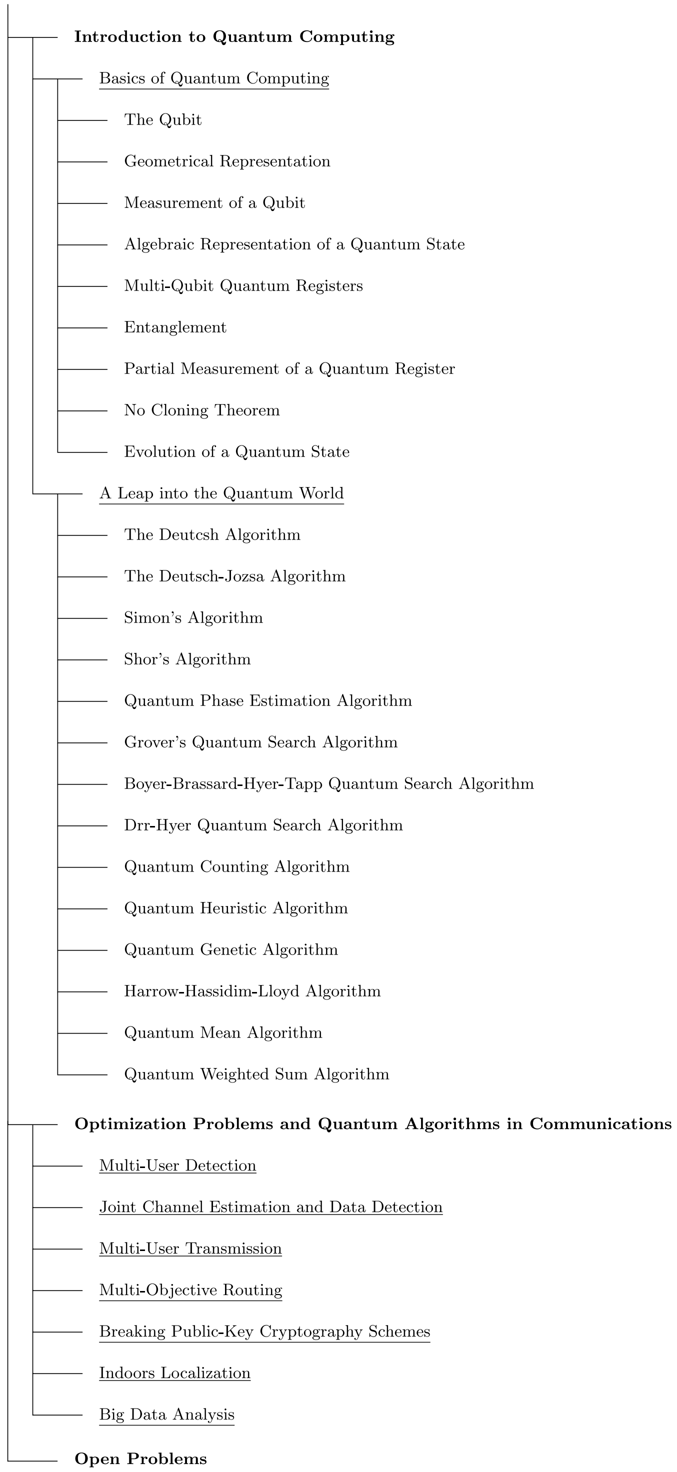

Introduction to Quantum Computing
Basics of Quantum Computing
The Qubit
Geometrical Representation
Measurement of a Qubit
Algebraic Representation of a Quantum State
Multi-Qubit Quantum Registers
Entanglement
Partial Measurement of a Quantum Register
No Cloning Theorem
Evolution of a Quantum State
A Leap into the Quantum World
The Deutcsh Algorithm
The Deutsch-Jozsa Algorithm
Simon's Algorithm
Shor's Algorithm
Quantum Phase Estimation Algorithm
Grover's Quantum Search Algorithm
Boyer-Brassard-Hyer-Tapp Quantum Search Algorithm
Drr-Hyer Quantum Search Algorithm
Quantum Counting Algorithm
Quantum Heuristic Algorithm
Quantum Genetic Algorithm
Harrow-Hassidim-Lloyd Algorithm
Quantum Mean Algorithm
Quantum Weighted Sum Algorithm
Optimization Problems and Quantum Algorithms in Communications
Multi-User Detection
Joint Channel Estimation and Data Detection
Multi-User Transmission
Multi-Objective Routing
Breaking Public-Key Cryptography Schemes
Indoors Localization
Big Data Analysis
Open Problems

Fig. 1. The structure of the paper.

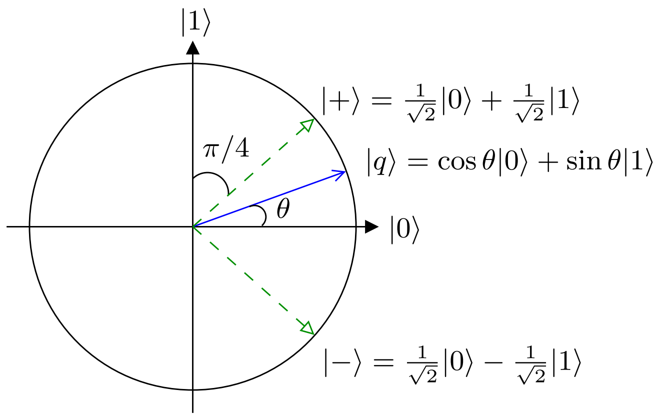

$|1\rangle$
$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$
$\pi/4$
$|q\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle$
θ
$|0\rangle$
$|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$

Fig. 2. The 2D representation of a qubit, when the amplitudes of its quantum states are real-valued.

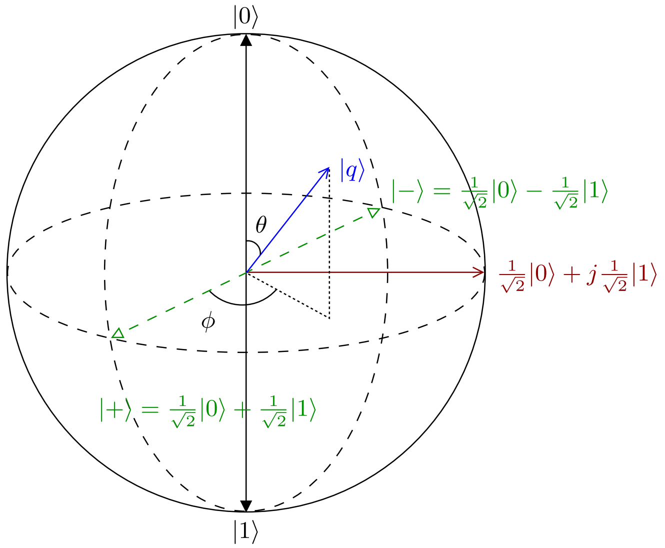

$|0\rangle$
$|q\rangle$
$|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$
θ
$\frac{1}{\sqrt{2}}|0\rangle + j\frac{1}{\sqrt{2}}|1\rangle$
ϕ
$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$
$|1\rangle$

Fig. 3. The generic 3D representation of a qubit using a Bloch sphere, when the amplitudes of its quantum states are complex-valued.

by the 3-D Bloch sphere [9]–[11] of Fig. 3, since a qubit's state may always be written as

$$|q\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle. \quad (6)$$

Many algorithms, such as Grover's QSA [28], the Boyer-Brassard-Høyer-Tapp (BBHT) QSA [31] and the Dürr-Høyer (DH) QSA [32] only consider real-valued amplitudes, therefore the 2-D representation is suitable for their analysis. However, other algorithms, like Shor's algorithm [33] and the quantum counting algorithm [34] exploit the complex-valued nature of the states' amplitudes and the Bloch sphere may be used for geometrically representing their quantum states.

3) Measurement of a Qubit: Before we continue with the investigation of the symmetrical state of (4), let us explicitly mention that even though a qubit may be in a superposition of two orthogonal states, if we desire to *observe,* or *measure* its value, we will only obtain one of the two orthogonal states. The measurement of a quantum state may be considered as a Quantum-to-Classical (Q/C) conversion, since it allows us to gain some insight on the quantum system.[7] The measurement of a qubit's state may also be done in a basis different from that which the qubit was prepared in. For now, let us use the computational basis also for measuring a quantum state.

[7] Please note that the amount of insight obtained by a measurement heavily depends on the context of the quantum algorithm or protocol which the measurement is a part of.

According to the Copenhagen interpretation [35], which is the most widely adopted interpretation of a measurement's operation, a quantum state does not have specific properties before it is measured. However, when it is observed, the probabilities of its superimposed states define not only the outcome of the measurement, but also the new quantum state of the system.

The amplitudes a and b of the quantum state $|q\rangle$ in (1) uniquely define the probabilities of obtaining $|0\rangle$ or $|1\rangle$, when we measure the qubit's state $|q\rangle$ on the orthogonal basis $\{|0\rangle, |1\rangle\}$. More specifically, there is a $|a|^2$ probability that we will obtain the quantum state $|0\rangle$ and a $|b|^2$ probability that $|1\rangle$ will be observed. This is also the reason why $|a|^2 + |b|^2 = 1$ is always true. For example, in (2) and (3), since the system's state is already equal to one of the two states of the computational basis, which was used for the measurement, we would always observe $|1\rangle$ and $|0\rangle$, respectively. However, when we measure the quantum state of (4), there is a $|a|^2 = 1/2 = 50\%$ probability of obtaining the quantum state $|0\rangle$ and $|b|^2 = 1/2 = 50\%$ probability of obtaining the quantum state $|1\rangle$. Since the probability of observing either of the two states is the same, the quantum system of (4) is said to be in an *equiprobable superposition* of states, always with respect to the computational orthogonal basis.

After the measurement, the quantum state *collapses* to the observed quantum state. For example, let us assume that the output of the quantum state's measurement in (4) was $|1\rangle$. As mentioned before, this event had a 50% probability of occurrence. Given that it has happened however, the system's quantum state from that point onwards *becomes identical to the observed quantum state*, hence we have $|q'\rangle = |1\rangle$.

This feature is termed as *wave function collapse* in quantum mechanics and it is irreversible. In other words, we are not able to reconstruct the system's quantum state to that before the measurement, unless we have knowledge about the pre-measurement amplitudes a and b of (1).

4) Algebraic Representation of a Quantum State: A quantum state $|q\rangle$ may be fully described by its state vector [9]. The size of the state vector $|q\rangle$ is equal to the number of orthogonal states that the quantum state could be superimposed in. The values of the state vector $|q\rangle$ are the amplitudes of each orthogonal state. For example, when a qubit is in the state $|q\rangle = a|0\rangle + b|1\rangle$ as in (1), the 2-element state vector is

$$|q\rangle = \begin{bmatrix} a \\ b \end{bmatrix} = a|0\rangle + b|1\rangle, \tag{7}$$

implying that the first element corresponds to the amplitude of the state $|0\rangle$, while the second element to the amplitude of the state $|1\rangle$. As another example, the state vector of the equiprobable quantum state of (4) is

$$|q\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} = \frac{1}{\sqrt{2}} \cdot \begin{bmatrix} 1 \\ 1 \end{bmatrix}. \tag{8}$$

As expected, when more qubits are used, the system's state vector has more elements in order to accommodate the amplitudes of all legitimate state combinations.

5) Multi-Qubit Quantum Registers: In a two-qubit register, there are four legitimate states that the composite quantum system can be superimposed in. If the first qubit of the register is in the state $|q_1\rangle = a|0\rangle + b|1\rangle$ and the second qubit is in the state $|q_2\rangle = c|0\rangle + d|1\rangle$, the state of the system is

$$\begin{aligned} |q\rangle &= |q_1\rangle \otimes |q_2\rangle = |q_1 q_2\rangle & (9)\\ &= (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle) & (10)\\ &= a \cdot c|00\rangle + a \cdot d|01\rangle + b \cdot c|10\rangle + b \cdot d|11\rangle & (11)\\ &= \begin{bmatrix} a \cdot c \\ a \cdot d \\ b \cdot c \\ b \cdot d \end{bmatrix}, & (12) \end{aligned}$$

where $\otimes$ is the tensor product operator and the system's state vector includes the amplitudes of the four quantum states $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$.

In general, in an n-qubit register, the state vector will have 2^n entries, each corresponding to the amplitude of the respective orthogonal state. Now let us consider a 2-qubit register with the following quantum state

$$|q\rangle = \frac{\sqrt{3}}{2}|00\rangle + \frac{1}{2}|10\rangle = \begin{bmatrix} \frac{\sqrt{3}}{2} \\ 0 \\ \frac{1}{2} \\ 0 \end{bmatrix}. \tag{13}$$

After a potential measurement of that quantum register, there is a $(\sqrt{3}/2)^2 = 0.75$ probability of observing the state $|00\rangle$ and $(1/2)^2 = 0.25$ probability of obtaining the state $|10\rangle$. It is impossible to observe the states $|01\rangle$ or $|11\rangle$. We may also observe that it is possible to rewrite its state as

$$|q\rangle = \left(\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle\right) \otimes |0\rangle = \begin{bmatrix} \frac{\sqrt{3}}{2} \\ \frac{1}{2} \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |q_1\rangle|q_2\rangle. \tag{14}$$

This means that the first qubit is in a superposition (not equiprobable) of its two possible states, while the second qubit is at the state $|q_2\rangle = |0\rangle$. Since the state of the quantum register may be written as a tensor product of the quantum states of the individual qubits, the two qubits $|q_1\rangle$ and $|q_2\rangle$ are *independent* of each other.

6) Entanglement: When the quantum states of two or more qubits may not be represented separately and independently of each other, the qubits are *entangled* with each other. For example, let us consider the state

$$|q\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{bmatrix}. \tag{15}$$

This 2-qubit register is in an equiprobable superposition of the states $|00\rangle$ and $|01\rangle$. It is impossible to describe the states of the two qubits individually as in (14).[8] Therefore, the two qubits of the quantum register in (15) are entangled. Actually, the quantum state in (15) is one of the four *Bell states* [36], [37],

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle \tag{16}$$

[8] Try it, following the same methodology as in (13) and (14)!

$$\frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle \tag{17}$$

$$\frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle \tag{18}$$

$$\frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle, \tag{19}$$

which are widely used, since they are the only four quantum states of a two-qubit register that provide an equiprobable entanglement between two qubits.

7) Partial Measurement of a Quantum Register: In a multi-qubit quantum register, it is possible to only observe a subset of the qubits it consists of. Therefore, when we measure one of the qubits, its quantum state collapses to the observed state, while the quantum state of the rest of the *independent* qubits remains unaltered. However, this is not the case for the rest of the *entangled* qubits, whose state will also be affected by the observation of an entangled qubit.

As an example, let us try to only observe the second qubit of the quantum register in (14). The second qubit has an 100% probability of yielding the observation $|0\rangle$, therefore this is the state we will obtain. At the same time, the state of the first qubit $|q_1\rangle = \sqrt{3}/2|0\rangle + 1/2|1\rangle$ will remain unaltered, because it is in a superposition of its own, independent states.

Let us now try to measure the second qubit of the entangled 2-qubit register of (15). There is a $(1/\sqrt{2})^2 = 0.5 = 50\%$ chance of observing either the state $|0\rangle$ or the state $|1\rangle$. Let us assume that we observed the state $|0\rangle$. Therefore, the quantum state of the second qubit collapses to $|0\rangle$. Based on (15), we should notice that the state of the first qubit also collapses to $|0\rangle$ instantaneously, upon obtaining the measurement output of the second qubit. This happened because the whole quantum register could either be observed in the state $|00\rangle$, or in the state $|11\rangle$. Since we observed the second qubit in the state $|0\rangle$, the first qubit can only be in the state $|0\rangle$ from this point onwards.

Entanglement enables a plethora of applications, since it allows instantaneous information exchange between qubits. As it will be discussed in the following, the quantum algorithms appropriately manipulate the available qubits in order to finally measure a quantum state, which has a desirable property.

8) No Cloning Theorem: The irreversible nature of a quantum measurement is exploited in quantum cryptography [38]–[40], a field which also exploits the no cloning theorem [41]. According to the no cloning theorem, it is impossible to copy the unknown quantum state of a qubit into the quantum state of another qubit, while keeping their states independent of each other at the same time. In other words, it is impossible to make independent copies of qubits, without entangling them with each other in the process.

The rules of entanglement, the no cloning theorem and the irreversible nature of measurements allow quantum-based communications to be very promising for sharing private keys between two parties. By exploiting these features in the available QKD protocols, such as the Bennett-Brassard-1984 (BB84) protocol [42], one or both parties become capable of detecting whether an eavesdropper tempered with their communications or not, due to the imperfections that the eavesdropper would have imposed on the measured and retransmitted states, since the eavesdropper would have been unable to simply copy and forward the intercepted qubits. If the two parties determine that an eavesdropper was present during the transmission of the qubits, the whole process is aborted and restarted.

9) Evolution of a Quantum State: The state of a quantum register may be changed by applying *unitary operators or gates* to its qubits [9]. Let us first investigate a single-qubit system. One of the most widely used single-qubit unitary operators is the *Hadamard operator H*, which creates equiprobable superpositions of the two states, given that the initial state was either $|0\rangle$ or $|1\rangle$, as encapsulated in

$$H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle = |+\rangle \tag{20}$$

$$H|1\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle = |-\rangle. \tag{21}$$

The states $|+\rangle$ and $|-\rangle$ form the orthogonal Hadamard basis, as depicted in Fig. 2. The matrix representation of the single-qubit Hadamard operator is

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \tag{22}$$

while that of the two-qubit Hadamard operator is

$$H^{\otimes 2} = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}. \tag{23}$$

An *n*-qubit Hadamard gate has to be employed for creating an equiprobable superposition of all legitimate states at the beginning of most quantum algorithms, which is achieved by applying it to an *n*-qubit quantum register in the all-zero state $|0\rangle^{\otimes n}$. The circuit representation of the Hadamard gate is shown in Fig. 4.

The parallel evolution of the state of a quantum register that consists of multiple qubits is termed as *quantum parallelism.* Quantum parallelism is one of the pivotal features of quantum computing, which is exploited in order to create quantum algorithms that solve problems by requiring for example fewer CF evaluations than their classical counterparts.

Another popular set of single-qubit quantum gates is represented by the Pauli gates [9]–[11]

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \; Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \; Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}. \tag{24}$$

Explicitly, the *X* operator is the *NOT* gate, also known from classical logic circuits, since it swaps the amplitudes of the quantum states of a qubit as in

$$X(a|0\rangle + b|1\rangle) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} b \\ a \end{bmatrix} = b|0\rangle + a|1\rangle.$$

The *Z* operator is the gate imposing a *phase shift* by π radians, since it flips the sign of the amplitude of just the state $|1\rangle$, as described in

$$Z(a|0\rangle + b|1\rangle) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \cdot \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} a \\ -b \end{bmatrix} = a|0\rangle - b|1\rangle.$$

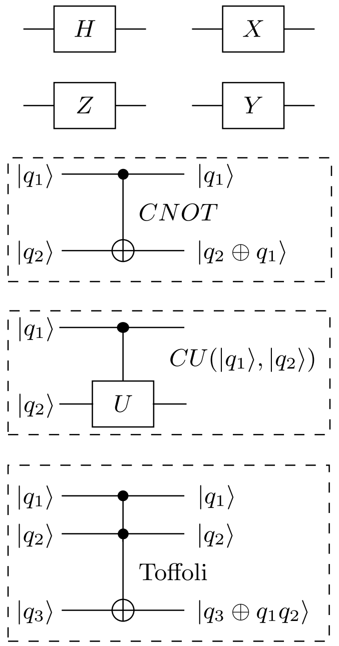


Fig. 4. The circuit representation of the Hadamard gate *H*, of the three Pauli gates *X*, *Z* and *Y*, as well as of the Controlled-NOT operation, of the general Controlled-U gate and of the Toffoli gate.

The Y operator may be considered as a combination of the X and Z gates, since it results in

$$\begin{aligned} Y(a|0\rangle + b|1\rangle) &= \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \cdot \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} -ib \\ ia \end{bmatrix} \\ &= i(-b|0\rangle + a|1\rangle). \end{aligned}$$

The circuit representation of the Pauli gates is also depicted in Fig. 4.

Other popular gates require the use of *control qubits*. For example, the Controlled-NOT (*CNOT*) gate applies the *NOT* operation to the qubit $|q_2\rangle$, only when the qubit $|q_1\rangle$ is in the state $|1\rangle$, as described by

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \tag{25}$$

For example, if the first (control) qubit was in the state $|q_1\rangle = a|0\rangle + b|1\rangle$ and the second (target) qubit was in the state $|q_2\rangle = c|0\rangle + d|1\rangle$, the *CNOT* gate would result into

$$\begin{aligned} CNOT(|q_1\rangle|q_2\rangle) &= a \cdot c|00\rangle + a \cdot d|01\rangle + b \cdot d|10\rangle \\ &\quad + b \cdot c|11\rangle \\ &= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} a \cdot c \\ a \cdot d \\ b \cdot c \\ b \cdot d \end{bmatrix} \\ &= \begin{bmatrix} a \cdot c \\ a \cdot d \\ b \cdot d \\ b \cdot c \end{bmatrix} = a \cdot c|00\rangle + a \cdot d|01\rangle \\ &\quad + b \cdot d|10\rangle + b \cdot c|11\rangle. \end{aligned}$$

TABLE I
OPERATION OF A *CU* GATE

Before: $\|q_1\rangle\|q_2\rangle$	After: $CU\|q_1\rangle\|q_2\rangle$
$\|0\rangle\|0\rangle$	$\|0\rangle\|0\rangle$
$\|0\rangle\|1\rangle$	$\|0\rangle\|1\rangle$
$\|1\rangle\|0\rangle$	$\|1\rangle U\|0\rangle$
$\|1\rangle\|1\rangle$	$\|1\rangle U\|1\rangle$

We may observe that the amplitudes of the quantum states where the first qubit is equal to $|1\rangle$ have been swapped. In general, the *Controlled-U* gate applies a general quantum gate U to a target qubit only when the control qubit is equal to $|1\rangle$, as described by

$$CU = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{11} & u_{12} \\ 0 & 0 & u_{21} & u_{22} \end{bmatrix}, \tag{26}$$

where the aforementioned general single-qubit unitary operator U is

$$U = \begin{bmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{bmatrix}. \tag{27}$$

When the control qubits is equal to $|0\rangle$, the identity gate is applied to the target qubit, as stated in (26). Table I states the operation that the *CU* gate would carry out based on the four possible quantum states of two qubits, where the first one is the control qubit and the second one is the target qubit.

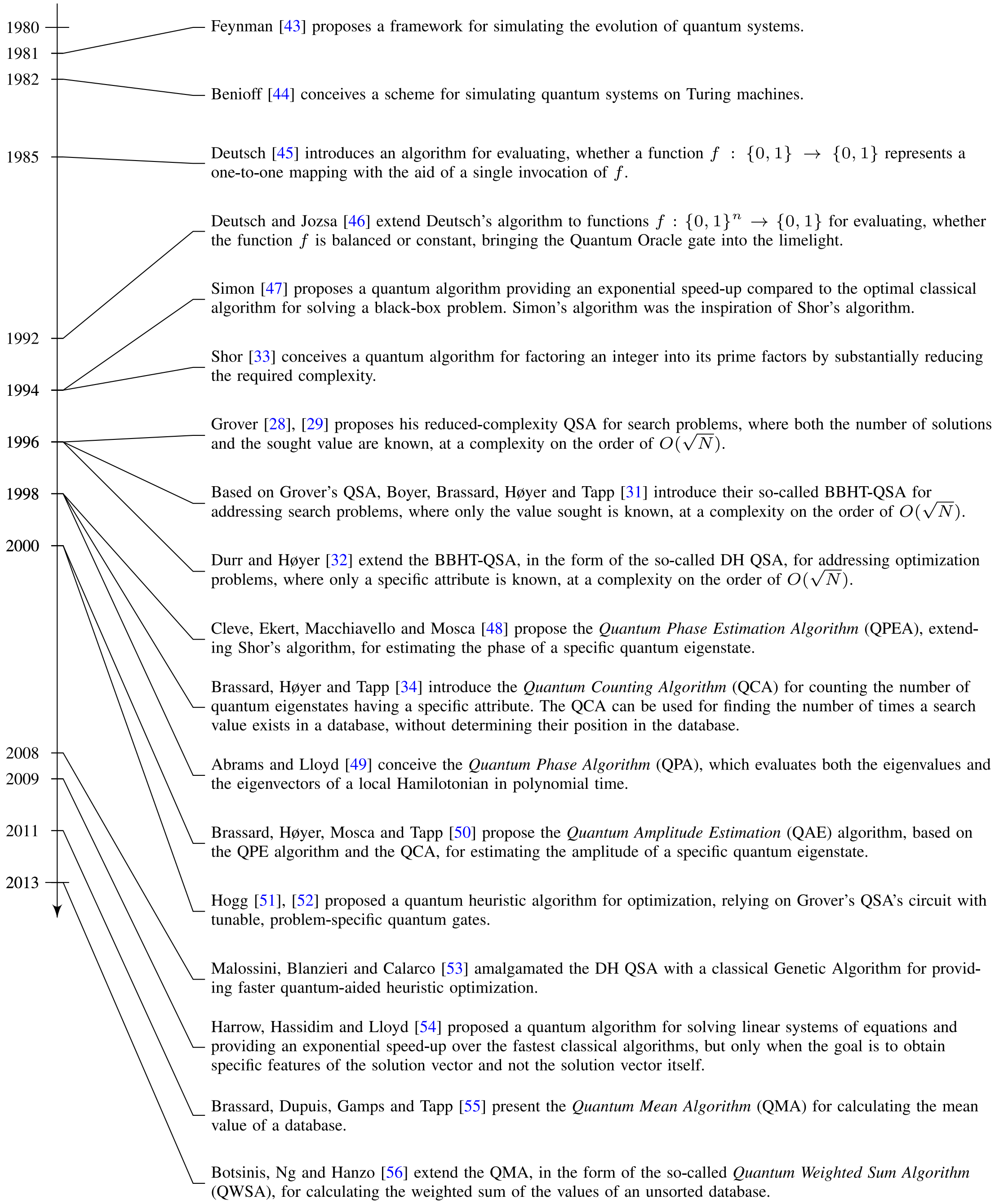
Finally, the Toffoli gate accepts two control qubits and flips the state of the target qubit, if and only if both control qubits are in the state $|1\rangle$. The matrix representation of the Toffoli gate is [9]:

$$CCNOT = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}. \tag{28}$$

The circuit representation of the controlled gates is also depicted in Fig. 4. Table II portrays both the initial and resultant states of a three-qubit register, when the Toffoli gate is applied to it, where the first two qubits are the control qubits and the last one is the target qubit.

B. A Leap Into the Quantum World

Research on quantum mechanics was initiated by Planck, Bohr, Heisenberg, Einstein and Schrödinger in 1923. Even though arguments and conflicts arose regarding whether the theory of quantum mechanics encapsulates a complete description of Nature, it is currently considered as the most suitable interpretation of both the microscopic and the macroscopic worlds.



Feynman [43] proposes a framework for simulating the evolution of quantum systems.

Benioff [44] conceives a scheme for simulating quantum systems on Turing machines.

Deutsch [45] introduces an algorithm for evaluating, whether a function $f : \{0, 1\} \rightarrow \{0, 1\}$ represents a one-to-one mapping with the aid of a single invocation of f.

Deutsch and Jozsa [46] extend Deutsch's algorithm to functions $f : \{0, 1\}^n \rightarrow \{0, 1\}$ for evaluating, whether the function f is balanced or constant, bringing the Quantum Oracle gate into the limelight.

Simon [47] proposes a quantum algorithm providing an exponential speed-up compared to the optimal classical algorithm for solving a black-box problem. Simon's algorithm was the inspiration of Shor's algorithm.

Shor [33] conceives a quantum algorithm for factoring an integer into its prime factors by substantially reducing the required complexity.

Grover [28], [29] proposes his reduced-complexity QSA for search problems, where both the number of solutions and the sought value are known, at a complexity on the order of $O(\sqrt{N})$.

Based on Grover's QSA, Boyer, Brassard, Høyer and Tapp [31] introduce their so-called BBHT-QSA for addressing search problems, where only the value sought is known, at a complexity on the order of $O(\sqrt{N})$.

Durr and Høyer [32] extend the BBHT-QSA, in the form of the so-called DH QSA, for addressing optimization problems, where only a specific attribute is known, at a complexity on the order of $O(\sqrt{N})$.

Cleve, Ekert, Macchiavello and Mosca [48] propose the *Quantum Phase Estimation Algorithm* (QPEA), extending Shor's algorithm, for estimating the phase of a specific quantum eigenstate.

Brassard, Høyer and Tapp [34] introduce the *Quantum Counting Algorithm* (QCA) for counting the number of quantum eigenstates having a specific attribute. The QCA can be used for finding the number of times a search value exists in a database, without determining their position in the database.

Abrams and Lloyd [49] conceive the *Quantum Phase Algorithm* (QPA), which evaluates both the eigenvalues and the eigenvectors of a local Hamilotonian in polynomial time.

Brassard, Høyer, Mosca and Tapp [50] propose the *Quantum Amplitude Estimation* (QAE) algorithm, based on the QPE algorithm and the QCA, for estimating the amplitude of a specific quantum eigenstate.

Hogg [51], [52] proposed a quantum heuristic algorithm for optimization, relying on Grover's QSA's circuit with tunable, problem-specific quantum gates.

Malossini, Blanzieri and Calarco [53] amalgamated the DH QSA with a classical Genetic Algorithm for providing faster quantum-aided heuristic optimization.

Harrow, Hassidim and Lloyd [54] proposed a quantum algorithm for solving linear systems of equations and providing an exponential speed-up over the fastest classical algorithms, but only when the goal is to obtain specific features of the solution vector and not the solution vector itself.

Brassard, Dupuis, Gamps and Tapp [55] present the *Quantum Mean Algorithm* (QMA) for calculating the mean value of a database.

Botsinis, Ng and Hanzo [56] extend the QMA, in the form of the so-called *Quantum Weighted Sum Algorithm* (QWSA), for calculating the weighted sum of the values of an unsorted database.

Fig. 5. Timeline of quantum computing milestones.

The inspiration of quantum computation was provided by Feynman [43], who proposed in 1981 a novel framework for conveying information by the spin of an electron and for simulating the evolution of the quantum states. In the following year, Benioff [44] proposed a technique of simulating quantum systems on Turing machines. Based on these contributions, further quantum algorithms were inspired. In the following sections we describe the general problems and the high-level operation of the major quantum algorithms, before delving into their applicability in wireless communications. A short description of the major quantum algorithms is provided in Fig. 5.

1) The Deutsch Algorithm: A few years later, the benefits of quantum parallelism were exploited by Deutsch [45], who conceived an algorithm, which now has the fond connotation of *Deutsch algorithm*. Let us first define the black box problem that we can solve using Deutsch's algorithm. Generally, a black box problem involves a function *f*, whose operation is unknown. We have to determine the features of the function by only evaluating it with the aid of different input arguments and then observing its corresponding outputs. Here, we have to determine whether the binary function $f : \{0, 1\} \rightarrow \{0, 1\}$ does or does not have a one-to-one mapping. When the function f has a one-to-one mapping we would expect

TABLE II
Operation of a Toffoli Gate

Before: $\vert q_1\rangle\vert q_2\rangle\vert q_3\rangle$	After: $CCNOT\vert q_1\rangle\vert q_2\rangle\vert q_3\rangle$
$\vert 0\rangle\vert 0\rangle\vert 0\rangle$	$\vert 0\rangle\vert 0\rangle\vert 0\rangle$
$\vert 0\rangle\vert 0\rangle\vert 1\rangle$	$\vert 0\rangle\vert 0\rangle\vert 1\rangle$
$\vert 0\rangle\vert 1\rangle\vert 0\rangle$	$\vert 0\rangle\vert 1\rangle\vert 0\rangle$
$\vert 0\rangle\vert 1\rangle\vert 1\rangle$	$\vert 0\rangle\vert 1\rangle\vert 1\rangle$
$\vert 1\rangle\vert 0\rangle\vert 0\rangle$	$\vert 1\rangle\vert 0\rangle\vert 0\rangle$
$\vert 1\rangle\vert 0\rangle\vert 1\rangle$	$\vert 1\rangle\vert 0\rangle\vert 1\rangle$
$\vert 1\rangle\vert 1\rangle\vert 0\rangle$	$\vert 1\rangle\vert 1\rangle\vert 1\rangle$
$\vert 1\rangle\vert 1\rangle\vert 1\rangle$	$\vert 1\rangle\vert 1\rangle\vert 0\rangle$

$f(0) \oplus f(1) = 1$, otherwise it would be $f(0) \oplus f(1) = 0$, since that would mean $f(0) = f(1)$, where $\oplus$ is the modulo-2 addition. In classical computing, a single evaluation for each of the legitimate inputs would be required, bringing the total number of function evaluations to two. Deutsch algorithm [45] succeeds in determining whether the function f has a one-to-one mapping by only using a single function evaluation.

2) The Deutsch-Jozsa Algorithm: An extension of this algorithm, namely the *Deutsch-Jozsa algorithm* [46], was conceived for determining whether a function $f : \{0,1\}^n \rightarrow \{0,1\}$ is balanced or constant.[9] Let us consider the problem in a real scenario, where the two parties Alice and Bob communicate with each other. Alice sends an n-bit number to Bob, who uses it as the input argument of his function f. Bob then transmits back the output bit. Alice has to determine whether the function that Bob used was balanced or constant. In classical computing, the best-case scenario would only be achieved if the function was balanced, Alice transmitted two different numbers and these two numbers happened to yield the two different outputs. The worst-case scenario is always encountered, when the function is constant, since Alice has to transmit $(2^{n-1} + 1)$ different input arguments (one more than half the set of inputs), before she realizes that the function Bob is using is constant. By using the Deutsch-Jozsa algorithm, Alice is able to determine whether the function f used by Bob is balanced or constant, with just a single transmission of n qubits in an equiprobable superposition of all possible inputs. Bob uses an extra auxiliary qubit, Hadamard gates and a quantum gate U_f that performs the same operation as f, but accepts qubits as its inputs. Finally, Bob measures the quantum state of the n qubits at the output of his quantum circuit. If the observed state is the all-zero state $|0\rangle^{\otimes n}$, the function f is constant, otherwise it is balanced.

The Deutsch-Jozsa algorithm solves the generalized black-box problem of the previous section. Indeed, if the function f allows only 0 or 1 as its legitimate inputs, determining whether the function has a one-to-one mapping, or if it is balanced answers exactly the same question. The algorithm was later improved by Cleve *et al.* [48] for achieving a 100% probability of success.

The Deutsch-Jozsa algorithm laid the foundations for the development of the so-called *Quantum Oracle* gates [9], which are quantum circuits implementing a generic function $f : \{0,1\}^N \rightarrow \{0,1\}^M$ and they are capable of calculating all the pairs of possible inputs-outputs of f using a single call of f by exploiting quantum parallelism.

3) Simon's Algorithm: In 1994, Simon managed to solve a black-box problem by using on the order of $O(n)$ queries addressed to the black box, while the optimal classical algorithm has to use $\Omega(2^{n/2})$ queries for the same task [47]. The black box U_f implements a function $f : \{0,1\}^n \rightarrow \{0,1\}^n$ and has the property that $f(x) = f(y)$ if and only if $x = y$ or if $x \oplus y = s$, for some unknown $s \in \{0,1\}^n$, where $x, y \in \{0,1\}^n$. Simon's algorithm succeeds in finding the value s that satisfies the function's above-mentioned property.

4) Shor's Algorithm: In 1994, Shor proposed a quantum algorithm [33], [57] for efficiently solving the problem of factoring a given integer N. The best classical algorithm is the General Number Field Sieve (GNFS) [58]. Shor's algorithm requires an exponentially lower complexity than the GNFS, which is achieved by combining classical and quantum processing. It first reduces the factoring problem to the so-called order-finding problem addressed below using a classical algorithm. Initially, it randomly picks a number $a<N$. Let us assume that the greatest common divisor between a and N is equal to 1.[10] Then a quantum circuit is employed for finding the period r of the function[12]

$$f(x) = a^x \bmod N. \tag{29}$$

If the estimated period r is even and $a^{r/2} = -1 \bmod N$ is false, then $gcd(a^{r/2} + 1, N)$ and $gcd(a^{r/2} - 1, N)$ are two non-trivial factors of N and the algorithm ends.

The order-finding quantum algorithm initially creates an equiprobable superposition of $C = 2^c$ states, using an appropriate number of c qubits,[13] as shown in Fig. 6. It then employs *controlled-*U_f operators,[14] where each of the c qubits controls the operation of a quantum gate that performs the function $f(x)$ of (29) on $n = \log_2 N$ auxiliary qubits. All n auxiliary qubits should initially be in the quantum state $|1\rangle^{\otimes n}$. This part is the bottleneck of Shor's algorithm, since it requires the operation of multiple controlled-U_f gates and $n = \log_2 N$ auxilliary qubits. Therefore, when N is high, more gates are required for a single U_f operation. At the same time, when C is high, the estimation of the period will be more accurate, but

[9] A function f is constant if it yields the same value at its output regardless of the input argument. On the other hand, a function f is balanced, if it yields one value (e.g., 0) for half the input arguments and another value (e.g., 1) for the other half of the input arguments.

[10] If the greatest common divisor between a and N was not equal to 1, then a would be a non-trivial factor[11] of N and the algorithm ends, since N can be factored in a and N/a. Then we have the problem of factoring i and N/a, if they are not prime numbers, and so on.

[12] The period of a function $f(x)$ is the smallest positive integer r so that $f(x+r) = f(x)$ for all values of x.

[13] Any number of qubits c that results in $C = 2^c$ states such that $N^2 \leq C < 2N^2$ would suffice.

[14] Please note that a controlled-U_f gate performs the U_f gate to the input target qubits only if the control qubits are in the state $|1\rangle$. When the control qubits are in the state $|0\rangle$, the identity operator is applied instead.

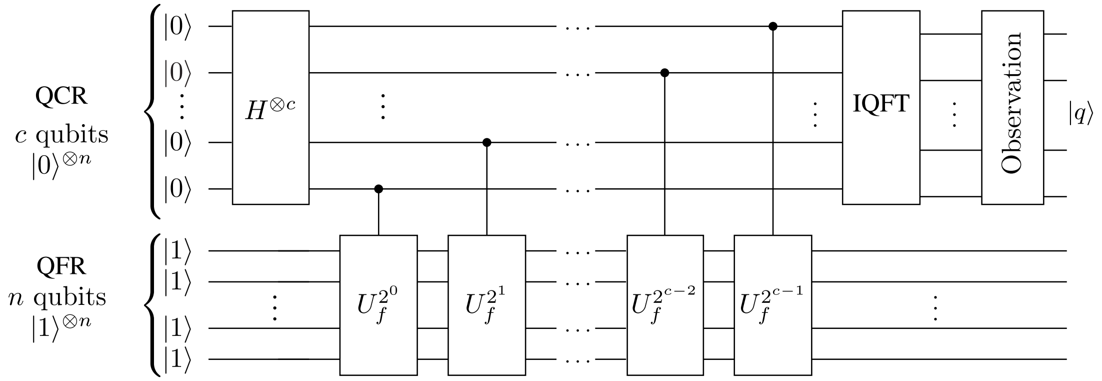


Fig. 6. The quantum circuit employed in Shor's algorithm for finding the period of the function in (29) [33].

more controlled-U_f operations are required, hence increasing the complexity.

After the operation of the controlled-U_f gates in Fig. 6, the c qubits pass through an Inverse Quantum Fourier Transform (IQFT) [10], [59] operator. The IQFT has the same effect as a classical IDFT, where the amplitude of each of the superimposed states is equally spread over the amplitudes of the resultant superimposed state. At the output of the IQFT, if we measure the resultant state of the c-qubit register, we will obtain a value $|q\rangle$, which may then be classically processed to approximate the period r. As mentioned earlier, after finding the period i, classical processing is employed for the rest of Shor's algorithm.

5) Quantum Phase Estimation Algorithm: A few years after Shor's algorithm was introduced, the order-finding quantum algorithm of Fig. 6 used in Shor's algorithm was found in [48] to be just a specific application of a general quantum circuit and algorithm, which is termed as the Quantum Phase Estimation Algorithm (QPEA). The QPEA follows exactly the same procedure as the period-finding quantum algorithm of Section II-B4. More specifically, given a unitary operator U that operates on n qubits and an eigenvector $|\phi\rangle$, such that

$$U|\phi\rangle = 2^{i\pi\theta}|\phi\rangle, \tag{30}$$

the QPEA estimates the period θ, which means that it can find the eigenvalue of a unitary operator. The quantum circuit of the QPEA is given in Fig. 7. The upper c qubits are termed as the *control register*, while the bottom n qubits represent the *function register*.

The QPEA is used as a building block for multiple quantum algorithms. As an example, let us now revisit Shor's algorithm, for the sake of relating it to the operation of the QPEA. In Shor's algorithm, the factoring problem was reduced to finding the period r of the function $f(x)$ of (29). In order to solve this problem, we have $U = f(x)$ and $\theta = r$ in (30). Comparing the quantum circuits of Fig. 6 and Fig. 7, we may observe that in the former, the n qubits of the function register are initialized to the all-one state $|1\rangle^{\otimes n}$, because it is one of the eignevectors of $f(x)$ of (29). Essentially, since we force a controlled function CU to operate on its eigenvectors, instead of altering the quantum states of the function register, we manage to rotate the states of the c-qubit control register. By applying the QFT to that control register, we are able to estimate the phase, eigenvalue, or period of the unitary transform U, upon its measurement.

6) Grover's Quantum Search Algorithm: In 1996, Grover [28], [29] proposed a *Quantum Search Algorithm* (QSA), which solves a search problem. Specifically, the search problem seeks to find a desired value δ in a database of N entries. We aim to find which of the N entries is equal to δ, i.e., we are interested in finding the position of δ in the database. If the database is sorted from lowest to highest values, the classical iterative halving-based search algorithm [60] is indeed optimal. On the other hand, if the database is unsorted, the optimal classical algorithm relies on a full search of the database. The average complexity of the full search would be on the order of $O(N)$ database queries. The worst case scenario occurs when the desired value is found at the entry that is checked last.

By contrast, Grover's QSA succeeds in finding the desired entry with 100% probability of success after querying the database on the order of $O(\sqrt{N})$ times [28]. This provides a quadratic reduction in complexity over the classical full search. Grover's QSA has been shown to be optimal by Zalka [61]. However, Grover's QSA requires some additional knowledge about the database. More explicitly, Grover's QSA employs the Grover operator $\mathcal{G}$ depicted in Fig. 8 L_{opt} number of consecutive times. Apart from knowing N and (obviously) the desired value δ, additionally Grover's QSA requires the knowledge of how many times the entry δ appears in the database, which is termed as the *number of solutions S*. For example, when we have $\delta = 2$ and $N = 16$, if $S = 3$ entries out of $N = 16$ are equal to $\delta = 2$, a different number of iterations L_{opt} is used in Grover's QSA, compared to the scenario, where only $S = 1$ out of $N = 16$ entries is equal to $\delta = 2$. However, in both examples the same procedure is followed at each iteration. Using fewer or more Grover iterations than L_{opt} may reduce the success probability, which might even approach 0%. Grover's QSA relies on the generic *amplitude amplification* process of Brassard *et al.* [50]. Explicitly, the optimal number of Grover operator applications is $L_{opt} = \lfloor 0.25\pi\sqrt{N/S} \rfloor$.

In Fig. 8, the $n = \log_2 N$ qubits in the register $|x\rangle_1$ are initialized to an equiprobable superposition of N states, each corresponding to the index of an entry in the database. The unitary operator O is termed as the *Oracle*, which marks the indices of the specific entries in the database that are equal

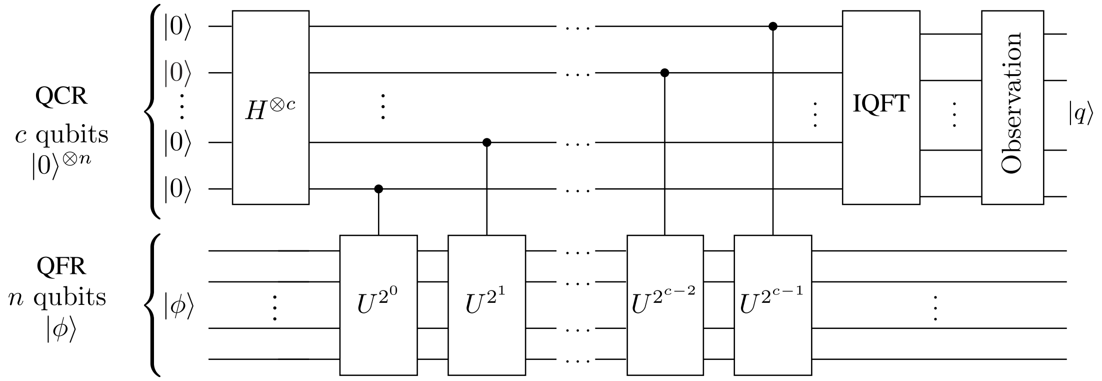


Fig. 7. The quantum circuit of the Quantum Phase Estimation Algorithm, which estimates the eigenvalues of a unitary operator U, which corresponds to its eigenvector $|\phi\rangle$, as described in (30) [48].

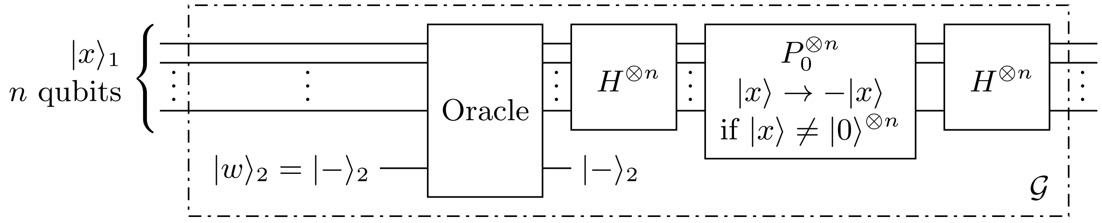

$|x\rangle_1$
n qubits
Oracle
$H^{\otimes n}$
$P_0^{\otimes n}$
$|x\rangle \rightarrow -|x\rangle$
if $|x\rangle \neq |0\rangle^{\otimes n}$
$H^{\otimes n}$
$|w\rangle_2 = |-\rangle_2$
$|-\rangle_2$
$\mathcal{G}$

Fig. 8. Grover operator's quantum circuit including an Oracle, two n-qubit Hadamard gates H and an n-qubit phase shift gate P_0. The HP_0H operator forms the diffusion operator of the Grover operator $\mathcal{G} = HP_0H \cdot O$ [28].

to the sought value δ. Specifically, the Oracle marks an index by changing its sign in the superposition of states. In order to achieve this, an auxiliary qubit $|w\rangle_1$ initialized to the $|-\rangle$ state is used, along with the value δ represented in form of a quantum state. The two Hadamard gates H and a phase rotation gate P_0 that follow the Oracle in Fig. 8 constitute the *diffusion operator* of Grover's circuit, which essentially changes the amplitude of each state by reflecting it with respect to the average amplitude of the current superposition of the states. This has been proven in [28] to result in an amplitude closer to $\sqrt{1/S}$ for each of the specific S states that correspond to the solution entries, while yielding a lower amplitude for the rest of the states that do not correspond to solutions. By repeating this process L_{opt} number of times, the amplitudes of the S quantum states in the superposition that correspond to solution entries gradually become close to $\sqrt{1/S}$, resulting in an $S \cdot (\sqrt{1/S})^2 = 100\%$ probability of observing a state that is indeed the solution state. The resultant amplitude of each solution state prior to measurement is equal to $\sqrt{1/S}$ because all solution states are treated in the same way in Grover's QSA and hence have the same probability $(\sqrt{1/S})^2 = 1/S$ of being observed at the output.

Let us clarify the operation of Grover's QSA with the aid of an example. Let us assume that a database has a size of $N = 32$ entries. Let us also assume that the sought value δ is only stored in a single entry of the database, but we do not know in which portion exactly. Therefore, we have a single solution $S = 1$, leading us to apply the Grover operator $L_{opt} = \lfloor 0.25\pi\sqrt{N/S} \rfloor = 4$ times. As shown in Fig. 9a, we commence with an equiprobable superposition of all indices, since we do not have a particular preference as to which may be associated with the desired entry. After applying the Oracle operator in Fig. 9b, the sign of the amplitude of index 18 is flipped.[15] The red dashed horizontal line in Fig. 9 indicates the mean value of the amplitudes of all superimposed states after the application of the Oracle. In Fig. 9c, the diffusion operator reflects the amplitudes of each state with respect to the aforementioned mean value of the amplitudes. This concludes the first iteration of Grover's QSA. We may conclude that the index 18 has a higher probability of being observed at this stage than the rest of the superimposed states. However, we may increase the probability of observing the solution state 18 even further by applying three more Grover iterations. Following the same approach, Fig. 9d and Fig. 9e characterize the second Grover iteration, Fig. 9f and Fig. 9g the third Grover iteration, while Fig. 9h and Fig. 9i illustrate the fourth and final Grover iteration. In Fig. 9i, the probability of observing the solution state 18 after the fourth Grover iteration is equal to 99.92%. Again, these intermediate steps of Grover's QSA are not readily accessible to us, therefore we have to find another way of determining, when to stop the iterations and observe the resultant state. For that, we have to know both the number of solutions in the database and the size of the database.

Please note that if there are no solutions in a search problem, corresponding to $S = 0$, the Oracle in Fig. 8 will not mark any quantum state and hence the diffusion operator will leave the amplitudes of the quantum states unaltered, since the amplitude of each of the states found in an equiprobable

[15] Please note that in practice we will not be aware of that, since we have not observed the quantum system yet. However, for the sake of clarity, we show the intermediate steps of Grover's QSA.

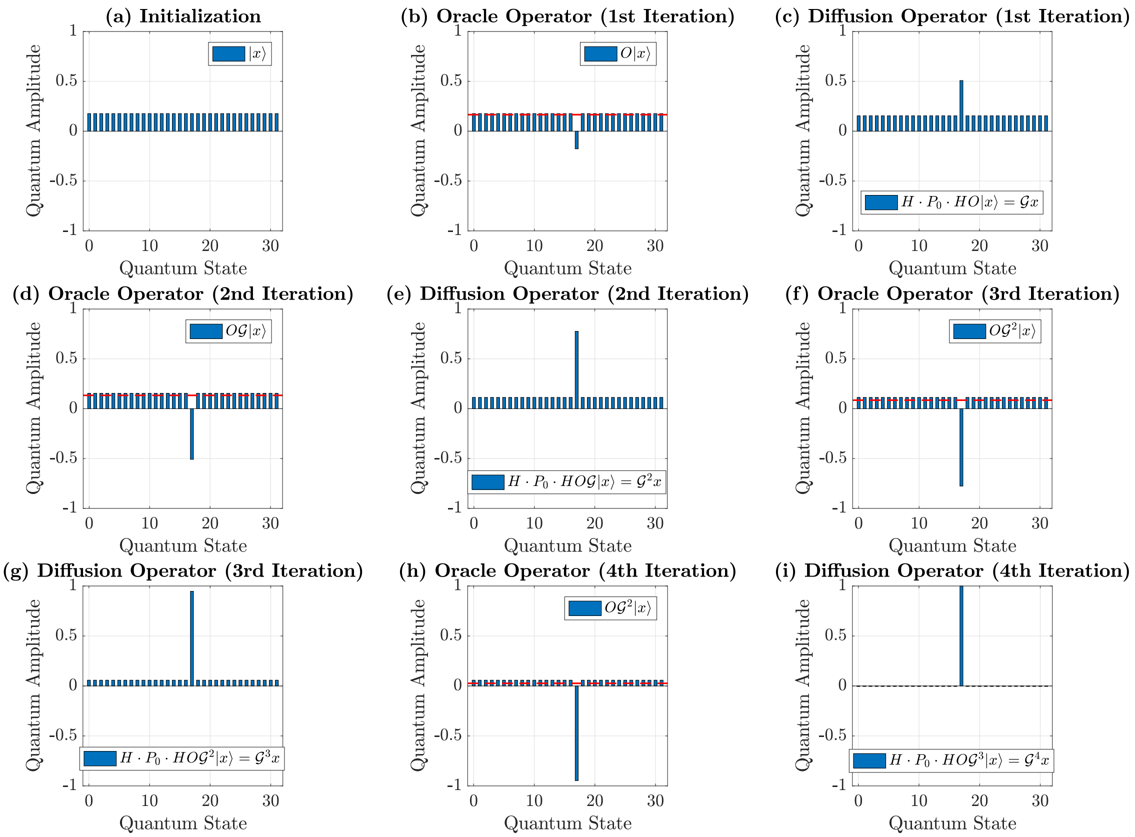


Fig. 9. Example of Grover's QSA in a database with $N = 32$ entries, where the searched value exists only in the entry with index 18. Since there is only a single solution $S = 1$ in a database of size $N = 32$, we have to perform $L_{opt} = 4$ Grover iterations. The red dashed lines indicate the mean value of the amplitudes after each Oracle operation.

superposition of states is equal to the average amplitude and hence a reflection with respect to the average amplitude will not affect the system. Therefore, regardless of the number of Grover iterations, the initial superposition will not change and a potential measurement at the end will result in any of the N states with equal probability. We can then classically check that the observed index does not correspond to a solution in the database, and hence conclude that there is no solution to the search problem.

7) Boyer-Brassard-Høyer-Tapp Quantum Search Algorithm: Nevertheless, requiring *a priori* knowledge of the number of solutions that exist in the system may not always be viable in practical engineering problems. A beneficial extension of Grover's QSA has been introduced by Boyer *et al.* [31] in the form of the so-called Boyer-Brassard-Høyer-Tap (BBHT) QSA, which is applicable in the specific scenario, where the actual number S of valid solutions is unknown, whilst imposing the same order of complexity as Grover's QSA, namely $O(\sqrt{N})$ in a database having N entries. The BBHT QSA solves the same problem as Grover's QSA, while assuming less knowledge about the database. Therefore, it may be employed in a higher number of engineering problems, where no information is available about the entries of the database. Since the number of solutions S is unknown, we are unable to find the optimal number of Grover iterations L_{opt} that we should apply to the initial equiprobable superposition of states in Fig. 8. Hence, it employs classical processing and a "trial-and-error" approach for finding L_{opt}, proven to eventually lead to a 100% probability of success in [31]. The flowchart of the BBHT QSA is depicted in Fig. 10, where $\lambda = 6/5$ is a constant that should be chosen to be in the range [6/5, 4/3] [31]. If the BBHT QSA is not terminated after $4.5\sqrt{N}$ applications of Grover's operator, we may conclude that there is no solution for this search problem.

8) Dürr-Høyer Quantum Search Algorithm: A quantum search algorithm that solves a different search problem was conceived by Dürr and Høyer [32]. More specifically, the Dürr-Høyer (DH) QSA is employed for identifying the extreme values of an unsorted database having N entries, while imposing a low complexity, which is on the order of $O(\sqrt{N})$. In this problem, either the minimum or the maximum entry of a database is sought, without knowing the specific value of that minimum or maximum entry. Therefore, the sought value δ is unknown. Let us describe the problem, when the minimum entry of the database is desired, without any loss of generality, as described in the flowchart of Fig. 11. The DH QSA starts by randomly picking one of the N entries in the database. Let us assume that the randomly selected entry has a value δ_i and an index i. It then invokes the BBHT QSA for finding any entry that has a lower value than the randomly picked one. Since there is no knowledge about the database, it is not possible to know how many entries have a value lower than δ_i, therefore only the BBHT QSA can be used. If we somehow were

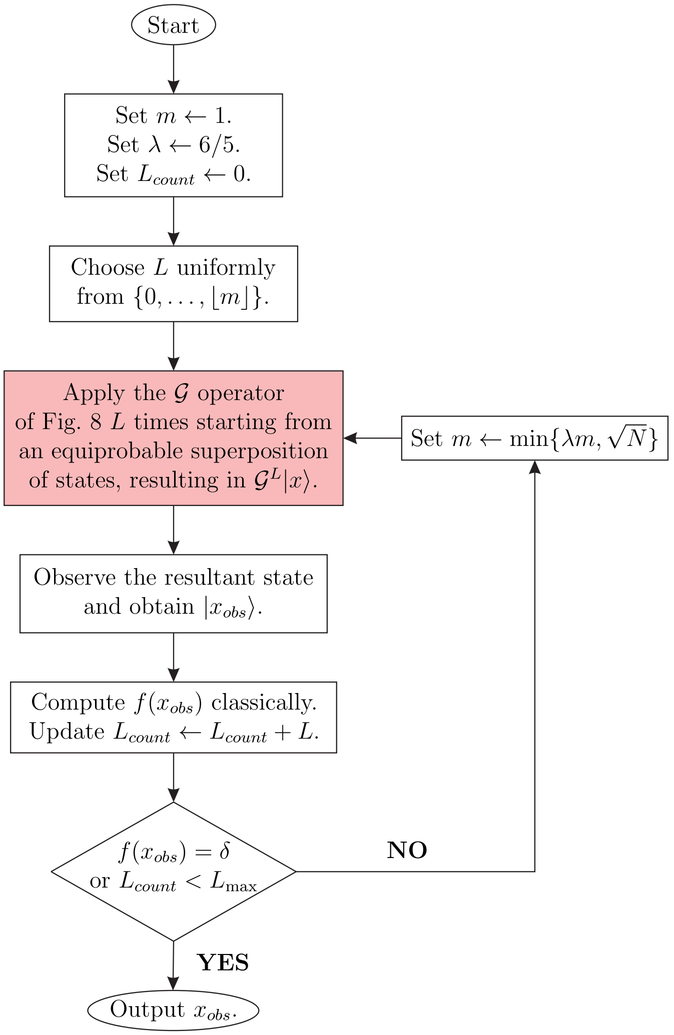

Start
Set $m \leftarrow 1$.
Set $\lambda \leftarrow 6/5$.
Set $L_{count} \leftarrow 0$.
Choose L uniformly from $\{0, \ldots, \lfloor m \rfloor\}$.
Apply the $\mathcal{G}$ operator of Fig. 8 L times starting from an equiprobable superposition of states, resulting in $\mathcal{G}^L|x\rangle$.
Set $m \leftarrow \min\{\lambda m, \sqrt{N}\}$
Observe the resultant state and obtain $|x_{obs}\rangle$.
Compute $f(x_{obs})$ classically.
Update $L_{count} \leftarrow L_{count} + L$.
$f(x_{obs}) = \delta$ or $L_{count} < L_{\max}$
NO
YES
Output x_{obs}.

Fig. 10. Flowchart of the BBHT QSA. The colored box represents the operation of Grover's QSA's quantum circuit of Fig. 8, while the rest of the steps are performed in the classical domain. The value of λ remains constant throughout the operation, while m is always initialized to 1. When the maximum number of allowed iterations $L_{\max}$ is at least $4.5\sqrt{N}$, there is a $\approx 100\%$ probability of success.

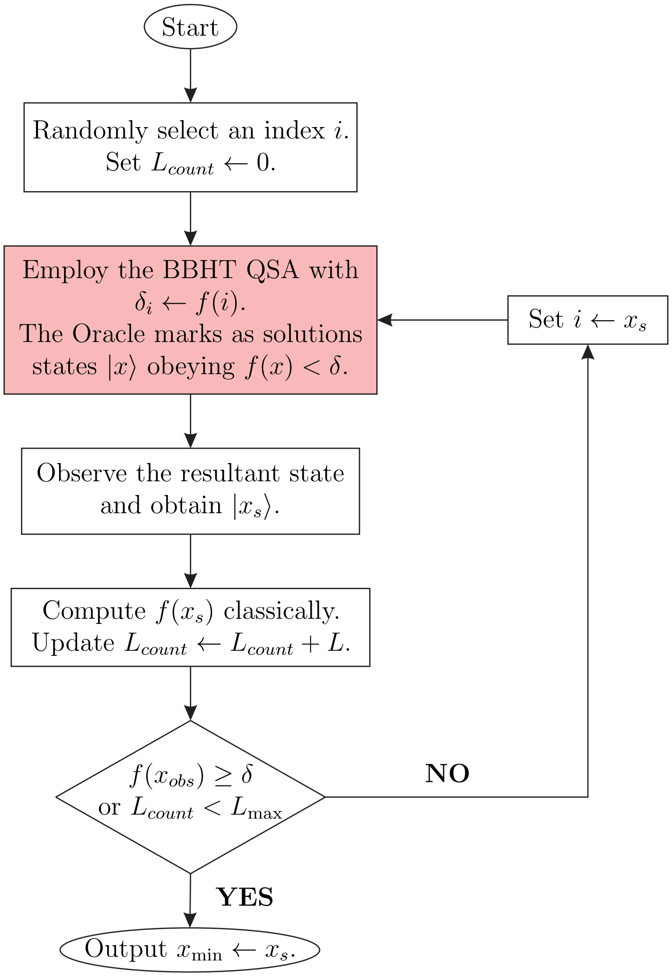

Start
Randomly select an index i.
Set $L_{count} \leftarrow 0$.
Employ the BBHT QSA with $\delta_i \leftarrow f(i)$.
The Oracle marks as solutions states $|x\rangle$ obeying $f(x) < \delta$.
Set $i \leftarrow x_s$
Observe the resultant state and obtain $|x_s\rangle$.
Compute $f(x_s)$ classically.
Update $L_{count} \leftarrow L_{count} + L$.
$f(x_{obs}) \geq \delta$ or $L_{count} < L_{\max}$
NO
YES
Output $x_{\min} \leftarrow x_s$.

Fig. 11. Flowchart of the DH QSA. The colored box represents the operation of Grover's QSA's quantum circuit of Fig. 8, while the rest of the steps are performed in the classical domain. The randomly selected index i at the beginning of the algorithm may be replaced by a deterministically selected index, if there is knowledge that specific indices are favoured to correspond to low-valued entries. The maximum number of applications of Grover's operator is $L_{\max} = 22.5\sqrt{N}$.

aware of the number of entries that have a value lower than δ_i, then Grover's QSA could also be used. Once an entry with a lower value than δ_i is found, corresponding to the index x_s and hence $f(x_s) < \delta_i$, we update the value δ_i with the newly found entry's value $\delta_i = f(x_s)$. Then another BBHT QSA iteration is employed for finding an entry that has a lower value than the updated δ_i. This process is repeated until no better value is found.

Since the DH QSA uses the BBHT QSA, its minimum complexity is equal to $4.5\sqrt{N}$ Grover iterations, referring to the case, where the initially selected entry δ_i was indeed the minimum entry in the database. That would result in the BBHT QSA not being able to find an entry with a lower value, causing it to terminate after $4.5\sqrt{N}$ applications of Grover's operator. The maximum number of Grover iterations required for finding the minimum of the database was proven by Dürr and Høyer to be equal to $22.5\sqrt{N}$ Grover iterations [32]. In [62] it was shown that if the initial entry is carefully chosen instead of being randomly chosen, the average complexity of the DH QSA is further reduced. At the same time, if offline statistics are available about the database of the specific engineering problem, a one-to-one relationship between the number of Grover iterations used and the success probability may be found [62].

9) Quantum Counting Algorithm: In 2000, Brassard *et al.* proposed the Quantum Counting Algorithm (QCA) [50], by combining Grover's QSA [28] and the QPEA [48]. The problem that is solved by using the QCA is the search for the number of solutions S in a search problem. Given a database having N entries, we are interested in finding how many times a known value δ appears in the database, without aiming to find its position in the database. In order to achieve this, the controlled-U_f gates of Fig. 7 are replaced by controlled-Grover operators. Explicitly, the Grover operators of Fig. 8, are used in the quantum circuit of Fig. 12. Furthermore, the function register consists of $n = \log_2 N$ qubits initialized in an equiprobable superposition of $2^n = N$ states. The eigenvector

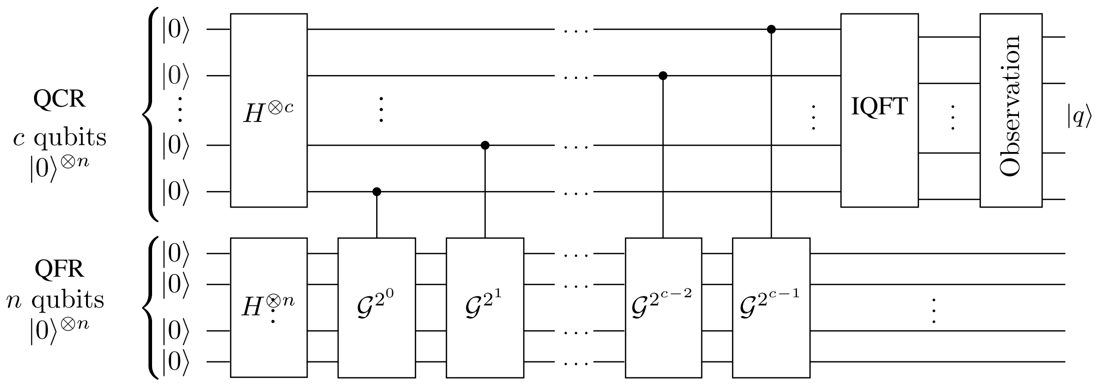


Fig. 12. The quantum circuit of the Quantum Counting Algorithm [34]. It employs the quantum circuit of the QPEA shown in 7, where the U operator is the Grover operator $\mathcal{G}$ and the quantum function register is initialized to an equiprobable superposition of all states, which represents the eigenvector of Grover's operator.

of Grover's QSA consists of a superposition of the specific states that do correspond to solutions in the database and a superposition of the states that do not correspond to solutions in the database. By creating an equiprobable superposition of all states at the beginning of the circuit, we essentially feed the controlled-Grover operators with their eigenvector. Therefore, an application of Grover's operator to such a superimposed state will result in a rotation of their amplitudes [50]. The rotation angle depends on the ratio between the number of solutions S and the size of the database N. Therefore, by applying the QPEA using Grover's QSA, the QCA obtains the number of solutions S upon observing the control register at the output of the QFT seen in Fig. 12, followed by classical processing.

The QCA's accuracy depends on both the number of qubits in the control register c. Its complexity depends on both the number of qubits in the control register c and in the function register n. In other words, the complexity to be invested depends on the required accuracy in terms of the number of solutions, as well as on the size of the database. Again, the optimal classical algorithm is the full search, since all entries in the unsorted database should be checked in order to count the number of solutions. This results in a complexity on the order of $O(N)$ for the full search. The QCA achieves a quadratic speedup compared to the full search, with the specific complexity required depending on both the estimation error margin and on the size of the database [50].

10) Quantum Heuristic Algorithm: In 2000, Hogg proposed a Quantum Heuristic Algorithm (QHA) [51], [52], which relies on Grover's QSA's circuit. The aim of the QHA is to solve the particular optimization problem of finding either the minimum or the maximum of a database by requiring fewer CFEs than the DH QSA, when the database has some form of correlation. In more detail, Grover's QSA, the BBHT QSA and the DH QSA are optimal, when they perform search in an unsorted database. When the entries of a database are inherently correlated to each other, heuristic algorithms may succeed in solving the optimization problem, while requiring fewer queries to the database. In order to achieve this, Hogg changed both the Oracle and the diffusion operator used in Grover's QSA. Recall that in Grover's QSA, where δ is known, the Oracle marks the quantum states that correspond to solutions by flipping the sign of their amplitudes. This may be interpreted as a rotation by π for the amplitudes of the solution states and no rotation for the rest of the states. Since in the optimization problem the minimum value δ is unknown, Hogg conceived a different Oracle, where the rotation angle of the amplitudes of *each* state depends on the value of the entry it corresponds to. The QHA has been demonstrated to outperform Hogg QSA [51], but it needs fine-tuning for each specific system and scenario, since the exact rotation angles applied by the Oracle and the diffusion operator have to be appropriately chosen. This is reminiscent of the employment of classical heuristic algorithms, like the Genetic Algorithm (GA) [63], [64], where the algorithm's parameters have to be carefully selected in order for a heuristic algorithm to converge to the solution.

11) Quantum Genetic Algorithm: In order to solve the same optimization problem of finding either the minimum or maximum of a database, Malossini *et al.* proposed the Quantum Genetic Algorithm (QGA) [53], which is an amalgam of the classical GA [63], [64] and of the DH QSA. Please note that as with the QHA, the QGA may be employed in particular problems, where there is correlation between the entries of the database.

More specifically, in the classical GA, a population of P *agents* or *chromosomes* is generated, where each agent represents an index of the database. The database is then queried P times, once for each of the agents of the population. After combining the two best so-far found[16] agents, the next generation of the population is created based on them, with the aim of having agents representing even smaller values. Eventually, after a sufficiently high number of generations, an agent corresponding to the minimum value of the database is found. Since it cannot be mathematically predicted, when the GA will find the minimum of the database, the algorithm is terminated after a predetermined number of generations.

In the QGA, the same procedure is followed as in the GA with one difference. The DH QSA is invoked for searching

[16] By "best so-far found" we refer to the agents that correspond to the smallest entries in the database in that population.

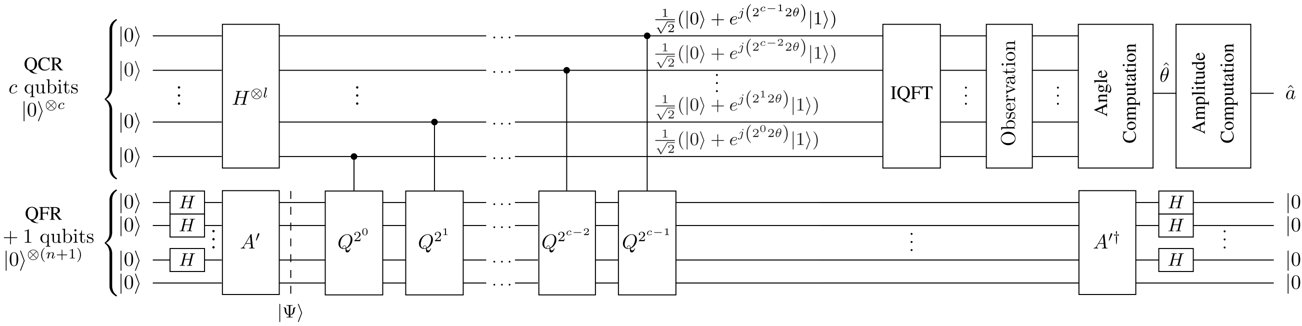

QCR
c qubits
$|0\rangle^{\otimes c}$
$|0\rangle$
$H^{\otimes l}$
$\frac{1}{\sqrt{2}}(|0\rangle + e^{j(2^{c-1}2\theta)}|1\rangle)$
$\frac{1}{\sqrt{2}}(|0\rangle + e^{j(2^{c-2}2\theta)}|1\rangle)$
$\frac{1}{\sqrt{2}}(|0\rangle + e^{j(2^{1}2\theta)}|1\rangle)$
$\frac{1}{\sqrt{2}}(|0\rangle + e^{j(2^{0}2\theta)}|1\rangle)$
IQFT
Observation
Angle Computation
$\hat{\theta}$
Amplitude Computation
$\hat{a}$
QFR
$n+1$ qubits
$|0\rangle^{\otimes(n+1)}$
H
A'
$|\Psi\rangle$
Q^{2^0}
Q^{2^1}
$Q^{2^{c-2}}$
$Q^{2^{c-1}}$
$A'^{\dagger}$

Fig. 13. The quantum circuit of the Quantum Mean Algorithm [55]. It employs the quantum circuit of the QPEA shown in 7, where the *U* operator is the function's operator $U_f = f(x)$. The quantum function register is initialized to the superposition of states $|\Psi\rangle$, using *n* Hadamard gates and the operator *A*, which includes two operations of U_f and a controlled rotation of the (*n*+1)th auxiliary qubit. The circuit estimates the mean value of the function's values $a = \sum_{x=0}^{N} f(x)/N$.

through the population of each generation for finding the best agents. In other words, the DHA QSA in the QGA is employed for reducing the complexity imposed by the GA while querying the database during each generation. Since only the two best agents have to be found in order to create the subsequent generation's population, the DH QSA may be employed twice. The QGA was demonstrated to outperform the GA for the same complexity, or to require a lower complexity for the same success probability.

12) Harrow-Hassidim-Lloyd Algorithm: The Harrow-Hassidim-Lloyd (HHL) algorithm [54] is a quantum algorithm, which relies on the QPEA and solves linear systems of equations at an exponential reduction of the computational complexity required. The problem of solving a linear system of equations may be formulated as follows. Given an (*N* × *N*)-element matrix **A** and an (*N* × 1)-element vector **b**, find an (*N* × 1)-element vector **x**, so that we have $\mathbf{A} \cdot \mathbf{x} = \mathbf{b}$.

In order for the HHL algorithm to be practically applicable, the goal of the problem should be a bit different from the aforementioned one. The linear system of equations has to exhibit a few specific features. Firstly, the output is a superposition of *N* states $|x\rangle$, where the values of the solution vector are encoded in the amplitudes of that superposition of states. Therefore, it cannot provide all values of the solution vector **x** for further classical processing. Alternatively, it may result in specific properties for the solution vector, for example for its moments. Moreover, both the solution vector $\overrightarrow{\mathbf{x}}$ and the vector $\overrightarrow{\mathbf{b}}$ should be unit-vectors. Furthermore, the matrix **A** should be sparse.

The HHL algorithm estimates the eigenvalues of the matrix **A**, using an appropriately modified version of the QPEA of Section II-B5. The QPEA circuit is employed as a subroutine of an amplitude amplification procedure in the HHL algorithm, in order to further reduce its complexity of obtaining the solution quantum state $|x\rangle$. The HHL algorithm's complexity was further reduced by Ambainis in [67], while the precision of the estimated solution was exponentially increased by Childs *et al.* in [68].

13) Quantum Mean Algorithm: In 2011, Brassard *et al.* [55] proposed the Quantum Mean Algorithm (QMA), which succeeds in finding the mean value $a = \sum_{x=0}^{N} f(x)/N$ of a function *f* requiring an exponentially reduced number of evaluations of the function than the optimal classical algorithm, since the latter would require access to all legitimate evaluations of the function. In order to achieve this, a modified QPEA is used, where the controlled-U_f operation evaluates the output of the function *f* to its inputs, as illustrated in Fig. 13. One of the main differences between the QMA and the QPEA is that even though there are *N* legitimate inputs for the function *f*, $\log_2(N) + 1 = n + 1$ qubits are employed in the function register, instead of $n = \log_2(N)$, which would have been the case in the QPEA. The above-mentioned extra qubit is required, because the function register is initialized using a unitary operator *A*, which relies on the function *f* and it performs controlled-rotations on the extra qubit [55], [56]. At the output of the unitary operator *A*, there is a superposition of states $|\Psi\rangle$. Each state of Ψ was used for evaluating U_f in the unitary operator *A*. Based on the U_f and the controlled-rotations imposed on the auxiliary qubit, the amplitudes of half of the states in $|\Psi\rangle$ are equal to their respective function's output. In fact, this is true for the specific states, for which the auxiliary qubit is equal to $|1\rangle$. The size of the control register determines the precision of the estimated mean value, similarly to the QPEA.

14) Quantum Weighted Sum Algorithm: The Quantum Weighted Sum Algorithm (QWSA) [56], [69] is based on the QMA of Section II-B13 and it finds the weighted sum of the values of a function *f* with *N* inputs, again requiring $O(\sqrt{N})$ evaluations of the function *f*. The difference between the QWSA and the QMA is the initialization of the function register, as seen in Fig. 14. Instead of initializing it in an equiprobable superposition of states, the inputs of the function *f* are initializated in a superposition of states, where each state's amplitude is the weight of the wanted weighted sum. Therefore, the QWSA may be considered as a generalization of the QMA, since in the latter all weights are the same and equal to 1/*N* in an *N*-element database, resulting in the use of Hadamard gates instead of general unitary rotation gates, as shown in Fig. 13.

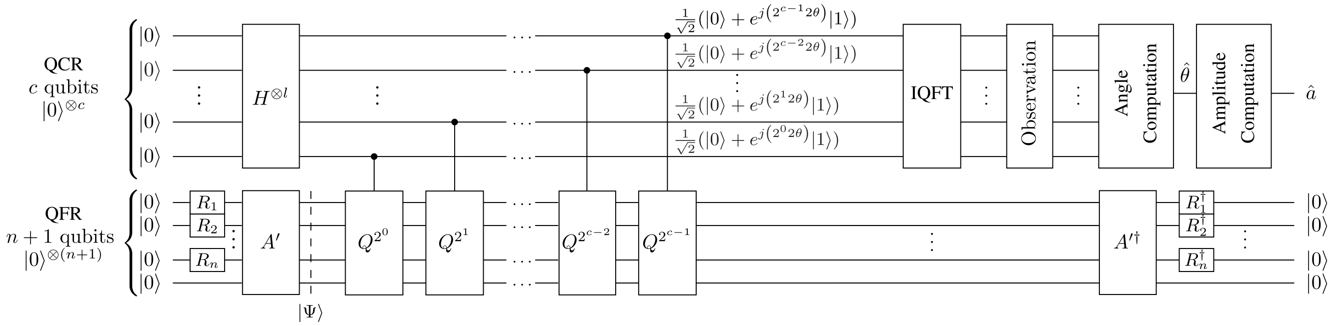


Fig. 14. The quantum circuit of the Quantum Weighted Sum Algorithm [56]. It employs the quantum circuit of the QMA shown in 13, with the difference that the quantum function register is not equiprobably initiliazed. Rather, the initilization is performed based on unitary rotation gates, which rely on the weights of the desired weighted sum.

Last but not least, an overview of the quantum algorithms discussed in this survey in terms of their application and complexity is carried out in Tables III and IV. In terms of practical implementation, *IBM Q Experience* has a *drag and drop editor* for the sake of synthesizing quantum circuits out of the fundamental quantum gates of Fig. 4 as well as a *Python toolkit*[17] for designing more complex quantum circuits. Consequently, Grover operator's quantum circuit, presented in Fig. 8, may be readily implemented using IBM's framework at least for a limited number of qubits. Nevertheless, we should state that at the time of writing, there has not yet been any real-life demonstration of employing a quantum-assisted solution in order to solve a practical wireless problem. Therefore, the comparisons between the classical and the quantum solutions employed in the wireless communication problems in the following section are based on the theoretical capabilities of the algorithms.

III. Optimization Problems and Quantum Algorithms in Communications

Let us now shift our attention to discussing potential applications in the field of wireless communications, which would benefit from using a quantum computer. Most of these optimization problems in the current state-of-the-art employ algorithms for finding suboptimal solutions, because of the excessive cost of finding an optimal solution. This is particularly so for joint optimization of several functions, such as joint channel estimation, data detection and synchronization for example, or for multi-component optimization, where the search space is expanded.

A. Multi-User Detection

1) The Problem: In the uplink of an OMA system, like Code Division Multiple Access (CDMA) [70], Orthogonal Frequency Division Multiple Access (OFDMA) [71], Single-Carrier Frequency Division Multiple Access (SC-FDMA) or Time Division Multiple Access (TDMA), the users are either allocated all available resources in a round-robin fashion, or they are allowed to share orthogonal resources simultaneously. For example, in TDMA the whole bandwidth is allocated to a single user for a few time slots. On the other hand, in CDMA the whole bandwidth is used by all users supported in the system simultaneously, in order to transmit their narrowband signal after spreading it by a unique user-specific, orthogonal spreading code. In OFDMA, where the spectrum is partitioned in multiple orthogonal subcarriers, each user may be allocated a subset of user-specific subcarriers, which no other user is allowed to activate.

By contrast, in the uplink of a NOMA system [5], [72]–[76] the users are allowed to simultaneously share the same frequency and time resources in order to increase the cell throughput by being able to support more users simultaneously. However, the BS now has the new task of extracting the signal of each user from the received superposition of signals,[18] as illustrated in Fig. 15, given the knowledge of the channel states and the symbol constellation that was used by each user. In more detail, each user transmits its own symbol based on its constellation. Since the system is synchronous, every transmitted signal is added together at each receive antenna. Each transmitted signal is modified based on the channel it utilizes. At the receiver, Additive White Gaussian Noise (AWGN) is added at each receive RF chain. The Multi-User Detector has to estimate the three transmitted symbols based on the received signals, the channel states, the noise power and any prior estimates that may be available. This extraction is also currently required in the uplink of the specific CDMA systems, where non-orthogonal spreading codes have been allocated to the users [70]. This is termed as the problem of Multi-User Detection (MUD).

2) The Classical Algorithms: The optimal Maximum Likelihood (ML) detector finds the most likely U-user symbol vector, relying on the received signal, on the estimates of the channels and on the estimated noise power. More specifically, the ML MUD searches through all legitimate transmitted multi-user symbol combinations that may have resulted in the reception of that specific signal and in the end outputs the most likely U-user symbol vector. As an example, let us assume that $U = 20$ users are supported by the system and that each of them transmits $L = 4$-ary Quadrature Phase Shift Keying (QPSK) symbols. Then, the signal received at the BS

[17] https://developer.ibm.com/code/open/projects/qiskit/

[18] Please note that the mentioned superposition of signals is their addition in the classical domain, since in a synchronous system the signals arrive simultaneously. It should not be confused with the superposition of quantum states.

TABLE III
THE QUANTUM ALGORITHMS REVIEWED

Algorithm	Application	Description	Complexity
Deutsch Algorithm [45]	Classification	Determines whether a binary function $f : \{0,1\} \rightarrow \{0,1\}$ does or does not have a one-to-one mapping.	$O(1)$
Deutsch-Jozsa Algorithm [46]	Classification	Determines whether a function $f : \{0,1\}^n \rightarrow \{0,1\}$ is balanced or constant.	$O(1)$
Simon's Algorithm [47]	Evaluates a Function's Property	Operates on functions $f : \{0,1\}^n \rightarrow \{0,1\}^n$ that satisfy $f(x) = f(y)$ if and only if $x = y$ or if $x \oplus y = s$, and finds the value s.	$O(n)$
Shor's Algorithm [33]	Factoring	Solves the problem of factoring a given integer N.	$O(\log N)$
Quantum Phase Estimation Algorithm [48]	Order finding, Factoring, Search	Estimates the eigenvalue of a given unitary operator with the aid of c control qubits, which define the estimation precision. The complexity depends on whether that unitary operator is less or more complex than the IFFT operator employed.	$O(2^c)$
Grover's Algorithm [28]	Search	Finds the index of an entry in a database of size N that is equal to δ with $\sim$100% probability of success. The number of times that δ appears in the database has to be known *a priori*.	$O\left(\sqrt{N}\right)$
Boyer-Brassard-Høyer-Tapp (BBHT) Algorithm [31]	Search	Finds the index of an entry in a database of size N that is equal to δ with $\sim$100% probability of success. The number of times that δ appears in the database is not required to be known *a priori*.	$O\left(\sqrt{N}\right)$, but higher than Grover's QSA
Dürr-Høyer Algorithm [32]	Search	Finds the index of the minimum entry in a database of size N with $\sim$100% probability of success. Only the size of the database is required to be known *a priori*.	$O\left(\sqrt{N}\right)$, but higher than BBHT's QSA
Quantum Counting Algorithm [50]	Search	Estimates the number of times a known value δ appears in a database of size N, with the aid of c control qubits. The complexity depends on whether the employed Grover operator is less or more complex than the employed IFFT operator.	$O(2^c)$
Quantum Heuristic Algorithm [51]	Search	Finds the index of an entry in a database of size $N = 2^n$ that is equal to δ using a heuristic approach of Grover's QSA.	$O\left(e^{-\frac{3n}{4}+\frac{\ln n}{4}}\right)$

has been constructed based on only one out of $L^U = 4^{20}$ possible combinations. In other words, the ML MUD has to search through more than one *trillion* legitimate U-symbol vectors in order to find the most likely one. In general, the computational complexity of the ML MUD is on the order of $O(L^U)$. In an OMA system, where a received signal conveys the information of a single user, the ML MUD may have an affordable complexity, which is on the order of $O(L)$.

Next-generation wireless communication systems may employ iterative receivers in the uplink of a NOMA system. In iterative receivers, information is allowed to be exchanged between the MUD and the channel decoders.[19] In this case, an MUD that outputs soft information and also accepts

[19] Since each of the U users has encoded its own bit information stream independently, the BS has to employ U channel decoders in parallel.

TABLE IV
THE QUANTUM ALGORITHMS REVIEWED (CONTINUED)

Algorithm	Application	Description	Complexity
Quantum Genetic Algorithm [53]	Search	Finds the index of an entry in a database of size $N = 2^n$ that is equal to δ using an amalgam of the DH algorithm and the classical genetic algorithm.	User-defined
Harrow-Hassidim-Lloyd Algorithm [54]	Solving Linear Systems of Equations	Solves llinear systems of equations $Ax = b$, with κ being the ratio of the largest over the lowest eigenvalue of the sparse matrix A and N the dimension of A, with the aid of the phase estimation algorithm. The estimated solution cannot be readily obtained classically, but rather further manipulation may be performed in the quantum domain in order to extract the desired properties of the solution.	$O\left(\kappa^2 \log N\right)$
Quantum Mean Algorithm [55]	Function's Moment Finding	Estimates the mean value a function f over its argument space of size N, with the aid of c control qubits, which determine the estimation's precision.	$O\left(\sqrt{N} c \log c\right)$
Quantum Weighted Sum Algorithm [56]	Function's General Moment Finding	Estimates the weighted sum of the outputs of a function f over its argument space of size N, with the aid of c control qubits, which determine the estimation's precision.	$O\left(\sqrt{N} c \log c\right)$
Non-dominated Quantum Optimization [65]	Search & Solving Non-Linear Systems of Inequalities	Finds the entire set of Pareto-optimal solutions in a database of N entries.	$O\left(N\sqrt{N}\right)$
Non-dominated Quantum Iterative Optimization [66]	Search & Solving Non-Linear Systems of Inequalities	Finds N_{OPF} Pareto-optimal solutions in a database of N entries.	$O\left(N_{\text{OPF}}\sqrt{N}\right)$

soft estimates as input should be used. The optimal Soft-Input Soft-Output (SISO) MUD is the Maximum *A posteriori* Probability (MAP) MUD [6], which outputs bit-based or symbol-based Log-Likelihood Ratios (LLR). The LLR of a bit represents the log-domain probability of that bit to have been 0 or 1, when it was transmitted. Similarly, the symbol LLR describes the log-domain probability of that symbol to have been transmitted as one of the legitimate symbols in the constellation. The MAP MUD creates the LLRs by taking into account all possible multi-level symbol vectors, requiring a computational complexity on the same order as the ML MUD [6].

The excessive complexity required by the ML and MAP MUDs in NOMA systems has driven the research community to low-complexity sub-optimal solutions, such as the Minimum Mean Square Error (MMSE) detector [70], the Zero Forcing (ZF) detectors [70], the Ant Colony Optimization (ACO) based MUD [77], the Particle Swarm Optimization (PSO) based MUD [78] and the SIC [70] MUD.

In the uplink of a multi-user system, the SIC MUD detects the signal of the user experiencing the best channel first, by treating as interference the signals of the rest of the users, which are also present in the superimposed received signal. Having detected the signal of the best user, it reconstructs that user's noiseless transmitted signal and subtracts it from the received signal. Therefore, only the transmitted signals of $(U - 1)$ users are left in the composite received signal. The same procedure is repeated until the signals of all users are detected. The SIC MUD requires a low complexity on the order of $O(L{\cdot}U)$, which scales linearly with the number of users supported. However, it does not perform well in rank-deficient scenarios and when the channel conditions of different users are similar. In the latter case Parallel Interference Cancellation (PIC) is preferred [70]. Therefore, when SIC is employed, appropriate scheduling is required for matching groups of users together in order to share the medium simultaneously.

3) The Quantum Algorithms: In order to reduce the computational complexity of the optimal ML detection, which requires a full search, the DH QSA of Section II-B8 was employed in [56] and [62], where it was demonstrated that it approaches the optimal performance. The operation of the DH QSA in the problem of MUD is described in Fig. 16. The

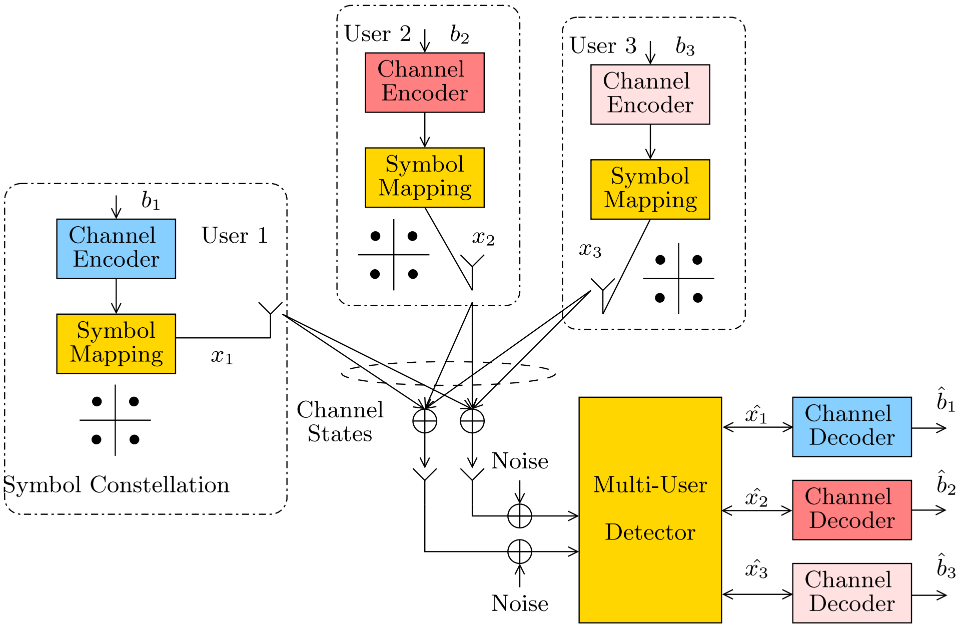


Fig. 15. The problem of Multi-User Detection in the uplink of a synchronous multiple access system.

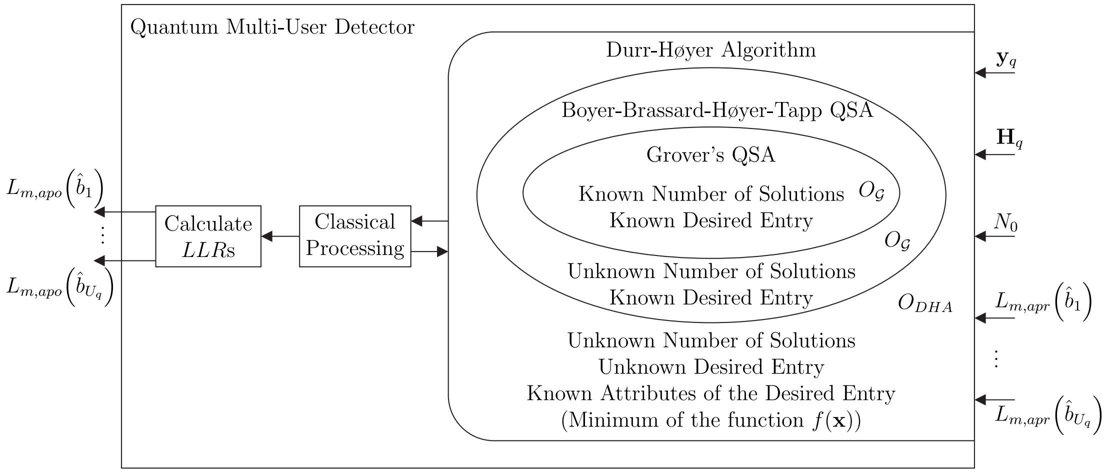

Quantum Multi-User Detector
Durr-Høyer Algorithm
Boyer-Brassard-Høyer-Tapp QSA
Grover's QSA
Known Number of Solutions
Known Desired Entry
$O_{\mathcal{G}}$
$O_{\mathcal{G}}$
Unknown Number of Solutions
Known Desired Entry
O_{DHA}
Unknown Number of Solutions
Unknown Desired Entry
Known Attributes of the Desired Entry
(Minimum of the function $f(\mathbf{x})$)
Classical Processing
Calculate LLRs
$L_{m,apo}\left(\hat{b}_1\right)$
$L_{m,apo}\left(\hat{b}_{U_q}\right)$
$\mathbf{y}_q$
$\mathbf{H}_q$
N_0
$L_{m,apr}\left(\hat{b}_1\right)$
$L_{m,apr}\left(\hat{b}_{U_q}\right)$

Fig. 16. Inside a quantum multi-user detector.

DHA employed in the QMUDs makes multiple calls to the BBHT QSA. Grover's QSA is not used, but it is included for completeness, since the BBHT QSA uses the same Oracle O, but may even be capable of finding a solution with a $\sim$100% probability, when the number of solutions is unknown. The QMUD may also be performed on a subcarrier basis in a multicarrier system. The DHA processes the signals received $\mathbf{y}_q$ at all the receive AEs on the qth subcarrier, along with the channel state estimates $\mathbf{H}_q$, the noise's variance N_0 and the *a priori* LLRs $L_{m,\,apr}(\hat{\mathbf{b}})$. After it completes its initial procedure, the DHA exchanges information with a classical processing unit, which determines whether the DHA should or should not be called again, while additionally determining its search space. Finally, the QMUD outputs the calculated *a posteriori* LLRs $L_{m,\,apo}(\hat{\mathbf{b}})$.

In [62], a deterministic initialization of the DH QSA was proposed for exploiting the low-complexity Zero Forcing (ZF) and Minimum Mean Square Error (MMSE) [79] detectors. More specifically, instead of randomly initializing the DH QSA, initially a ZF or MMSE detector is employed and its output is used as the initial guess of the DH QSA. This was shown to further reduce the complexity of the QMUD. Moreover, an early-stopping criterion was proposed in [62], where the DH QSA is terminated after a specific number of Grover iterations, without degrading the Bit Error Rate (BER) performance of the system. The specific number of Grover iterations used for the early-stopping criterion was found via simulations and histograms.

When iterative detection is employed at the base station, a SISO MUD should be used in order to exchange LLRs with the SISO decoders. Therefore, the DH QSA-based hard-output QMUD is not suitable. In [56] and [80], a SISO QMUD was proposed based on the QWSA of Section II-B14, exhibiting near-optimal performance, while requiring fewer

CFEs[20] (CFE) than the MAP MUD. In order to calculate an LLR, two weighted sums have to be calculated; one for the LLR's numerator and one for its denominator. The MAP MUD evaluates the Cost Function (CF) for all legitimate multi-level symbols. By using the QWSA twice, we may estimate the weighted sums requiring a lower computational complexity. Please note that there is a performance vs. complexity trade-off, when using the QWSA, due to the control register of the QPEA of Section II-B5. In other words, if we employ more qubits at the control register, a higher precision is achieved during the estimation of the weighted sums, hence resulting in a more accurate LLR value. However, a higher complexity is required, since the complexity of the QWSA scales with the size of the control register [56].

In [80] and [81] another SISO QMUD was proposed, relying on an amalgamation of classical processing and the DH QSA. The SISO QMUD was demonstrated to achieve near-optimal performance with respect to the MAP MUD, while requiring substantially fewer CFEs. The DH QSA-based SISO QMUD employs the DH QSA multiple times in different databases, in order to create a pool of the "*k*-best"[21] multi-level symbols of each weighted sum of each LLR. By classically processing the values found, we are able to estimate the weighted sums of the LLRs and hence to attain a near-optimal performance. Please note that even though the precision of the weighted sums, and hence the LLRs, is lower than that achieved by the QWSA QMUD and the MAP MUD, it is sufficiently close to the real values for the channel decoders to successfuly decode each user's bits. Therefore, since a SISO MUD or QMUD is always followed by channel decoders, the DH QSA-based QMUD of [81] achieves a near-optimal performance, while imposing a lower complexity than the MAP MUD.

B. Joint Channel Estimation and Data Detection

1) The Problem: In the uplink of wireless communications system, accurate channel estimation has to be performed at the base station in order to predict and counteract the effect of the channel, when the signal arrives [79], [82], [83]. In a multi-user NOMA system, all channels between the antennas of all users and the antennas of the base station have to be accurately estimated, otherwise the performance of the MUD would be degraded.

In a multi-carrier system like OFDM, the multi-path channel may be estimated either in the time domain or in the frequency domain. For example, let us assume the scenario where the Power Delay Profile (PDP) of a channel exhibits four paths and that we partition the available bandwidth in 512 non-dispersive subchannels. The channel envelope of each of the four paths may be deemed to fade independently. Assuming that the channel envelope at each path is quasi-static[22] during the channel estimation process, we may either estimate the four time-domain (TD) channel gains of the four paths, or the 512 frequency-domain (FD) subcarrier gains, which represent the Fast Fourier Transform (FFT) of the time-domain PDP, having taken the delay spread of the channel and the sampling frequency into consideration. Typically the FD channel is represented by the terminology of FD CHannel Transfer Function factor (FD-CHTF) [71]. Naturally, a lower complexity may be required for estimating the four time-domain channel gains, than for estimating the channel gain of each subcarrier.

However, the FD channel estimation lends itself to joint channel and data estimation, where the FD channel estimation problem may be thought of as a search for the true continuous-valued subcarrier channel gains. This prohibits the employment of the full search approach, which was previously followed in the MUD problem of Section III-A, since an infinite-sized database should be constructed. The joint channel estimation and data detection problem may however also be considered as two separate problems, the former being dedicated to searching for continuous-valued channel gains, while the latter to searching for discrete-valued multi-user symbols.

2) The Classical Algorithms: In LTE [84], FD pilot signals are transmitted on specific subcarriers of certain OFDM symbols, enabling the user or the base station to estimate the channels for the rest of the subcarriers with the aid of interpolation in the downlink or uplink, respectively. The estimated channel states may be used for the subsequent OFDM information symbols between a pair of OFDM symbols having pilot-subcarriers without any change at the cost of accepting a performance degradation, but not imposing any additional complexity. Alternatively, the estimated subcarrier gain may be used for predicting the subcarrier gains of each subsequent OFDM symbol using linear predictions.

Furthermore, as alluded to above, channel estimation may be combined with data detection for improving both the estimation accuracy of the subcarrier gains and of the detection error probability of the transmitted data, resulting in a joint channel estimator and data detector [85]–[88]. In a multi-user scenario, the MUD replaces the single-usedr symbol detector, hence joint channel estimation and MUD may be used [89]–[93]. In the iterative receiver of a NOMA system, information may be exchanged between the channel estimator, the MUD and the channel decoders for further increasing the channel estimation's accuracy and the channel decoding performance [90]. The Decision-Directed Channel Estimation (DDCE) [94] used in multi-carrier systems initially estimates the FD channel gains based on a pilot OFDM symbol, as depicted in Fig. 17. Initially, the super-imposed pilot signals are used for performing conventional, pilot-assisted channel estimation, associated with the received OFDM symbol period. Based on those channel estimates, the Channel Impulse Response (CIR) prediction filter predicts the channel states that would correspond to the next OFDM symbol, which now carries data. The output of the CIR prediction filter becomes the initial output of the quantum channel estimator. When the next OFDM symbol is received, it invokes the MUD using the predicted channel gains.

[20] The cost function in the MUD problem is the Euclidean distance of the received, noisy multi-level symbol from a legitimate multi-level symbol from the multi-user constellation.

[21] By "best" here we mean the multi-level symbols of each weighted sum that correspond to the highest CF values.

[22] In an OFDM system, a channel is quasi-static, when its channel gain remains constant during an OFDM symbol period. The channel gain between two OFDM symbols may be different, but still constant within their OFDM symbols.

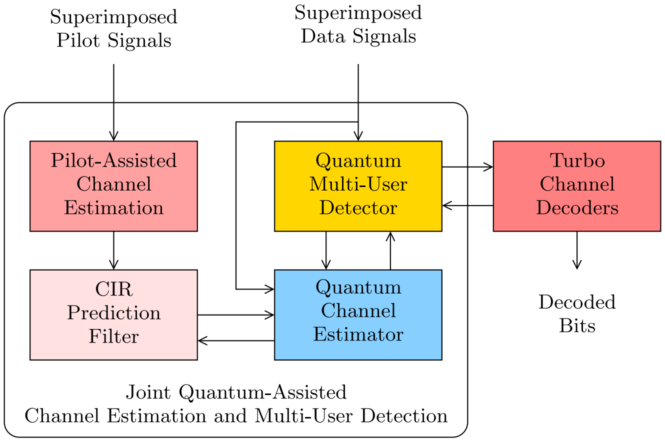

Superimposed Pilot Signals
Superimposed Data Signals
Pilot-Assisted Channel Estimation
Quantum Multi-User Detector
Turbo Channel Decoders
CIR Prediction Filter
Quantum Channel Estimator
Decoded Bits
Joint Quantum-Assisted Channel Estimation and Multi-User Detection

Fig. 17. System model of a joint channel estimation and multi-user detection receiver in the uplink of a multi-carrier NOMA system employing decision-directed channel estimation.

It then selects the specific multi-level symbols, which were detected sufficiently reliably,[23] and assumes that these were known pilot symbols. Hence it refines the channel estimation process based on those "hypothesized" pilot symbols. In other words, the DDCE combines the separate problems of channel estimation and data detection by employing them sequentially, allowing them to "lend" their output to the other process, in order for it to perform a search in a more accurately constructed database, as exemplified in Fig. 17. The updated FD channel gains may be used for performing a refined MUD process for the same OFDM symbol for improving the estimated LLRs. Similarly, the updated LLRs can be used aftewards for improving the accuracy of the FD channel gains even further. The number of iterations between the channel estimation process and the MUD constitute a design parameter. The DDCE aims for reducing the pilot overhead, and hence increasing the system's effective throughput. Naturally, it imposes a higher complexity than the purely pilot-based channel estimation.

In order to reduce the complexity of the joint channel estimation and data detection, heuristic search algorithms may be used instead of a full search.[24] In [95] a GA-aided joint channel estimator and data detector was proposed, while in [91] the Differential Evolution Algorithm (DEA) was employed for joint channel estimation and data detection. In [93] various heuristic algorithms, such as the GA, the Particle Swarm Optimization (PSO) and the Repeated Weighted Boosting Search (RWBS) algorithm were used instead of a full search for the true continuous-valued channel gains, as well as for the full search of the discrete-valued symbol-space of the MUD. As another design option, a factor-graph based approach was used for joint channel estimation and MUD in MC-IDMA systems in [92]. By exploiting the sparsity of the wireless channels, Prasad *et al.* [88] proposed a methodology that requires fewer pilot symbols, without degrading the performance.

3) The Quantum Algorithms: In [96] the Quantum Repeated Weighted Boosting Search (QRWBS) algorithm was proposed for reducing the computational complexity of the classical evolutionary algorithms-based joint channel estimation and data detection, without degrading the system's performance. To elaborate a little further, the QRWBS is an amalgam of the DH QSA and the RWBS algorithm. Both the RWBS and the QRWBS algorithms create a population of agents, which are transformed to better agents via multiple generations. Please note that an agent in the context of channel estimation represents a continuous-valued FD channel gain, while in the context of data detection it represents a discrete-valued symbol. Therefore, a continuous-valued QRWBS and a discrete-valued QRWBS are employed in [96] for solving the two problems. An agent is deemed to have a higher fitness than another agent, if its channel gain or symbol corresponds to a lower cost function value than the other agent's.

The maximum affordable number of generations[25] is Ξ In both the RWBS and the QRWBS. In the classical RWBS a specific number of agents P is created during each generation. During the ξth generation, where $\xi = 1, \ldots, \Xi$, the agents are classically processed in order to create a new agent, which is termed as the best agent or winner of that generation. The lower the cost function values of the P agents during the ξth generation are, the lower the cost function value of the best agent of that generation will be. Therefore, it is beneficial to create populations, which have agents with as low cost function values as possible. The best agent of a generation is subsequently used as the basis for creating new agents for the next generation. Therefore, the population of the $(\xi + 1)$st generation is created randomly in the vicinity of the best agent of the ξth generation.

The QRWBS algorithm obeys the same procedure, but differs in the creation of the population of each generation. Instead of creating Z agents in each generation, it creates a much higher number of agents $Z_Q \gg Z$. It then employs the DH QSA in that database of Z_Q agents in order to find the specific agent of the population that corresponds to the minimum cost function value of that generation. As discussed in Section II-B8, in the process of searching for the minimum value, the DH QSA also queries the database for other entries, which are later proven not to be the minimum ones. However, due to the particular nature of the DH QSA, most of the extra observed agents have a cost function value close to the minimum one in the database. All these entries are used in the QRWBS in order to form a population of $Z_\xi \ll Z_Q$ agents. The subscript ξ of Z_ξ reflects the fact that due to the probabilistic nature of the DH QSA, the population size may differ from one generation to the next. Both the continuous-valued and

[23] Please recall that a symbol's LLR value may be considered an indicator of how reliably it has been detected.

[24] The full search here is meant in the context of finding the channel gain that minimizes a cost function designed based on the maximum likelihood criterion.

[25] In an evolutionary algorithm, there are individuals and generations. Each individual takes the form of a legitimate solution to the search problem. Individuals that are created at the same "round" or "iteration" belong to the same generation. The subsequent generations apart from updated individuals, who rely on the previous generations' individuals in order to take the form a better solution. After a number of generations the evolutionary algorithm stops and the best individual is the output of the algorithm.

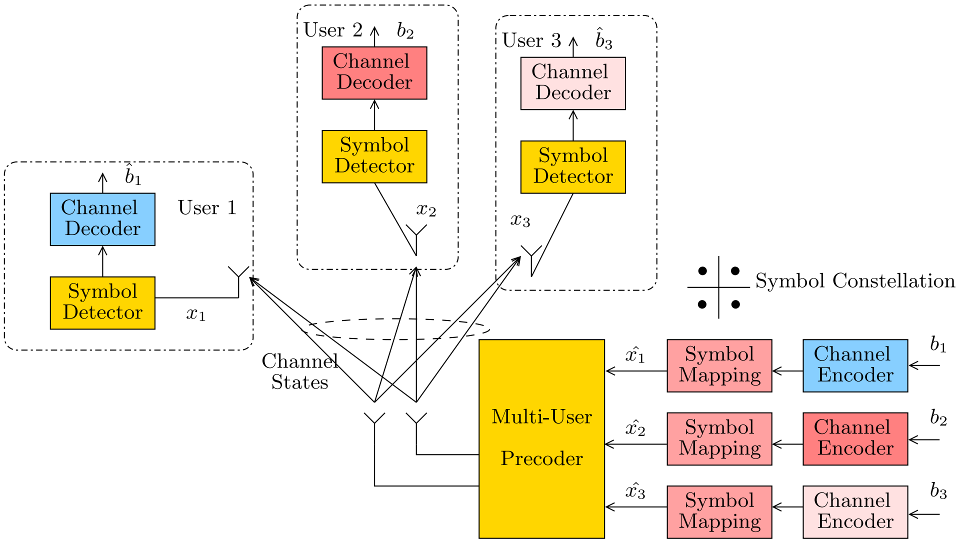


Fig. 18. The problem of Multi-User Transmission in the downlink of a multiple access system.

discrete-valued QRWBS employed for channel estimation and MUD, respectively, in the context of a joint channel estimation and MUD receiver was shown to outperform its classical counterpart [96].

C. Multi-User Transmission

1) The Problem: Let us now consider the dual counterpart of MUDs. In a nutshell, given the FD-CHTF of all users, the MUD detects the multi-user symbol vector. By contrast, the Multi-User Transmitter (MUT) relies on the FD-CHTF of all users signalled back to the BS. Explicitly, the multi-user symbol vector is "pre-distorted" by the MUT of the BS invoking the FD-CHTFs of all users for ensuring that after passing through the predicted channel each user receives a symbol-vector having the single non-interfered symbol destined for it. The duality of MUDs and MUTs was discussed for example by [97]. The substantial benefit is that a low-complexity single-user detector may be invoked by the mobile user terminal. This MUT principle is applicable both to OMA and NOMA systems. Hence in the downlink of a NOMA system, the base station may appropriately combine the different information symbols destined for the users supported and transmit a single multi-user signal, in order to increase the system throughput as depicted in Fig. 18 [5], [97]. It is up to each user then to detect and decode their own information upon the reception of the combined multi-user symbol vector. Since the user terminals do not have the same complexity capabilities as the base stations, the complex processing should be performed at the base station's side. Let us assume that the base station desires to transmit a multi-user symbol vector, where each entry of the vector corresponds to a different user. To elaborate a little further, the multi-user transmission problem is that given the symbol vector, as well as the system and channel characteristics, we should find a $(U \times N_t)$-element Transmit Pre-Coding (TPC) matrix $\mathbf{P}$, where U is the number of users and N_t the number of transmit antennas at the base station, in order to multiply with the information symbol vector as in

$$\mathbf{s} = \mathbf{P} \cdot \mathbf{x}, \tag{31}$$

1where $\mathbf{x}$ is the $(U \times 1)$-element multi-user vector and $\mathbf{s}$ is the transmitted $(N_t \times 1)$-element vector. Again, by doing so, when each user receives the composite multi-user symbol vector, they can detect and decode their own symbol by employing a low complexity single-user detector. Different criteria may be used for finding the optimal TPC matrix, such as the MMSE [98] or the Minimum Bit Error Ratio (MBER) [99] criteria.

2) The Classical Algorithms: Linear channel inversion algorithms, such as the ZF and the MMSE algorithms [98] perform adequately in underloaded or in full-rank systems, where the number of antennas at the base station is higher than the number of users supported. However, in challenging rank-deficient systems, where the number of users supported is higher than the number of antennas at the base station, more powerful non-linear algorithms should be used for performing the transmit precoding process.

In the 5G NOMA systems, the precoding matrix is expected to be calculated based on the distance between the users and the base stations, as well as on their channels' quality [5], [73], [74]. More specifically, assuming a two-user system, a higher power is allocated to the symbol of the user, who experiences the worse channel and higher losses. This way that user is able to detect and decode its own symbol, treating the other user's symbol as low-power interference. On the other hand, the user experiencing the better channel has received a signal with high multi-user interference, due to the worse user's symbol having been allocated a higher portion of the power. Therefore, the higher-power symbol is detected first, whilst treating the lower-power symbol as interference. Then the detected signal is remodulated and deducted from the composite signal, leaving the weaker signal behind. This is termed as Successive Interference Cancellation (SIC) and it has also been used as an MUD [100] as described in Section III-A.

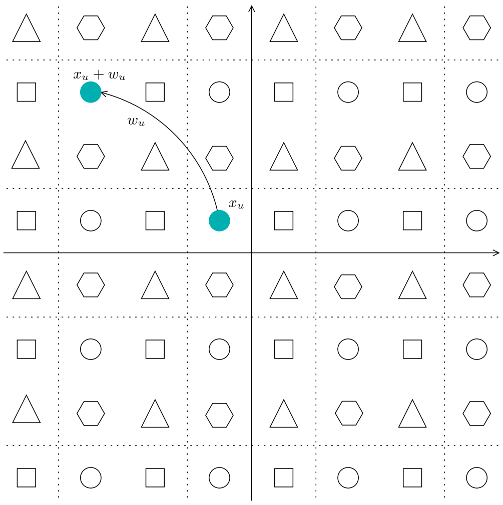


Fig. 19. The resultant legitimate constellation of each user layer, after applying a perturbation vector.

In [101], the vector perturbation precoding technique was proposed for the downlink of multiple access systems, where a vector $\mathbf{w}$ is added to the multi-user information symbol vector before it is transformed into a multi-antenna vector by multiplying it with the precoding matrix, as encapsulated in

$$\mathbf{s} = \mathbf{P} \cdot (\mathbf{x} + \mathbf{w}). \tag{32}$$

Given an already calculated precoding matrix $\mathbf{P}$, the goal of the perturbation vector is to minimize the required transmission power, while also minimizing the MMSE or the MBER criterion. If the average transmission power at the base station is constant, a scaling factor should be applied to the resultant symbol vector, since its power will depend on the selected perturbation vector. This scaling factor should be signalled to the receivers through a side channel. Since the perturbation vector is discrete-valued, it may be considered as shifting the whole symbol constellation an integer number of times in power as shown in Fig. 19. As an example in Fig. 19, the specific symbol x_u represented by the filled circle of the original QPSK constellation, which is the closest to the origin, would have been transmitted as the uth user's symbol, if no perturbation vector was applied. When that symbol is subjected to the perturbation $w_u = 1 + j$, the top left filled circle $(x_u + w_u)$ will be transmitted instead for the sake of minimizing the transmission power and the interference at the receiver. This operation is performed for each user's symbol, hence the jointly optimal perturbation vector should be found. A simple modulo operation on the perturbed symbol vector may recover the original symbol vector.

Therefore, using the above-mentioned scaling factor and a low-complexity modulo operation is sufficient at the users in order to map their received signals to the original constellation [101], [102]. The high-complexity part of this problem is to search for the optimal discrete-valued perturbation vector $\mathbf{w}$ of (32). Alternatively, one can immediately search for the optimal continuous-valued transmit vector $\mathbf{s}$ of (32).

A joint block diagonalization and vector perturbation multiple access downlink techinque was proposed in [103].

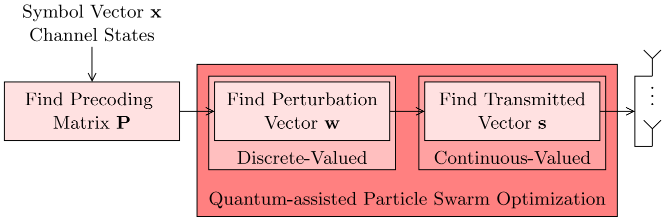

Symbol Vector **x**
Channel States
Find Precoding Matrix **P**
Find Perturbation Vector **w**
Discrete-Valued
Find Transmitted Vector **s**
Continuous-Valued
Quantum-assisted Particle Swarm Optimization

Fig. 20. The design methodology for the vector perturbation precoding for MUT.

Furthermore, Yao *et al.* employed a discrete-valued PSO algorithm for finding the perturbation vector that minimizes the MBER criterion in [104], while in [99] a continuous-valued PSO algorithm was proposed for further improving the output of the discrete-valued PSO algorithm. It should be noted that even though the perturbation vector is discrete-valued, the eventually transmitted signal vector is continuous-valued, therefore a continuous-valued fine tuning of the output of the discrete-valued PSO may reduce the system's BER even further. The system model of the vector perturbation precoding technique is shown in Fig. 20. After the precoding matrix is estimated based on the known symbol vector $\mathbf{x}$, the channel states and a selected criterion (such as the MMSE criterion), the optimal – with respect to a selected criterion – perturbation vector $\mathbf{w}$ is found using discrete-valued classical or quantum search. The found perturbation vector determines a transmitted vector $\mathbf{s}$. A continuous-valued classical or quantum search may be employed for further fine-tuning the resultant transmitted vector $\mathbf{s}$.

Masouros *et al.* [105] proposed a sphere search technique for reducing the complexity of searching for the optimal perturbation vector, with the objective of minimizing the transmission power of the base station. Masouros *et al.* [102] conceived a vector perturbation algorithm for improving the system's performance, when there is a finite-precision feedback of the scaling factor from the base station to the users, mainly due to the indispensible quantization prior to transmission. The vector perturbation precoding methodology was also employed in the downlink of Coordinated Multi-Point (CoMP) systems [106].

3) The Quantum Algorithms: In [107], the discrete-valued and continuous-valued Quantum-assisted Particle Swarm Optimization (QPSO) algorithms were proposed in the context of finding the optimal perturbation vector and the optimal transmitted vector, respectively, as depicted in Fig. 20. Both the discrete-valued and the continuous-valued QPSO algorithms combine the DH QSA with the classical PSO algorithm. The classical PSO algorithm creates a population of Z particles during each of the Ξ generations. Each particle is associated with a *position* and a *velocity*. The position refers to a legitimate input to the CF, or in other words, an entry in the database. The velocity describes the rate and the direction of the change of its position between two successive generations. During each generation of the classical PSO algorithm, the CF is evaluated for the positions of all particles in the specific generation. Their position and velocity calculated for the subsequent generation are updated based on their current position and velocity, as well as on the current generation's "best" particle's position and velocity.[26] Therefore, a full search of each generation's population has to be performed in order to find the best particle.

The QPSO algorithm employs the DH QSA for finding the best particle during each generation of both the discrete-valued and the continuous-valued QPSO algorithms. This way we are not only able to efficiently search for the best particle, but due to the trial-and-error nature of the DH QSA, only a subset of the original population is available to us. This procedure may be considered as selecting a few of the elite high-fitness particles for creating the population. As shown in [107], both the discrete-valued and continuous-valued QPSO algorithms outperform their classical counterparts for the same number of CF evaluations.

D. Multi-Objective Routing

1) The Problem: So far we have primarily focused our attention on network structures, where the transmission of the messages relies on a single hop, from the mobile users to the BS and vice versa. However, this is not always the case, since occasionally multihop communications are employed to reach remote nodes, which would otherwise be inaccessible [108]. These particular nodes have random locations and limited resources in terms of bandwidth and power and thus they rely on optimal routing for the sake of maximizing their performance. Optimal routing relies on a delicate balance amongst several *Quality of Service* (QoS) criteria apart from the ubiquitous BER performance, which was considered as the primary optimization objective in the majority of the previous applications. On one hand, mobile nodes rely on their batteries having for their communications with the rest of the network, bringing the optimization of their power consumption into the limelight as well [109]. This concept is commonly referred to as *"green" radio* [110]. On the other hand, the widespread use of lip-synchronized audio and video streaming resulted in considering both the delay and the achievable rate [111] as additional QoS criteria. Over the years several other metrics have been proposed such as the routing overhead [112], the control-channel cost [113] or the communication security [114]. Consequently, it becomes clear that routing optimization has to cater for multiple QoS criteria.

Most of the studies in the literature utilize single-component aggregate functions, which combine multiple QoS criteria. In this context, one of the most prominent optimization metrics is the network lifetime [115]. In fact, this specific metric encapsulates several optimization objectives [116], such as the power consumption, the nodes' battery levels and the route's delay. Additionally, the *Network Utility* (NU) also takes into account the routes' achievable rate [117], hence providing a more holistic perspective on the routing problem.

Despite the numerous single-objective approaches advocated in the literature, focusing on a single requirement may unduly degrade all the rest of the metrics. This problem may be mitigated [119] by using a multi-objective approach utilizing the concept of Pareto optimality[27] [120] for evaluating the fitness of multi-objective problems. Likewise, all the requirements considered may be optimized jointly without the need for user-defined parameters in order to aggregate the different design objectives [121]. In this way, we end up with a set of Pareto-optimal solutions, which cannot improve their individual objectives without degrading the rest. *Based on this approach, our ultimate goal is to identify the entire set of Pareto-optimal routes from a database of L routes, given a set of QoS requirements.* To elaborate further, an illustrative example is shown in Fig. 21, where a fully-connected *Heterogeneous Network* (HetNet) [118] is portrayed. In this specific scenario, the *Source Node* (SN) has to transmit its message to the *Destination Node* (DN) through a cloud of heterogeneous mobile *Relay Nodes* (RN). Note that the DN acts as a cluster head and has access to a quantum computer for employing quantum-assisted routing optimization. This specific topology has been studied in [65], [66], [122], and [123], where the following *Utility Vector* (UV) $\mathbf{f}(x)$ has been utilized:

$$\mathbf{f}(x) = [P_e(x), D(x), P_L(x)]. \tag{33}$$

Observe in Eq. (33) that the routes' end-to-end BER $P_e(x)$, their end-to-end delay $D(x)$ and their total power dissipation $P_L(x)$ are jointly minimized under the Pareto optimality principle. This process involves a complexity on the order of $O(L^2)$ [65], when using exhaustive search. However, the total number L of routes increases exponentially with the number of nodes [124], as we can observe in Fig. 22, hence rendering the problem NP-hard. Consequently, sophisticated methods are required for addressing the multi-objective routing problem.

2) The Classical Algorithms: A plethora of single-objective studies exist in [110], [116], [117], and [125]–[131], each addressing different routing aspects. In a nutshell, these specific studies consider the optimization objectives in a single-component aggregate function in an attempt to optimize the latter using either a heuristic or a formal systematic optimization method. To elaborate further, several of these studies [110], [125]–[127] utilize Dijkstra's algorithm [132] for the sake of identifying the optimal routes. Explicitly, this technique is capable of approaching the optimal routes at the cost of imposing a complexity on the order of $O(E^3)$, where E corresponds to the number of edges in the network's graph. For instance, Zuo *et al.* [126] employed this specific algorithm for optimizing the route's energy efficiency in the context of wireless ad-hoc networks. Hu *et al.* [125] utilized Dijkstra's algorithm for minimizing both the power consumption and the delay, quantified in terms of the number of hops, in socially-aware networks. Additionally, Dehghan *et al.* [127] adapted this specific algorithm to the problem of cooperative routing and attempted to maximize the route's energy efficiency.

[26] Here, by "best" particle we mean the particle in the current population, whose position yields the minimum CF value.

[27] In multi-objective routing, each route is now associated with a *Utility Vector* (UV) $\mathbf{f}(x) = [f_1(x), \ldots, f_n(x)]$, where $f_i(x)$ corresponds to the i-th optimization objective out of n objectives in total. For minimization (maximization) problems, a specific route is dominates another if all of its objectives are strictly lower than (greater than) the respective objectives of the second route. Hence, a route is then considered as Pareto-optimal if there exist no other routes dominating it.

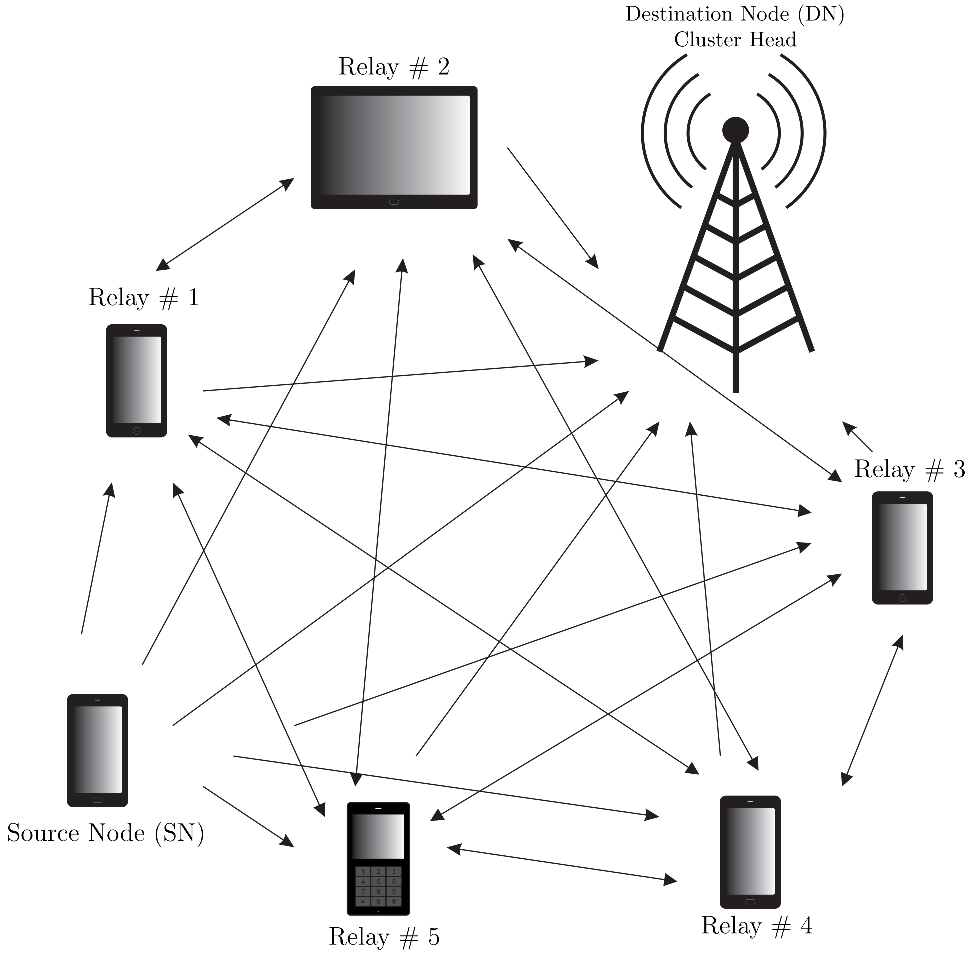


Fig. 21. Exemplified topology for routing optimization in a *Heterogeneous Network* (HetNet) [118].

The beneficial properties of *convex optimization* [133] have also been exploited in the context of routing optimization. To elaborate further, Dall'Anese and Giannakis [128] transformed the non-convex routing problem of cognitive random access networks into a convex one using successive convex approximations for the sake of minimizing both the routes' *Packet Loss Ratio* (PLR) and the resultant outage probability. Additionally, Yetgin *et al.* [129] maximized the network lifetime in the context of *Wireless Sensor Networks* (WSN) using a similar approach. Based on this specific metric, Abdulla *et al.* [130] have maximized the lifetime of WSNs by introducing a range of Hybrid Multihop Network (HYMN) parameters. The so-called *Network Utility* [131] also constitutes a meritorious single-component optimization.

The employment of Pareto optimality comes at the cost of increased complexity and thus primarily heuristic evolutionary methods have been employed for the sake of making the problem tractable. In fact, there are some comprehensive studies in [124] and [135]–[138], each investigating networks from a diverse perspective using the multi-objective approach, while relying on evolutionary algorithms. For instance, both the Non-dominated Sorting Genetic Algorithm II (NSGA-II) and the Multiobjective Differential Evolution Algorithm (MODE) have been invoked in [124] for optimizing their end-to-end delay and power dissipation of transmission routes established in WSNs. Additionally, the NSGA-II has been employed in [135] for satisfying the same QoS requirements in context both of the ubiquitous Voice over Internet Protocol (VoIP) and for file transfer in WSNs. Moreover, Perez *et al.* [136] minimization of the WSN's deployment cost by using a multi-objective model for optimizing both the total energy

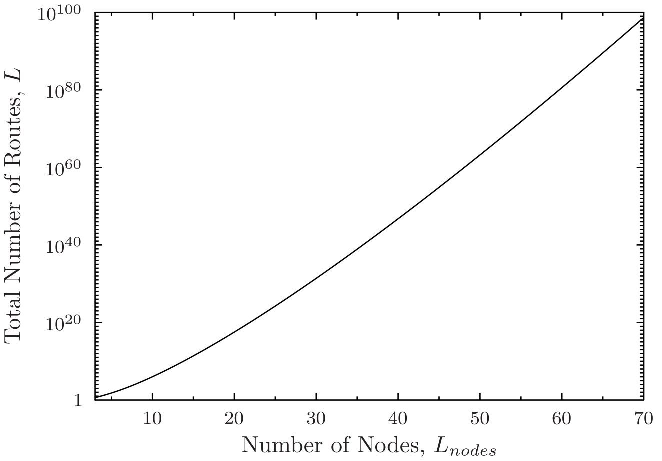


Fig. 22. Total number L of Hamiltonian routes as a function of the number L_{nodes} of nodes of a HetNet.

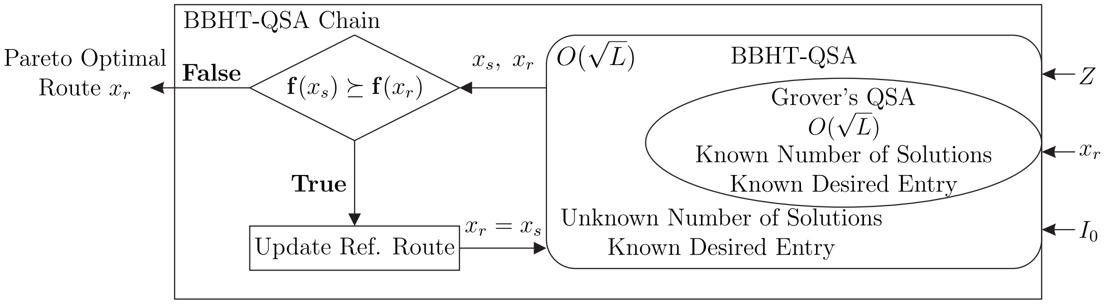


Fig. 23. The *BBHT-QSA chain* process used in [65], [66], [122], and [134] for identifying a single Pareto-optimal route.

dissipation and the number of deployed sensor nodes in WSNs. Martins *et al.* [137] employed a hybrid multi-objective evolutionary algorithm for solving the Dynamic Coverage and Connectivity Problem (DCCP) of WSNs subjected to node failures. Additionally, Pinto and Barán [138] introduced the concept of Pareto Optimality in the ubiquitous single-objective ACO and proposed the so-called *Multiobjective Max-Min Ant System* (MMAS) for solving the multi-objective mutlicast routing problem.

3) The Quantum Algorithms: The application of the aforementioned multi-objective heuristics results in reduced performance due to their tendency to convergence to local optima [65]. Fortunately, quantum computing provides a powerful framework for addressing the multi-objective routing problem by exploiting the complexity reduction offered by the QP, while guaranteeing a near-full-search-based accuracy. In fact, several quantum-assisted treatises have been disseminated in [65], [66], [122], and [134] in the context of the multi-objective routing problem.

To the best of our knowledge, the first ever quantum-assisted multi-objective approach to the routing problem is the so-called *Non-dominated Quantum Optimization* (NDQO) algorithm [65]. This specific algorithm extended the DH QSA of Section II-B8 for solving the Pareto optimality problem for the sake of successively approaching the Pareto-optimal routes at a reduced complexity. Assuming a database of L routes in total, the NDQO algorithm succeeds in identifying the entire set of Pareto-optimal routes at a complexity on the order of $O(L\sqrt{L})$, while exhibiting near-optimal routing performance by exploiting the probabilistic nature of the BBHT QSA. In a nutshell, the NDQO algorithm invokes the BBHT QSA to conclude as to whether a reference route is optimal by searching for routes that dominate this specific route.

This process is referred to as a *BBHT-QSA chain* in [65] and its sub-processes are highlighted in Fig. 23. The BBHT-chain's input parameters are shown at the right-hand-side, namely the nodes' geo-locations Z, the initial reference route x_r and the nodes' interference power levels I_0. Initially, the BBHT QSA is invoked for searching for routes that dominate the reference route x_r. The output of this process is the route x_s, which is checked as to whether it dominates x_r. This is denoted by the condition $\mathbf{f}(x_s) \succeq \mathbf{f}(x_r)$, where the operator $\succeq$ corresponds to the Pareto dominance comparison operator. If the referece route x_r is dominated by x_s, x_r is then set equal to x_s and a new BBHT QSA is invoked with the updated reference route value. This process is repeated until the BBHT QSA outputs a route that does not dominate its reference route, thus ensuring that the current reference route is indeed Pareto-optimal in the absence of dominant routes.

Since the BBHT QSA exhibits a $\sim$100% probability of correctly detecting a solution as detailed in Section II-B7, some sub-optimal routes may be erroneously classified as being Pareto-optimal due to BBHT QSA's inability to guarantee 100% probability of correctly detecting a route that dominates the reference route. Therefore, the NDQO algorithm exhibits a modest error floor owing the low-probability inclusion of sub-optimal routes into the set of Pareto-optimal routes. Its error floor has been mitigated by its successor, namely the so-called *Non-dominated Quantum Iterative Optimization* (NDQIO) algorithm [66], where a repair process guaranteeing the identification of only true Pareto-optimal routes has been proposed. The NDQIO algorithm succeeds in further reducing the complexity imposed, which is quantified on the order of $O(L_{\text{OPF}}\sqrt{L})$, with L_{OPF} corresponding to the number of Pareto-optimal routes, while reducing the associated performance error floor to infinitesimally low levels.

An additional source of complexity reduction, namely that of the database correlation exploitation, has been combined with the quantum parallelism for the sake of further complexity reduction. Explicitly, it has been confirmed by Zalka [61] that Grover's QSA and its variants are optimal in terms of the number of database queries in uncorrelated databases. Therefore, database correlation exploitation would significantly increase the efficiency of quantum parallelism. In this context, the so-called *Multi-Objective Decomposition Quantum Optimization* (MODQO) algorithm [134] has been proposed for multi-objective routing in *socially-aware networks* [125]. Note that the topology considered in [134] is different from that of Fig. 21, since multiple pairs of SNs and DNs are considered. In this scenario, the MODQO algorithm exploited the specific property that the Pareto-optimal route combinations are constituted by individual Pareto-optimal routes. Therefore, by exploiting this observation, the search space has been partitioned into several less correlated databases, where the quantum parallelism framework proposed in [66] can be more efficiently exploited. As for its complexity, the MODQO algorithm succeeds in identifying the entire set of Pareto-optimal route combinations at a complexity, which is on the orders of $O(\sqrt{L})$ and $O(L_{MR}\sqrt{L} + L_{MR}^{2L_{MC}})$ for the best- and worst-case scenarios, respectively, where L_{MR} and L_{MC} correspond to the number mesh routers and clients, respectively. Note that the classical exhaustive search would impose a complexity on the order of $O(L^{L_{MC}})$, where we have $O(L) \gg O(L_{MR})$, hence rendering the problem unsolvable in polynomial time.

Apart from the exploiting the correlations in the formation of Pareto-optimal route combinations, the potential correlations in the formation of Pareto-optimal routes has been investigated in [122] and [123]. To elaborate further, it has been proven in [122] that Pareto-optimal routes exclusively consist of Pareto-optimal sub-routes. Based on this observation, the so-called *Evolutionary Quantum Pareto Optimization* (EQPO) algorithm [122] and an *irregular trellis graph* [139] has been proposed for the sake of guiding the search, hence effectively transforming the search space into a series of weakly correlated databases with the aid of dynamic programming [140], [141]. A quantum-assisted feed-forward process resembling the ubiquitous Viterbi algorithm [142] is then invoked for the sake of identifying the Pareto-optimal routes by processing the trellis-stages. More specifically, the NDQIO algorithm is activated for each trellis-stage to identify the respective Pareto-optimal routes. The EQPO algorithm succeeds in identifying 99.9% of the set Pareto-optimal routes at a complexity order of $O(L_{opt}^{3/2} L_{nodes}^2)$, while exhibiting a performance associated with a low heuristic error floor. Therefore, since the total number L of routes has an exponential relationship with respect to the number L_{nodes} of nodes, as seen in Fig. 22, a substantial complexity reduction is achieved compared to full-search-based NDQO and NDQIO algorithms.

Apart from the aforementioned treatises, which primarily rely on Grover's operator and thus harnessing the power of quantum parallelism, some others exploit the beneficial complexity reduction offered by the *quantum tunneling* effect [16]. Explicitly, the particular quantum algorithms relying on quantum tunneling are referred to as *quantum annealers* [143], [144]. More specifically, a quantum annealer may be treated as a sampler, which approximates the global optimum of a function or of a database with the aid of quantum tunneling. In the context of multi-objective routing, Wang *et al.* [145] proposed a quantum annealing algorithm designed for optimizing the scheduling of the wireless links in interference-limited networks. The proposed quantum annealing algorithm succeeded in jointly optimizing both the network's throughput as well as its interference, whilst imposing a substantially lower complexity than its classical counterpart, namely the simulated annealing algorithm.

E. Breaking Public-Key Cryptography Schemes

1) The Problem: Public-key cryptosystems, such as the RSA [146], named after its creators Rivest, Shamir and Adleman, encrypt data using a public key, which may be eavesdropped by anyone, and they decrypt data using a private key. Node A randomly picks two large prime numbers. Based on these two prime numbers, a public key and a private key are generated. The public key can be used by any other node for encrypting their data and transmitting it back to the node A. However, only node A has the private key, which is the only key that can be used for correctly decrypting the received data. Please note that none of the transmitting nodes should be able to decrypt the data they encrypted themselves. The same applies to any potential eavesdroppers, who have obtained both the public key and the encrypted messages from the transmitting nodes. This means that no processing of the public key should lead to any information concerning the private key. However, due to the process invoked for creating the public and the private keys, if the two prime numbers, which were used for creating the keys are obtained by an eavesdropper, the private key can be replicated and the information messages can be decrypted. This is termed as the RSA problem, which reduces to the following factorization problem. Given a large number N, we have to find its two prime factors.

Even though it would be beneficial if a solution did not exist to the RSA problem, creating algorithms that are able to break a cryptosystem inevitably provides insights for constructing post-quantum cryptosystems.

2) The Classical Algorithms: Integer factorization techniques may be used for finding the prime factors of an integer. The most efficient classical algorithm of solving an integer factorization problem is the *quadratic sieve* [147], when the number to be factored is less than 332 bits long. For higher numbers, the *general number field sieve* [147] outperforms all other classical algorithms, but it imposes a high computational complexity.

3) The Quantum Algorithms: Shor's algorithm [33] can be used for efficiently solving the RSA problem. As discussed in Section II-B4, Shor's algorithm employs a classical subroutine, which resembles the operation of the quadratic sieve, while the QPEA [48] of Section II-B5 is used for finding the necessary period of the function employed. Shor's algorithm achieves an exponential speed-up, over the general number field sieve, as a benefit of the inherent parallelism of quantum computing. In 2012, the number 21 was factored to its prime factors 3 and 7 using Shor's algorithm [148].

F. Indoor Localization

1) The Problem: The problem of indoor localization is to estimate the position of a user in a room, based on the user's transmit or received signals [149]. More precisely, the signals' Received Signal Strength Indicator (RSSI), Time of Arrival (ToA), Angle of Arrival (AoA), or Time Difference of Arrival (TDoA) may be exploited for estimating the user's location [150]. The localization's accuracy is enhanced, when the floor plan of the room is known. The localization problem is illustrated in Fig. 24.

Due to the paradigm shift to mm-Wave communications [151]–[153], *pencil* beams may be formed in order to minimize the multi-user interference and to increase the data rate [154]. In order to use very thin beams, accurate user localization is necessary.

Accurate localization may also be used for tracking the movement of a user in a room. Visible Light Communication (VLC) systems [155]–[157] may exploit accurate localization, since they will be able to form more accurate clusters of access points for serving the users supported by

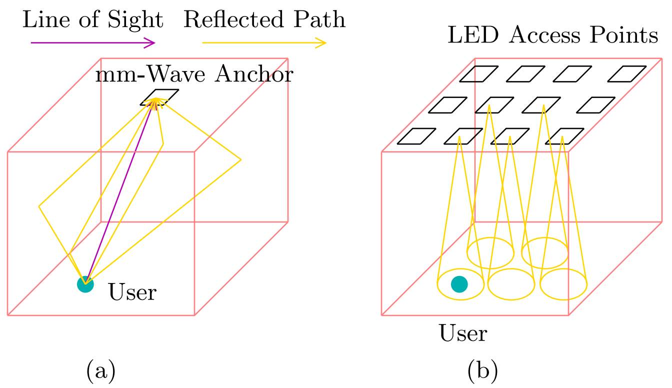


Fig. 24. The indoors localization problem, where an accurate position of the user has to be estimated. (a) Uplink localization, where a mm-Wave anchor processes the received line of sight path, as well as the reflected paths. Based on the RSSI, the ToA and the AoA, the mm-Wave anchor may initially reduce the search space. Then, it may employ the fingerprinting methodology for comparing the received signals to those stored in a pre-calculated database. (b) Downlink localization using a VLC system, where each LED panel is switched on and off sequentially. The RSSI at the user by each LED access point is compared to a pre-calculated database, following the fingerprinting methodology. Quantum search may be employed for searching in the databases in both the downlink and the uplink localization methods.

the system. More specifically, since multiple Light Emitting Diodes (LED) will be installed in a room, the accurate localization of users may support efficient spatial MIMO techniques for increasing the data rate of the downlink. Accurate tracking of the user's movement would help the system maintain the throughput attained.

2) The Classical Algorithms: Ultra WideBand (UWB) systems may also be employed for achieving accurate localization [149], [158]–[164] by exploiting the signals' inherently short symbol duration and the ToA of its Line Of Sight (LOS) component. If the floor plan of the room is known, the Multi-Path Components (MPC) of the signal's PDP may also be exploited for increasing the accuracy of the localization [158], [163], [164]. More specifically, the TOA of the LOS path and of the MPCs may be jointly processed in order to extract a small subset of legitimate areas in the room, where the user may be located, as exemplified in Fig. 24.

VLC-based localization has also been employed, by exploiting the limited coverage of the VLC access point [155], [165]. Based on the fingerprinting approach [166], the room may be partitioned into small virtual tiles. The localization algorithm has to determine the center of which specific tile the user is closest to. This is performed by building a database of the potentially received signals' RSSIs, ToAs, AoAs and TDoAs from each legitimate tile. A suitable CF which would compare the actual received signals to the saved ones at the known tile-centre positions would determine, which tile is closest to the supported user. Hence, the localization problem may be reduced to a search problem. The size of the search space depends on the size of each tile. The smaller the dimensions of a tile are, the more accurate the localization will be, but more tiles exist in the database. Therefore, there is a trade-off between the performance attained and the complexity imposed.

The triangulation method [166] combines the signals of three different access points by estimating the distance between them and the user based on their RSSI and then estimating the location of the user to be at the intersection of the three circles. When operating in a system, where the Signal to Noise Ratio (SNR) is low, using the triangulation method based on the RSSI may lead to inaccurate localization. The Global Positioning System (GPS) uses the triangulation method for localization.

3) The Quantum Algorithms: The DH QSA was combined with classical processing for performing indoor localization in the VLC downlink and in the mm-Wave uplink [167]. The fingerprinting approach is used in both systems. In the mm-Wave uplink , multiple antennas may be used at the access point for estimating the AoA. Based on the AoA and the ToA of the LOS and multipath signals, the initial search space may be reduced to a subset of surviving tiles, similarly to [158]. The DH QSA is then employed in the resultant database of CF values, in order to find the particular entry that minimizes the CF. In this problem, the CF takes into account the signal received at all antennas of the access point over the LOS path, as well as over all MPCs, and determines the square distance from the corresponding values associated with the center of each tile.

The fingerprinting approach is also used in the VLC downlink in [167]. Similarly to [155], the signal strength of each access points is measured and stored in a database, which corresponds to a specific tile's center. Therefore, if there are 64 access points and 90 tiles in the room, there are 90 databases with 64 entries each. The entries of each database are then combined and compared to the actual 64 received values at the user's true position and the search problem reduces to that of finding which of the 90 tiles offers the most similar RSSI from all access points to the actually received ones. The DH QSA was employed for offering a quadratic reduction in the associated computational complexity compared to a full search. Similarly, by appropriately reducing the size of each tile in order to increase the search space so that the DH QSA in the larger database requires the same complexity as a full search in a smaller database, a higher localization accuracy may be achieved.

In the uplink and downlink localization problems, the quantum-assisted solutions of [167] achieved an equivalent performance to the optimal classical methods, while requiring a lower computational complexity.

G. Big-Data Analysis

1) The Problem: In big-data systems, multiple-feature data has to be accessed and manipulated. Examples of problems existing in big-data systems involve classification of the high-dimensional data based on their features, search problems and existence problems [168].

In the classification problem [169], the entries of a database have to be classified into multiple classes, based on their features' values. The classification problem may be divided into two parts: a) the *supervised classification* problem, where a set of already classified data exists and can be exploited for aiding the classification of the rest of the data, and b) the *unsupervised classification* problem, where all entries have to be classified.

In a search problem, the index of the entry in a large unsorted database has to be found. Furthermore, the existence problem investigates whether there exists a specific entry in a database or not.

2) The Classical Algorithms: Classical machine learning [169], [170] can be used for solving both unsupervised and supervised classification problems [171]. Support Vector Machines (SVM) [172] may be employed for performing either supervised or the so-called *semi-supervised* classification [173]. They construct a model based on the classified training data for accurately predicting the class that new data should be classified into.

Both the search problem and the existence problem encountered in unstructured high-volume databases can be classically solved by a full search, which however often imposes an excessively high complexity.

3) The Quantum Algorithms: In [174] a Quantum Support Vector Machine (QSVM) was proposed for performing supervised classification in large databases. The QSVM imposes an exponentially lower complexity than its classical counterparts, when the latter are able to classify the same dataset in polynomial time. To elaborate further, the QSVM reformulates the classical SVM originally proposed in [175]. Explicitly, this reformulation transforms the SVM's quadratic formulation into a system of linear equations, which are in turn solved by using the HHL algorithm [54] of Section II-B12.

Grover's QSA [28] of Section II-B6 can be employed for searching through an unstructured database, whilst achieving a quadratic speed-up compared to the classical full search. When the exact position of the desired entry is not required, only the knowledge of whether that entry exists in the database or not is wanted, the Quantum Existence Testing (QET) algorithm of [9] and [176] may be used instead. The QET algorithm employs the QCA of Section II-B9, which finds the number of times a desired entry appears in a database. Since in the context of the existence problem we are not interested in finding the specific number of times a value appears in a database, but rather *if* it exists at all or not, the QET algorithm uses fewer qubits in the control register of the QCA of Fig. 12. This way, even though a precise estimate of the number of solutions in a database cannot be obtained the measured control qubits are non-zero, we are informed that there are indeed any solutions in the database. When carrying out this task, the QET algorithm imposes a lower complexity than the QCA, which in indicates a quadratic speed-up over the full search.

IV. Open Problems

A suite of quantum solutions have been proposed for classical wireless problems. Nevertheless, there are numerous open problems in both the physical and network layers of wireless communications systems that may benefit from the power quantum computing. For example, Coordinated Multi-Point [177], also referred to as cooperative network MIMO, is a compelling solution to the problem of degraded user performance at the cell edge. Based on CoMP, a user will be simultaneously connected to multiple base stations, which essentially treat interference as useful information. Quantum search algorithms [28], [31], [32] may be used in the context of CoMP for detecting and processing the excessive amount of information, since the notion of interference will have been eliminated.

Quantum computing may also be used for improving the routing performance of drone communications and networks [180], [181], given their limited battery lifespan and mission-critical nature. For instance, optimal routes may be found in drone networks using quantum algorithms, or when drones are used as emergency base stations, optimal drone placement planning may be performed by solving the associated optimization problem.

The multi-objective quantum computing framework constituted by the algorithms of Section III-D could be employed for addressing the problem of *proactive caching* [125], [182]–[184]. Explicitly, in proactive caching the packets are buffered in the nodes by carefully considering their popularity for the sake of reducing both the delay and the power consumption, which is reminiscent of the multi-objective routing problem. Additionally, this specific case study could be undertaken with the aid of *machine learning* [185]. In fact, Kapoor *et al.* [187] have recently proposed a model for quantum perceptrons, which may constitute beneficial building blocks for quantum-aided neural networks. Therefore, it would be worth investigating as to whether quantum-assisted solutions can be adopted in this context.

In addition to the above-mentioned open problems, novel quantum solutions may be explored in the specific wireless communication problems discussed in this contribution. For example, Hogg's heuristic quantum search algorithm [51], [52] may be employed in any database search, where there exists correlation between the database entries, in order to reduce the required search time. In the uplink multi-user detection problem, the constructed database includes the MSE between the actually received signal and a hypothetical noiseless received signal that is based on a legitimate symbol combination. Since there are different symbol combinations that partially consist of the same symbols, there is correlation in the constructed database. Therefore, Hogg's heuristic quantum search algorithm may further decrease the search complexity imposed.

V. Conclusion

In this contribution, we have surveyed the family of quantum algorithms that have been employed for solving realistic problems in wireless communications faster and more accurately than the available classical solutions. In Section II-A we have stated the basic characteristics of quantum computing with the aid of linear algebra and logical gates, reminiscent of classical computing. Familiarity with the basics of quantum computing was then exploited for highlighting the quantum circuits of major quantum algorithms that have been proposed. We have gathered the investigated quantum algorithms in Tables III and IV, where we briefly state their application and description.

Having acquired a feel for the capabilities of quantum computing via the quantum algorithms presented, in Section III, we have shifted the focus of our attention to classical wireless optimization problems. We have opted for discussing each of the optimization problems, as well as their state-of-the-art classical solutions. By comparing the presented quantum-assisted solutions to their classical counterparts, we have argued that for a specific complexity budget, a performance gain is observed when the quantum algorithms are used. Similarly, by employing the quantum algorithms, a specific performance target may be reached at a lower computational complexity.

Acknowledgment

The use of the IRIDIS High Performance Computing Facility at the University of Southampton is also acknowledged.

References

[1] L. Hanzo *et al.*, "Wireless myths, realities, and futures: From 3G/4G to optical and quantum wireless," *Proc. IEEE*, vol. 100, pp. 1853–1888, May 2012.

[2] H. Ji *et al.*, "Introduction to ultra reliable and low latency communications in 5G," *CoRR*, vol. abs/1704.05565, 2017.

[3] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for smart cities," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 22–32, Feb. 2014.

[4] G. Wunder *et al.*, "5GNOW: Non-orthogonal, asynchronous waveforms for future mobile applications," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 97–105, Feb. 2014.

[5] Y. Saito *et al.*, "Non-orthogonal multiple access (NOMA) for cellular future radio access," in *Proc. IEEE Veh. Technol. Conf. (VTC Spring)*, Jun. 2013, pp. 1–5.

[6] L. Hanzo, Y. Akhtman, M. Jiang, and L. Wang, *MIMO-OFDM for LTE, WIFI and WIMAX: Coherent Versus Non-Coherent and Cooperative Turbo-Transceivers*. Hoboken, NJ, USA: Wiley, 2010.

[7] C. She, C. Yang, and T. Q. S. Quek, "Radio resource management for ultra-reliable and low-latency communications," *IEEE Commun. Mag.*, vol. 55, no. 6, pp. 72–78, Jun. 2017.

[8] N. Kato *et al.*, "The deep learning vision for heterogeneous network traffic control: Proposal, challenges, and future perspective," *IEEE Wireless Commun.*, vol. 24, no. 3, pp. 146–153, Jun. 2017.

[9] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, 10th ed. New York, NY, USA: Cambridge Univ. Press, 2011.

[10] S. Imre and F. Balázs, *Quantum Computing and Communications: An Engineering Approach*. Chichester, U.K.: Wiley, 2005.

[11] S. Imre and L. Gyongyosi, *Advanced Quantum Communications: An Engineering Approach*. Hoboken, NJ, USA: Wiley, 2013.

[12] R. J. Lipton and K. W. Regan, *Quantum Algorithms via Linear Algebra: A Primer*. Cambridge, MA, USA: MIT Press, 2014.

[13] M. M. Waldrop, "The chips are down for Moore's law," *Nat. News*, vol. 530, no. 7589, pp. 144–147, 2016.

[14] S. Boixo, T. Albash, F. M. Spedalieri, N. Chancellor, and D. A. Lidar, "Experimental signature of programmable quantum annealing," *Nat. Commun.*, vol. 4, p. 2067, Jun. 2013.

[15] M. W. Johnson *et al.*, "Quantum annealing with manufactured spins," *Nature*, vol. 473, no. 7346, pp. 194–198, 2011.

[16] S. Boixo *et al.*, "Evidence for quantum annealing with more than one hundred qubits," *Nat. Phys.*, vol. 10, no. 3, pp. 218–224, 2014.

[17] Z. Babar, S. X. Ng, and L. Hanzo, "Near-capacity code design for entanglement-assisted classical communication over quantum depolarizing channels," *IEEE Trans. Commun.*, vol. 61, no. 12, pp. 4801–4807, Dec. 2013.

[18] Z. Babar, S. Ng, and L. Hanzo, "EXIT-chart-aided near-capacity quantum turbo code design," *IEEE Trans. Veh. Technol.*, vol. 64, no. 3, pp. 866–875, Mar. 2015.

[19] Z. Babar, P. Botsinis, D. Alanis, S. X. Ng, and L. Hanzo, "The road from classical to quantum codes: A hashing bound approaching design procedure," *IEEE Access*, vol. 3, pp. 146–176, 2015.

[20] Z. Babar, P. Botsinis, D. Alanis, S. Ng, and L. Hanzo, "Fifteen years of quantum LDPC coding and improved decoding strategies," *IEEE Access*, vol. 3, pp. 2492–2519, 2015.

[21] Z. Babar *et al.*, "Fully-parallel quantum turbo decoder," *IEEE Access*, vol. 4, pp. 6073–6085, 2016.

[22] P. Botsinis *et al.*, "Quantum error correction protects quantum search algorithms against decoherence," *Nat. Sci. Rep.*, vol. 6, Aug. 2016, Art. no. 38095.

[23] P. A. M. Dirac, *The Principles of Quantum Mechanics*, 4th ed. Oxford, MS, USA: Oxford Univ. Press, Feb. 1982.

[24] C. P. Williams, "Quantum search algorithms in science and engineering," *Comput. Sci. Eng.*, vol. 3, no. 2, pp. 44–51, Mar./Apr. 2001.

[25] M. Santha, *Quantum Walk Based Search Algorithms*. Heidelberg, Germany: Springer, 2008, pp. 31–46.

[26] A. M. Childs and W. van Dam, "Quantum algorithms for algebraic problems," *Rev. Mod. Phys.*, vol. 82, pp. 1–52, Jan. 2010.

[27] M. Mosca, *Quantum Algorithms*. New York, NY, USA: Springer, 2012, pp. 2303–2333.

[28] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proc. 28th Annu. ACM Symp. Theory Comput.*, May 1996, pp. 212–219.

[29] L. K. Grover, "Quantum mechanics helps in searching for a needle in a haystack," *Phys. Rev. Lett.*, vol. 79, no. 2, pp. 325–328, Jul. 1997.

[30] S. Jordan. (2011). *Quantum Algorithm Zoo*. [Online]. Available: http://math.nist.gov/quantum/zoo/

[31] M. Boyer, G. Brassard, P. Høyer, and A. Tapp, "Tight bounds on quantum searching," *Fortschritte der Physik*, vol. 46, nos. 4–5, pp. 493–506, 1998.

[32] C. Dürr and P. Høyer, "A quantum algorithm for finding the minimum," *eprint arXiv:quant-ph/9607014*, Jul. 1996.

[33] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. 35th Annu. Symp. Found. Comput. Sci.*, Nov. 1994, pp. 124–134.

[34] G. Brassard, P. Hoyer, and A. Tapp, "Quantum counting," *eprint arXiv:quant-ph/9805082*, May 1998.

[35] H. Wimmel, *Quantum Physics & Observed Reality: A Critical Interpretation of Quantum Mechanics*. Singapore, World Sci., 1992.

[36] J. S. Bell, "On the problem of hidden variables in quantum mechanics," *Rev. Mod. Phys.*, vol. 38, pp. 447–452, Jul. 1966.

[37] N. Chandra and R. Ghosh, *Quantum Entanglement in Electron Optics: Generation, Characterization, and Applications*. Heidelberg, Germany: Springer, 2013.

[38] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, pp. 145–195, Jan. 2002.

[39] V. Scarani *et al.*, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, pp. 1301–1350, Jul. 2009.

[40] R. Hughes and J. Nordholt, "Refining quantum cryptography," *Science*, vol. 333, no. 6049, pp. 1584–1586, 2011.

[41] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, pp. 802–803, Oct. 1982.

[42] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput. Syst. Signal Process.*, 1984, pp. 175–179.

[43] R. P. Feynman, "Simulating physics with computers," *Int. J. Theor. Phys.*, vol. 21, nos. 6–7, pp. 467–488, Jun. 1982.

[44] P. Benioff, "Quantum mechanical Hamiltonian models of turing machines," *J. Stat. Phys.*, vol. 29, no. 3, pp. 515–546, 1982.

[45] D. Deutsch, "Quantum theory, the church-turing principle and the universal quantum computer," in *Proc. Roy. Soc. London A Math. Phys. Sci.*, vol. 400, no. 1818, pp. 97–117, 1985.

[46] D. Deutsch and R. Jozsa, "Rapid solution of problems by quantum computation," *Proc. Roy. Soc. A Math. Phys. Sci.*, vol. 439, no. 1907, pp. 553–558, Dec. 1992.

[47] D. R. Simon, "On the power of quantum computation," *SIAM J. Comput.*, vol. 26, no. 5, pp. 1474–1483, 1997.

[48] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca, "Quantum algorithms revisited," *Proc. Roy. Soc. London A*, vol. 454, pp. 339–357, Jan. 1998.

[49] D. S. Abrams and S. Lloyd, "Quantum algorithm providing exponential speed increase for finding eigenvalues and eigenvectors," *Phys. Rev. Lett.*, vol. 83, no. 24, pp. 5162–5165, Dec. 1999.

[50] G. Brassard, P. Høyer, M. Mosca, and A. Tapp, "Quantum amplitude amplification and estimation," *eprint arXiv:quant-ph/0005055*, May 2000.

[51] T. Hogg, "Quantum search heuristics," *Phys. Rev. A*, vol. 61, Apr. 2000, Art. no. 052311.

[52] T. Hogg and D. Portnov, "Quantum optimization," *Inf. Sci.*, vol. 128, nos. 3–4, pp. 181–197, 2000.

[53] A. Malossini, E. Blanzieri, and T. Calarco, "Quantum genetic optimization," *IEEE Trans. Evol. Comput.*, vol. 12, no. 2, pp. 231–241, Apr. 2008.

[54] A. W. Harrow, A. Hassidim, and S. Lloyd, "Quantum algorithm for linear systems of equations," *Phys. Rev. Lett.*, vol. 103, no. 15, Oct. 2009, Art. no. 150502.

[55] G. Brassard, F. Dupuis, S. Gambs, and A. Tapp, "An optimal quantum algorithm to approximate the mean and its application for approximating the median of a set of points over an arbitrary distance," *eprint arXiv:quant-ph/1106.4267v1*, Jun. 2011.

[56] P. Botsinis, S. X. Ng, and L. Hanzo, "Quantum search algorithms, quantum wireless, and a low-complexity maximum likelihood iterative quantum multi-user detector design," *IEEE Access*, vol. 1, pp. 94–122, 2013.

[57] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM J. Comput.*, vol. 26, no. 5, pp. 1484–1509, 1997.

[58] C. Pomerance, "A tale of two sieves," *Notices Amer. Math. Soc*, vol. 43, pp. 1473–1485, Dec. 1996.

[59] J. Chiaverini *et al.*, "Implementation of the semiclassical quantum Fourier transform in a scalable system," *Science*, vol. 308, no. 5724, pp. 997–1000, 2005.

[60] D. E. Knuth, *The Art of Computer Programming, Volume 3: Sorting and Searching*, 2nd ed. Redwood City, CA, USA: Addison-Wesley, 1998.

[61] C. Zalka, "Grover's quantum searching algorithm is optimal," *Phys. Rev. A*, vol. 60, pp. 2746–2751, Oct. 1999.

[62] P. Botsinis, S. X. Ng, and L. Hanzo, "Fixed-complexity quantum-assisted multi-user detection for CDMA and SDMA," *IEEE Trans. Commun.*, vol. 62, no. 3, pp. 990–1000, Mar. 2014.

[63] D. E. Goldberg, *Genetic Algorithms in Search, Optimization and Machine Learning*, 1st ed. Boston, MA, USA: Addison-Wesley, 1989.

[64] G. Syswerda, "A study of reproduction in generational and steady-state genetic algorithms," *Found. Genet. Algorithms*, vol. 1, pp. 94–101, 1991.

[65] D. Alanis, P. Botsinis, S. X. Ng, and L. Hanzo, "Quantum-assisted routing optimization for self-organizing networks," *IEEE Access*, vol. 2, pp. 614–632, 2014.

[66] D. Alanis, P. Botsinis, Z. Babar, S. X. Ng, and L. Hanzo, "Non-dominated quantum iterative routing optimization for wireless multihop networks," *IEEE Access*, vol. 3, pp. 1704–1728, 2015.

[67] A. Ambainis, "Variable time amplitude amplification and a faster quantum algorithm for solving systems of linear equations," *arXiv: 1010/4458v2*, Oct. 2010.

[68] A. M. Childs, R. Kothari, and R. D. Somma, "Quantum algorithm for systems of linear equations with exponentially improved dependence on precision," *ArXiv e-prints*, Nov. 2015.

[69] P. Botsinis, S. X. Ng, and L. Hanzo, "Low-complexity iterative quantum multi-user detection in SDMA systems," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2014, pp. 5592–5597.

[70] L. Hanzo, L.-L. Yang, E.-L. Kuan, and K. Yen, *Single and Multi-Carrier DS-CDMA: Multi-User Detection, Space-Time Spreading, Synchronisation, Networking, and Standards*. New York, NY, USA: Wiley, 2003.

[71] L. Hanzo, M. Münster, B. Choi, and T. Keller, *OFDM and MC-CDMA for Broadband Multi-User Communications, WLANs and Broadcasting*. Chichester, U.K.: Wiley, 2003.

[72] Z. Ding, Z. Yang, P. Fan, and H. V. Poor, "On the performance of non-orthogonal multiple access in 5G systems with randomly deployed users," *IEEE Signal Process. Lett.*, vol. 21, no. 12, pp. 1501–1505, Dec. 2014.

[73] L. Dai *et al.*, "Non-orthogonal multiple access for 5G: Solutions, challenges, opportunities, and future research trends," *IEEE Commun. Mag.*, vol. 53, no. 9, pp. 74–81, Sep. 2015.

[74] Z. Yang, Z. Ding, P. Fan, and G. K. Karagiannidis, "On the performance of non-orthogonal multiple access systems with partial channel information," *IEEE Trans. Commun.*, vol. 64, no. 2, pp. 654–667, Feb. 2016.

[75] Z. Ding *et al.*, "Application of non-orthogonal multiple access in LTE and 5G networks," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 185–191, Feb. 2017.

[76] Z. Ding, P. Fan, and H. V. Poor, "Random beamforming in millimeter-Wave NOMA networks," *IEEE Access*, vol. 5, pp. 7667–7681, 2017.

[77] C. Xu, B. Hu, L.-L. Yang, and L. Hanzo, "Ant-colony-based multiuser detection for multifunctional-antenna-array-assisted MC DS-CDMA systems," *IEEE Trans. Veh. Technol.*, vol. 57, no. 1, pp. 658–663, Jan. 2008.

[78] K. K. Soo, Y. M. Siu, W. S. Chan, L. Yang, and R. S. Chen, "Particle-swarm-optimization-based multiuser detector for CDMA communications," *IEEE Trans. Veh. Technol.*, vol. 56, no. 5, pp. 3006–3013, Sep. 2007.

[79] L. Hanzo, T. H. Liew, B. Yeap, R. Y. S. Tee, and S. X. Ng, *Turbo Coding, Turbo Equalisation and Space-Time Coding: EXIT-Chart Aided Near-Capacity Designs for Wireless Channels*. Wiley, 2010.

[80] P. Botsinis, D. Alanis, S. X. Ng, and L. Hanzo, "Low-complexity soft-output quantum-assisted multiuser detection for direct-sequence spreading and slow subcarrier-hopping aided SDMA-OFDM systems," *IEEE Access*, vol. 2, pp. 451–472, 2014.

[81] P. Botsinis, D. Alanis, Z. Babar, S. X. Ng, and L. Hanzo, "Iterative quantum-assisted multi-user detection for multi-carrier interleave division multiple access systems," *IEEE Trans. Commun.*, vol. 63, no. 10, pp. 3713–3727, Jul. 2015.

[82] Y. Li, N. Seshadri, and S. Ariyavisitakul, "Channel estimation for OFDM systems with transmitter diversity in mobile wireless channels," *IEEE J. Sel. Areas Commun.*, vol. 17, no. 3, pp. 461–471, Mar. 1999.

[83] Y. G. Li, J. H. Winters, and N. R. Sollenberger, "MIMO-OFDM for wireless communications: Signal detection with enhanced channel estimation," *IEEE Trans. Commun.*, vol. 50, no. 9, pp. 1471–1477, Sep. 2002.

[84] S. Sesia, I. Toufik, and M. Baker, *LTE, The UMTS Long Term Evolution: From Theory to Practice*. Chichester, U.K.: Wiley, 2009.

[85] N. Seshadri, "Joint data and channel estimation using blind trellis search techniques," *IEEE Trans. Commun.*, vol. 42, no. 234, pp. 1000–1011, Feb./Mar./Apr. 1994.

[86] S. Chen and Y. Wu, "Maximum likelihood joint channel and data estimation using genetic algorithms," *IEEE Trans. Signal Process.*, vol. 46, no. 5, pp. 1469–1473, May 1998.

[87] D. K. C. So and R. S. Cheng, "Iterative EM receiver for space-time coded systems in MIMO frequency-selective fading channels with channel gain and order estimation," *IEEE Trans. Wireless Commun.*, vol. 3, no. 6, pp. 1928–1935, Nov. 2004.

[88] R. Prasad, C. R. Murthy, and B. D. Rao, "Joint channel estimation and data detection in MIMO-OFDM systems: A sparse Bayesian learning approach," *IEEE Trans. Signal Process.*, vol. 63, no. 20, pp. 5369–5382, Oct. 2015.

[89] A. Assra, W. Hamouda, and A. Youssef, "EM-based joint channel estimation and data detection for MIMO-CDMA systems," *IEEE Trans. Veh. Technol.*, vol. 59, no. 3, pp. 1205–1216, Mar. 2010.

[90] L. Zhang, L. Zhang, and H. Peng, "Quantum clone genetic algorithm based multi-user detection," in *Proc. 2nd Int. Conf. Next Gener. Inf. Technol. (ICNIT)*, Gyeongju, South Korea, Jun. 2011, pp. 115–119.

[91] J. Zhang, S. Chen, X. Mu, and L. Hanzo, "Turbo multi-user detection for OFDM/SDMA systems relying on differential evolution aided iterative channel estimation," *IEEE Trans. Commun.*, vol. 60, no. 6, pp. 1621–1633, Jun. 2012.

[92] C. Novak, G. Matz, and F. Hlawatsch, "IDMA for the multiuser MIMO-OFDM uplink: A factor graph framework for joint data detection and channel estimation," *IEEE Trans. Signal Process.*, vol. 61, no. 16, pp. 4051–4066, Aug. 2013.

[93] J. Zhang, S. Chen, X. Mu, and L. Hanzo, "Evolutionary-algorithm-assisted joint channel estimation and turbo multiuser detection/decoding for OFDM/SDMA," *IEEE Trans. Veh. Technol.*, vol. 63, no. 3, pp. 1204–1222, Mar. 2014.

[94] P. Zhang, S. Chen, and L. Hanzo, "Embedded iterative semi-blind channel estimation for three-stage-concatenated MIMO-aided QAM turbo transceivers," *IEEE Trans. Veh. Technol.*, vol. 63, no. 1, pp. 439–446, Jan. 2014.

[95] M. Jiang, J. Akhtman, and L. Hanzo, "Iterative joint channel estimation and multi-user detection for multiple-antenna aided OFDM systems," *IEEE Trans. Wireless Commun.*, vol. 6, no. 8, pp. 2904–2914, Aug. 2007.

[96] P. Botsinis, D. Alanis, Z. Babar, S. X. Ng, and L. Hanzo, "Joint quantum-assisted channel estimation and data detection," *IEEE Access*, vol. 4, pp. 7658–7681, 2016.

[97] L.-L. Yang, "Multiuser transmission via multiuser detection: Altruistic-optimization and egocentric-optimization," in *Proc. IEEE 65th Veh. Technol. Conf. (VTC)*, Dublin, Ireland, Apr. 2007, pp. 1921–1925.

[98] H. Sung, S.-R. Lee, and I. Lee, "Generalized channel inversion methods for multiuser MIMO systems," *IEEE Trans. Commun.*, vol. 57, no. 11, pp. 3489–3499, Nov. 2009.

[99] W. Yao, S. Chen, S. Tan, and L. Hanzo, "Minimum bit error rate multiuser transmission designs using particle swarm optimisation," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5012–5017, Oct. 2009.

[100] S. Verdu, *Multiuser Detection*, 1st ed. New York, NY, USA: Cambridge Univ. Press, 1998.

[101] C. B. Peel, B. M. Hochwald, and A. L. Swindlehurst, "A vector-perturbation technique for near-capacity multiantenna multiuser communication—Part I: Channel inversion and regularization," *IEEE Trans. Commun.*, vol. 53, no. 1, pp. 195–202, Jan. 2005.

[102] C. Masouros, M. Sellathurai, and T. Ratnarajah, "Vector perturbation based on symbol scaling for limited feedback MISO downlinks," *IEEE Trans. Signal Process.*, vol. 62, no. 3, pp. 562–571, Feb. 2014.

[103] C.-B. Chae, S. Shim, and R. W. Heath, "Block diagonalized vector perturbation for multiuser MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 7, no. 11, pp. 4051–4057, Nov. 2008.

[104] W. Yao, S. Chen, and L. Hanzo, "Improved MMSE vector precoding based on the MBER criterion," in *Proc. IEEE Veh. Technol. Conf.*, Barcelona, Spain, Apr. 2009, pp. 1–5.

[105] C. Masouros, M. Sellathurai, and T. Ratnarajah, "Computationally efficient vector perturbation precoding using thresholded optimization," *IEEE Trans. Commun.*, vol. 61, no. 5, pp. 1880–1890, May 2013.

[106] S. P. Herath, D. H. N. Nguyen, and T. Le-Ngoc, "Vector perturbation precoding for multi-user CoMP downlink transmission," *IEEE Access*, vol. 3, pp. 1491–1502, 2015.

[107] P. Botsinis *et al.*, "Quantum-aided multi-user transmission in non-orthogonal multiple access systems," *IEEE Access*, vol. 4, pp. 7402–7424, 2016.

[108] B. Alawieh, Y. Zhang, C. Assi, and H. Mouftah, "Improving spatial reuse in multihop wireless networks—A Survey," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 3, pp. 71–91, 3rd Quart., 2009.

[109] Y. Chen, S. Zhang, S. Xu, and G. Y. Li, "Fundamental trade-offs on green wireless networks," *IEEE Commun. Mag.*, vol. 49, no. 6, pp. 30–37, Jun. 2011.

[110] C. Luo *et al.*, "Green communication in energy renewable wireless mesh networks: Routing, rate control, and power allocation," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 12, pp. 3211–3220, Dec. 2014.

[111] J. Wen, M. Sheng, X. Wang, J. Li, and H. Sun, "On the capacity of downlink multi-hop heterogeneous cellular networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 8, pp. 4092–4103, Aug. 2014.

[112] M. Al-Rabayah and R. Malaney, "A new scalable hybrid routing protocol for VANETs," *IEEE Trans. Veh. Technol.*, vol. 61, no. 6, pp. 2625–2635, Jul. 2012.

[113] H. Huang *et al.*, "Near-optimal routing protection for in-band software-defined heterogeneous networks," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 11, pp. 2918–2934, Nov. 2016.

[114] J. Yao, S. Feng, X. Zhou, and Y. Liu, "Secure routing in multihop wireless ad-hoc networks with decode-and-forward relaying," *IEEE Trans. Commun.*, vol. 64, no. 2, pp. 753–764, Feb. 2016.

[115] H. Yetgin, K. T. K. Cheung, M. El-Hajjar, and L. H. Hanzo, "A survey of network lifetime maximization techniques in wireless sensor networks," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 828–854, 2nd Quart., 2017.

[116] H. Yetgin, K. T. K. Cheung, M. El-Hajjar, and L. Hanzo, "Network-lifetime maximization of wireless sensor networks," *IEEE Access*, vol. 3, pp. 2191–2226, 2015.

[117] Y. Shi, Y. T. Hou, and H. Sherali, "Cross-layer optimization for data rate utility problem in UWB-based ad hoc networks," *IEEE Trans. Mobile Comput.*, vol. 7, no. 6, pp. 764–777, Jun. 2008.

[118] A. Damnjanovic *et al.*, "A survey on 3GPP heterogeneous networks," *IEEE Wireless Commun.*, vol. 18, no. 3, pp. 10–21, Jun. 2011.

[119] K. Deb, "Multi-objective optimization," in *Search Methodologies*, E. K. Burke and G. Kendall, Eds. New York, NY, USA: Springer, 2005, pp. 273–316.

[120] W. Stadler, "A survey of multicriteria optimization or the vector maximum problem, part I: 1776–1960," *J. Optim. Theory Appl.*, vol. 29, no. 1, pp. 1–52, 1979.

[121] E. Masazade *et al.*, "A multiobjective optimization approach to obtain decision thresholds for distributed detection in wireless sensor networks," *IEEE Trans. Syst., Man, Cybern. B, Cybern.*, vol. 40, no. 2, pp. 444–457, Apr. 2010.

[122] D. Alanis *et al.*, "A quantum-search-aided dynamic programming framework for Pareto optimal routing in wireless multihop networks," *IEEE Trans. Commun.*, vol. 66, no. 8, pp. 3485–3500, Aug. 2018.

[123] D. Alanis *et al.*, "Quantum-aided multi-objective routing optimization using back-tracing-aided dynamic programming," *IEEE Trans. Veh. Technol.*, vol. 67, no. 8, pp. 7856–7860, Aug. 2018.

[124] H. Yetgin, K. T. K. Cheung, and L. Hanzo, "Multi-objective routing optimization using evolutionary algorithms," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Shanghai, China, 2012, pp. 3030–3034.

[125] J. Hu, L.-L. Yang, and L. Hanzo, "Energy-efficient cross-layer design of wireless mesh networks for content sharing in online social networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 9, pp. 8495–8509, Sep. 2017.

[126] J. Zuo *et al.*, "Cross-layer aided energy-efficient opportunistic routing in ad hoc networks," *IEEE Trans. Commun.*, vol. 62, no. 2, pp. 522–535, Feb. 2014.

[127] M. Dehghan, M. Ghaderi, and D. Goeckel, "Minimum-energy cooperative routing in wireless networks with channel variations," *IEEE Trans. Wireless Commun.*, vol. 10, no. 11, pp. 3813–3823, Nov. 2011.

[128] E. Dall'Anese and G. B. Giannakis, "Statistical routing for multihop wireless cognitive networks," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 10, pp. 1983–1993, Nov. 2012.

[129] H. Yetgin, K. T. K. Cheung, M. El-Hajjar, and L. Hanzo, "Cross-layer network lifetime maximization in interference-limited WSNs," *IEEE Trans. Veh. Technol.*, vol. 64, no. 8, pp. 3795–3803, Aug. 2015.

[130] A. E. A. A. Abdulla, H. Nishiyama, J. Yang, N. Ansari, and N. Kato, "HYMN: A novel hybrid multi-hop routing algorithm to improve the longevity of WSNs," *IEEE Trans. Wireless Commun.*, vol. 11, no. 7, pp. 2531–2541, Jul. 2012.

[131] L. Tan, Z. Zhu, F. Ge, and N. Xiong, "Utility maximization resource allocation in wireless networks: Methods and algorithms," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 45, no. 7, pp. 1018–1034, Jul. 2015.

[132] E. W. Dijkstra, "A note on two problems in connexion with graphs," *Numerische Mathematik*, vol. 1, no. 1, pp. 269–271, 1959.

[133] S. P. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.

[134] D. Alanis *et al.*, "Quantum-assisted joint multi-objective routing and load balancing for socially-aware networks," *IEEE Access*, vol. 4, pp. 9993–10028, 2016.

[135] M. Camelo, C. Omaña, and H. Castro, "QoS routing algorithm based on multi-objective optimization for wireless mesh networks," in *Proc. IEEE Latin Amer. Conf. Commun. (LATINCOM)*, Bogotá, Colombia, 2010, pp. 1–6.

[136] A. J. Perez, M. A. Labrador, and P. M. Wightman, "A multiobjective approach to the relay placement problem in WSNs," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Cancún, Mexico, 2011, pp. 475–480.

[137] F. V. C. Martins, E. G. Carrano, E. F. Wanner, R. H. C. Takahashi, and G. R. Mateus, "A hybrid multiobjective evolutionary approach for improving the performance of wireless sensor networks," *IEEE Sensors J.*, vol. 11, no. 3, pp. 545–554, Mar. 2011.

[138] D. Pinto and B. Barán, "Solving multiobjective multicast routing problem with a new ant colony optimization approach," in *Proc. ACM 3rd Int. IFIP/ACM Latin Amer. Conf. Netw.*, Cali, Colombia, 2005, pp. 11–19.

[139] W. Zhang, M. F. Brejza, T. Wang, R. G. Maunder, and L. Hanzo, "Irregular trellis for the near-capacity unary error correction coding of symbol values from an infinite set," *IEEE Trans. Commun.*, vol. 63, no. 12, pp. 5073–5088, Dec. 2015.

[140] Q. You, Y. Li, M. S. Rahman, and Z. Chen, "A near optimal routing scheme for multi-hop relay networks based on Viterbi algorithm," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Ottawa, ON, Canada, Jun. 2012, pp. 4531–4536.

[141] Y. Wang, M. Z. Bocus, and J. P. Coon, "Dynamic programming for route selection in multihop fixed gain amplify-and-forward relay networks," *IEEE Commun. Lett.*, vol. 17, no. 5, pp. 932–935, May 2013.

[142] G. D. Forney, "The Viterbi algorithm," *Proc. IEEE*, vol. 61, no. 3, pp. 268–278, Mar. 1973.

[143] E. Farhi, J. Goldstone, S. Gutmann, and M. Sipser, "Quantum computation by adiabatic evolution," *arXiv preprint quant-ph/0001106*, 2000.

[144] C. Wang, E. Jonckheere, and T. Brun, "Differential geometric treewidth estimation in adiabatic quantum computation," *Quantum Inf. Process.*, vol. 15, no. 10, pp. 3951–3966, Oct. 2016.

[145] C. Wang, H. Chen, and E. Jonckheere, "Quantum versus simulated annealing in wireless interference network optimization," *Sci. Rep.*, vol. 6, May 2016, Art. no. 25797.

[146] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[147] R. Crandall and C. Pomerance, *Prime Numbers: A Computational Perspective*. New York, NY, USA: Springer, 2005.

[148] E. Martín-López *et al.*, "Experimental realization of Shor's quantum factoring algorithm using qubit recycling," *Nat. Photon.*, vol. 6, pp. 773–776, Oct. 2012.

[149] S. Gezici *et al.*, "Localization via ultra-wideband radios: A look at positioning aspects for future sensor networks," *IEEE Signal Process. Mag.*, vol. 22, no. 4, pp. 70–84, Jul. 2005.

[150] A. Khalajmehrabadi, N. Gatsis, and D. Akopian, "Modern WLAN fingerprinting indoor positioning methods and deployment challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 3, pp. 1974–2002, 3rd Quart., 2017.

[151] T. S. Rappaport *et al.*, "Millimeter wave mobile communications for 5G cellular: It will work!" *IEEE Access*, vol. 1, pp. 335–349, 2013.

[152] W. Roh *et al.*, "Millimeter-wave beamforming as an enabling technology for 5G cellular communications: Theoretical feasibility and prototype results," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 106–113, Feb. 2014.

[153] I. A. Hemadeh, M. El-Hajjar, S. Won, and L. Hanzo, "Layered multi-group steered space-time shift-keying for millimeter-wave communications," *IEEE Access*, vol. 4, pp. 3708–3718, 2016.

[154] V. Degli-Esposti *et al.*, "Ray-tracing-based mm-Wave beamforming assessment," *IEEE Access*, vol. 2, pp. 1314–1325, 2014.

[155] S. Feng, X. Li, R. Zhang, M. Jiang, and L. Hanzo, "Hybrid positioning aided amorphous-cell assisted user-centric visible light downlink techniques," *IEEE Access*, vol. 4, pp. 2705–2713, 2016.

[156] S. Rajagopal, R. D. Roberts, and S.-K. Lim, "IEEE 802.15.7 visible light communication: Modulation schemes and dimming support," *IEEE Commun. Mag.*, vol. 50, no. 3, pp. 72–82, Mar. 2012.

[157] P. H. Pathak, X. Feng, P. Hu, and P. Mohapatra, "Visible light communication, networking, and sensing: A survey, potential and challenges," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2047–2077, 4th Quart., 2015.

[158] K. Witrisal *et al.*, "High-accuracy localization for assisted living: 5G systems will turn multipath channels from foe to friend," *IEEE Signal Process. Mag.*, vol. 33, no. 2, pp. 59–70, Mar. 2016.

[159] A. Şahin, Y. S. Eroğlu, İ. Güvenç, N. Pala, and M. Yüksel, "Hybrid 3-D localization for visible light communication systems," *J. Lightw. Technol.*, vol. 33, no. 22, pp. 4589–4599, Nov. 15, 2015.

[160] M. Biagi, S. Pergoloni, and A. M. Vegni, "LAST: A framework to localize, access, schedule, and transmit in indoor VLC systems," *J. Lightw. Technol.*, vol. 33, no. 9, pp. 1872–1887, May 1, 2015.

[161] A. Conti, M. Guerra, D. Dardari, N. Decarli, and M. Z. Win, "Network experimentation for cooperative localization," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 2, pp. 467–475, Feb. 2012.

[162] H. Wymeersch, S. Marano, W. M. Gifford, and M. Z. Win, "A machine learning approach to ranging error mitigation for UWB localization," *IEEE Trans. Commun.*, vol. 60, no. 6, pp. 1719–1728, Jun. 2012.

[163] P. Meissner and K. Witrisal, "Multipath-assisted single-anchor indoor localization in an office environment," in *Proc. Int. Conf. Syst. Signals Image Process. (IWSSIP)*, Vienna, Austria, Apr. 2012, pp. 22–25.

[164] E. Leitinger, P. Meissner, C. Rüdisser, G. Dumphart, and K. Witrisal, "Evaluation of position-related information in multipath components for indoor positioning," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 11, pp. 2313–2328, Nov. 2015.

[165] K. Qiu, F. Zhang, and M. Liu, "Let the light guide us: VLC-based localization," *IEEE Robot. Autom. Mag.*, vol. 23, no. 4, pp. 174–183, Dec. 2016.

[166] H. Liu, H. Darabi, P. Banerjee, and J. Liu, "Survey of wireless indoor positioning techniques and systems," *IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.*, vol. 37, no. 6, pp. 1067–1080, Nov. 2007.

[167] P. Botsinis *et al.*, "Quantum-assisted indoor localization for uplink mm-Wave and downlink visible light communication systems," *IEEE Access*, vol. 5, pp. 23327–23351, 2017.

[168] M. Marjani *et al.*, "Big IoT data analytics: Architecture, opportunities, and open research challenges," *IEEE Access*, vol. 5, pp. 5247–5261, 2017.

[169] K. P. Murphy, *Machine Learning: A Probabilistic Perspective*. Cambridge, MA, USA: MIT Press, 2012.

[170] C. M. Bishop, *Pattern Recognition and Machine Learning* (Information Science and Statistics). Secaucus, NJ, USA: Springer-Verlag, 2006.

[171] C. J. C. Burges, "A tutorial on support vector machines for pattern recognition," *Data Min. Knowl. Disc.*, vol. 2, no. 2, pp. 121–167, 1998.

[172] S.-T. Li and C.-C. Chen, "A regularized monotonic fuzzy support vector machine model for data mining with prior knowledge," *IEEE Trans. Fuzzy Syst.*, vol. 23, no. 5, pp. 1713–1727, Oct. 2015.

[173] Z. Qi, Y. Tian, and Y. Shi, "Successive overrelaxation for Laplacian support vector machine," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 26, no. 4, pp. 674–683, Apr. 2015.

[174] P. Rebentrost, M. Mohseni, and S. Lloyd, "Quantum support vector machine for big data classification," *Phys. Rev. Lett.*, vol. 113, Sep. 2014, Art. no. 130503.

[175] J. A. K. Suykens and J. Vandewalle, "Least squares support vector machine classifiers," *Neural Process. Lett.*, vol. 9, no. 3, pp. 293–300, Jun. 1999.

[176] S. Imre, "Quantum existence testing and its application for finding extreme values in unsorted databases," *IEEE Trans. Comput.*, vol. 56, no. 5, pp. 706–710, May 2007.

[177] S. Yang, X. Xu, D. Alanis, S. X. Ng, and L. Hanzo, "Is the low-complexity mobile-relay-aided FFR-DAS capable of outperforming the high-complexity CoMP?" *IEEE Trans. Veh. Technol.*, vol. 65, no. 4, pp. 2154–2169, Apr. 2016.

[178] C. Pan, M. Elkashlan, J. Wang, J. Yuan, and L. Hanzo, "User-centric C-RAN architecture for ultra-dense 5G networks: Challenges and methodologies," *IEEE Commun. Mag.*, vol. 56, no. 6, pp. 14–20, Jun. 2018.

[179] H. Ren *et al.*, "Low-latency C-RAN: An next-generation wireless approach," *IEEE Veh. Technol. Mag.*, vol. 13, no. 2, pp. 48–56, Jun. 2018.

[180] L. Gupta, R. Jain, and G. Vaszkun, "Survey of important issues in UAV communication networks," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1123–1152, 2nd Quart., 2016.

[181] J. Wang *et al.*, "Taking drones to the next level: Cooperative distributed unmanned-aerial-vehicular networks for small and mini drones," *IEEE Veh. Technol. Mag.*, vol. 12, no. 3, pp. 73–82, Sep. 2017.

[182] M. A. Maddah-Ali and U. Niesen, "Fundamental limits of caching," *IEEE Trans. Inf. Theory*, vol. 60, no. 5, pp. 2856–2867, May 2014.

[183] J. Tadrous and A. Eryilmaz, "On optimal proactive caching for mobile networks with demand uncertainties," *IEEE/ACM Trans. Netw.*, vol. 24, no. 5, pp. 2715–2727, Oct. 2016.

[184] B. Azimdoost, C. Westphal, and H. R. Sadjadpour, "Fundamental limits on throughput capacity in information-centric networks," *IEEE Trans. Commun.*, vol. 64, no. 12, pp. 5037–5049, Dec. 2016.

[185] C. Jiang *et al.*, "Machine learning paradigms for next-generation wireless networks," *IEEE Wireless Commun.*, vol. 24, no. 2, pp. 98–105, Apr. 2016.

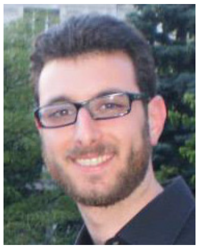
[186] J. Biamonte *et al.*, "Quantum machine learning," *Nature*, vol. 549, no. 7671, pp. 195–202, 2017.

[187] A. Kapoor, N. Wiebe, and K. Svore, "Quantum perceptron models," in *Proc. Adv. Neural Inf. Process. Syst.*, 2016, pp. 3999–4007.

[188] N. Wiebe, A. Kapoor, and K. M. Svore, "Quantum deep learning," *arXiv preprint arXiv:1412.3489*, 2014.

Panagiotis Botsinis (S'12–M'15) received the M.Eng. degree from the School of Electrical and Computer Engineering, National Technical University of Athens, Greece, in 2010 and the M.Sc. degree (with Distinction) and the Ph.D. degree in wireless communications from the University of Southampton, U.K., in 2011 and 2015, respectively, where he is currently a Research Fellow with the Southampton Wireless Group, School of Electronics and Computer Science. Since 2010, he has been a member of the Technical Chamber of Greece.

His research interests include quantum-assisted communications, quantum computation, iterative detection, OFDM, MIMO, multiple access systems, coded modulation, channel coding, cooperative communications, as well as combinatorial optimization.



Dimitrios Alanis (S'13) received the M.Eng. degree in electrical and computer engineering from the Aristotle University of Thessaloniki in 2011 and the M.Sc. degree in wireless communications from the University of Southampton in 2012, where he is currently pursuing the Ph.D. degree with the Southampton Wireless Group, School of Electronics and Computer Science.

His research interests include quantum computation and quantum information theory, quantum search algorithms, cooperative communications, resource allocation for self-organizing networks, bio-inspired optimization algorithms, and classical and quantum game theory.

Zunaira Babar received the B.Eng. degree in electrical engineering from the National University of Science and Technology, Islamabad, Pakistan, in 2008 and the M.Sc. degree (with Distinction) and the Ph.D. degree in wireless communications from the University of Southampton, U.K., in 2011 and 2015, respectively, where she is currently a Research Fellow with Southampton Wireless Group.

Her research interests include quantum error correction codes, channel coding, coded modulation, iterative detection, and cooperative communications.

Hung Viet Nguyen (S'09–M'14) received the B.Eng. degree in electronics and telecommunications from the Hanoi University of Science and Technology, Hanoi, Vietnam, in 1999 and the M.Eng. degree in telecommunications from the Asian Institute of Technology, Bangkok, Thailand, in 2002. Since 1999, he has been a Lecturer with the Post and Telecommunications Institute of Technology, Vietnam. He worked for the OPTIMIX and CONCERTO European as well as EPSRC funded projects. He is currently a Research Fellow with 5G Innovation Centre, University of Surrey, U.K. His research interests include cooperative communications, channel coding, network coding, and quantum communications.

Daryus Chandra (S'13) received the M.Eng. degree in electrical engineering from Universitas Gadjah Mada, Indonesia, in 2014. He is currently pursuing the Ph.D. degree with the Southampton Wireless Group, School of Electronics and Computer Science, University of Southampton. He was a recipient of the Scholarship Award from Indonesia Endowment Fund for Education.

His research interests include channel codes, quantum error correction codes, and quantum communications.

Soon Xin Ng (S'99–M'03–SM'08) received the B.Eng. degree (First Class) in electronics engineering and the Ph.D. degree in wireless communications from the University of Southampton, Southampton, U.K., in 1999 and 2002, respectively. From 2003 to 2006, he was a Post-Doctoral Research Fellow working on collaborative European research projects known as SCOUT, NEWCOM, and PHOENIX. Since 2006, he has been a member of academic staff with the School of Electronics and Computer Science, University of Southampton. He is involved in the OPTIMIX and CONCERTO European projects as well as the IUATC and UC4G projects. He is currently an Associate Professor of telecommunications with the University of Southampton. He has authored over 180 papers and co-authored two Wiley/IEEE Press books in his research field.

His research interests include adaptive coded modulation, coded modulation, channel coding, space–time coding, joint source and channel coding, iterative detection, OFDM, MIMO, cooperative communications, distributed coding, quantum error correction codes, and joint wireless-and-optical-fiber communications. He is a Chartered Engineer and a fellow of the Higher Education Academy in the U.K.

Lajos Hanzo (M'91–SM'92–F'04) received the degree in electronics in 1976, the Doctorate degree in 1983, and the Honorary Doctorate degrees *(Doctor Honoris Causa)* from the Technical University of Budapest in 2009 and the University of Edinburgh in 2015. During his 40-year career in telecommunications he has held various research and academic posts in Hungary, Germany, and the U.K. Since 1986, he has been with the School of Electronics and Computer Science, University of Southampton, U.K., where he holds the Chair in telecommunications. He has successfully supervised 112 Ph.D. students, co-authored 18 Wiley/IEEE Press books on mobile radio communications totalling in excess of 10 000 pages, published 1761 research contributions at IEEE Xplore, acted both as a TPC and the General Chair of IEEE conferences, presented keynote lectures, and has been awarded a number of distinctions. He is currently directing a 40-strong academic research team, working on a range of research projects in the field of wireless multimedia communications sponsored by industry, the Engineering and Physical Sciences Research Council, U.K., the European Research Council's Advanced Fellow Grant, and the Royal Society's Wolfson Research Merit Award. He is an enthusiastic supporter of industrial and academic liaison and he offers a range of industrial courses.

From 2008 to 2012, he was the Editor-in-Chief of the IEEE Press and a Chaired Professor with Tsinghua University, Beijing. He is also a Governor of the IEEE ComSoc and IEEE VTS. He is a fellow of the Royal Academy of Engineering, the Institution of Engineering and Technology, and the European Association for Signal Processing. For further information on research in progress and associated publications please refer to http://wwwmobile.ecs.soton.ac.uk.