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)
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)

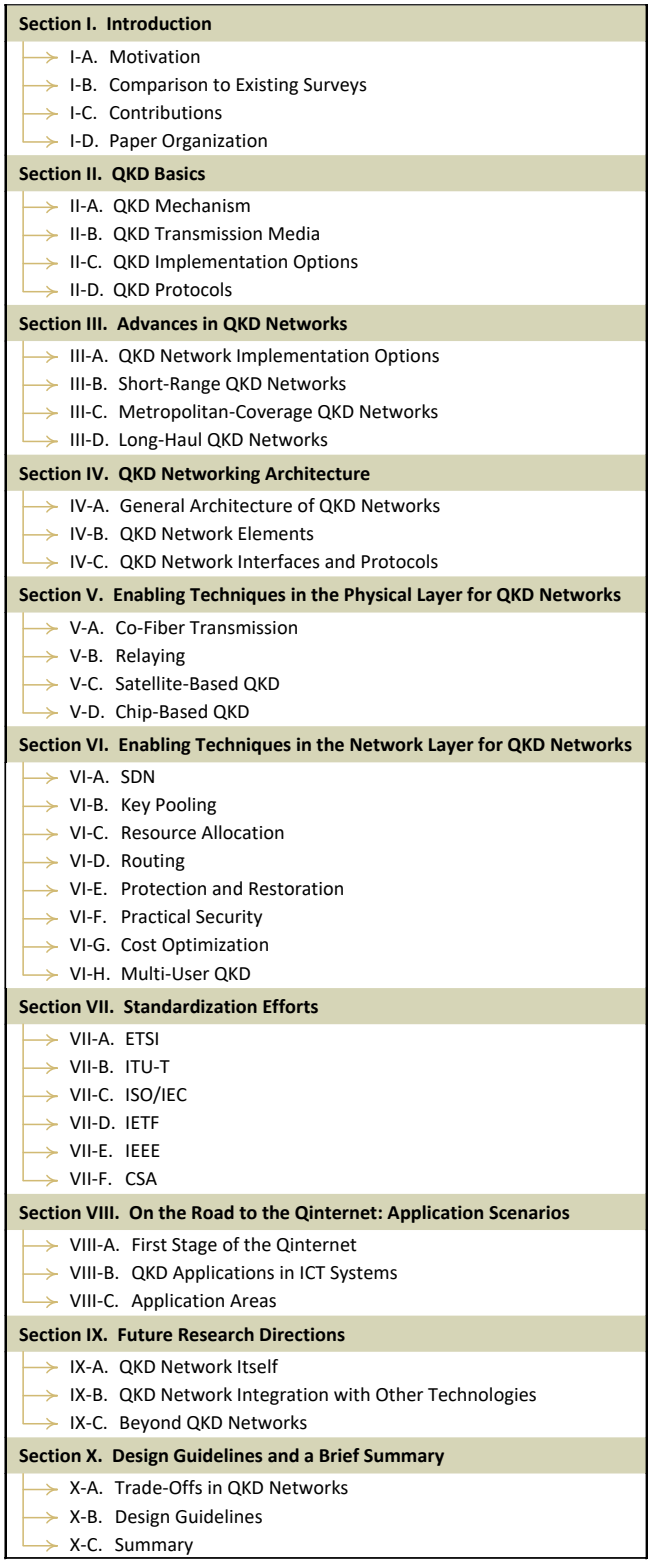

Fig. 1. Outline of this survey paper.

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

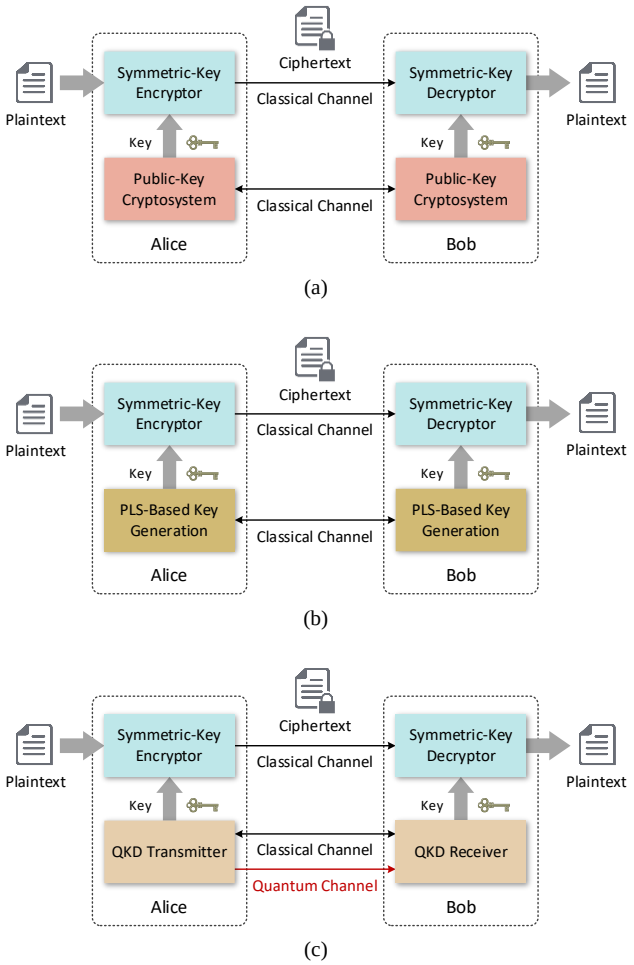

Fig. 2. Illustration of (a) a classic cryptographic scheme; (b) a PLS-based cryptographic scheme; (c) a QKD-based cryptographic scheme.

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.

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].

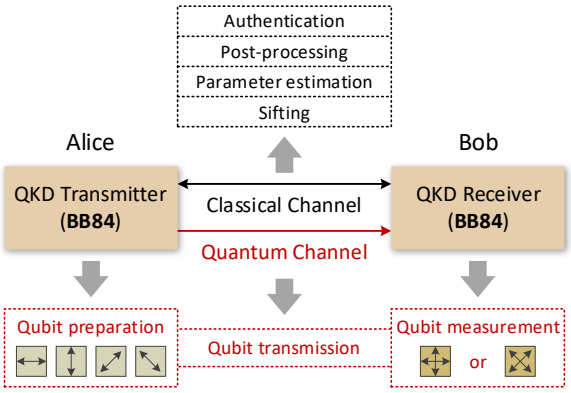

Fig. 3. Illustration of five stages in the BB84 protocol.

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.

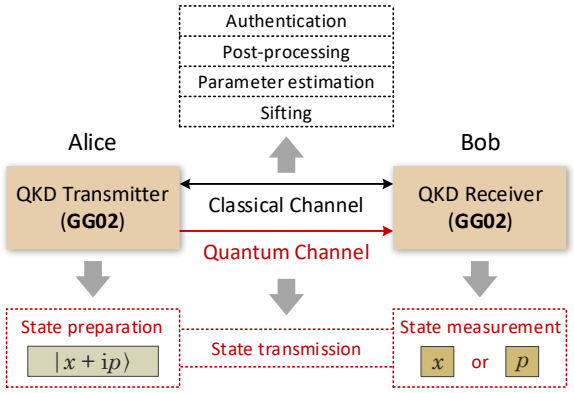

Fig. 4. Illustration of five stages in the GG02 protocol.

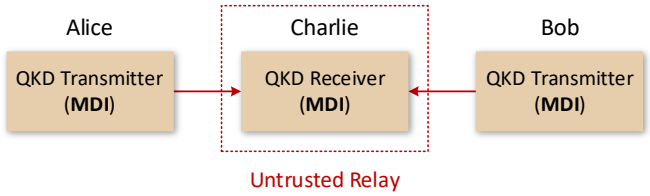

Fig. 5. Illustration of MDI-QKD.

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].

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.

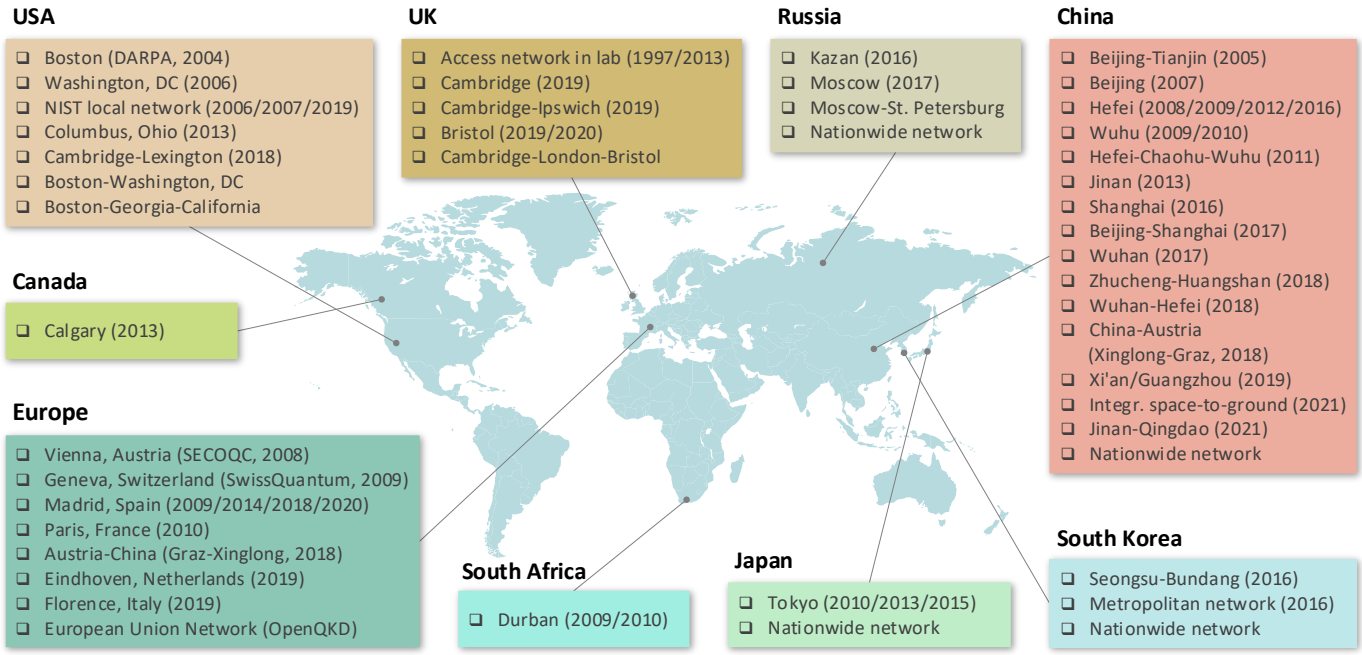

Fig. 6. Overview of QKD network testbeds and field trials around the world.

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

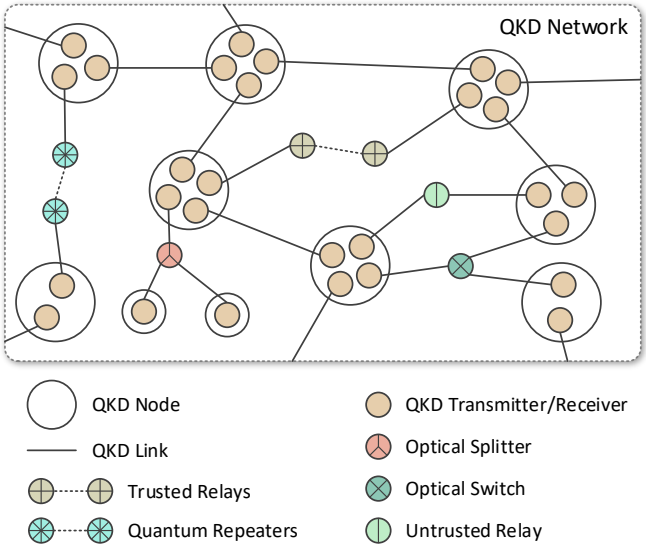

Fig. 7. Illustration of a QKD network incorporating the four relaying options.

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.

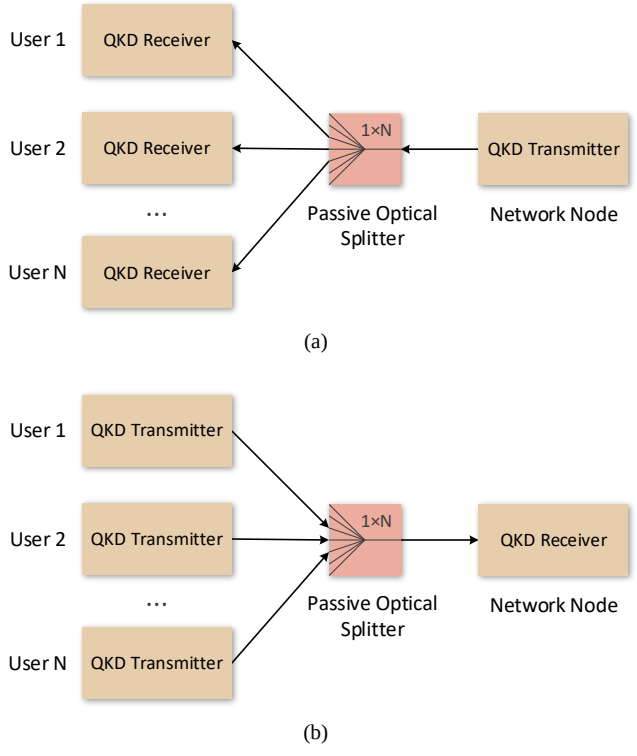

Fig. 8. Illustration of (a) downstream and (b) upstream QKD access networks.

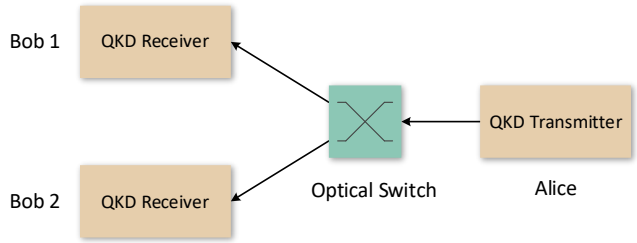

Fig. 9. Illustration of a local QKD network.

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

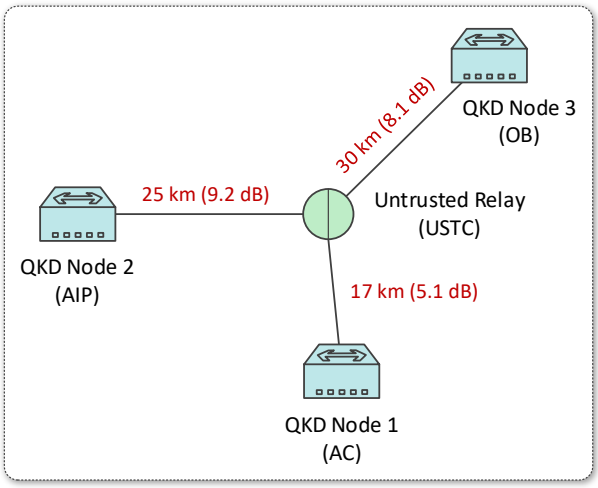

Fig. 10. Illustration of a MDI-QKD metropolitan network in Hefei [132].

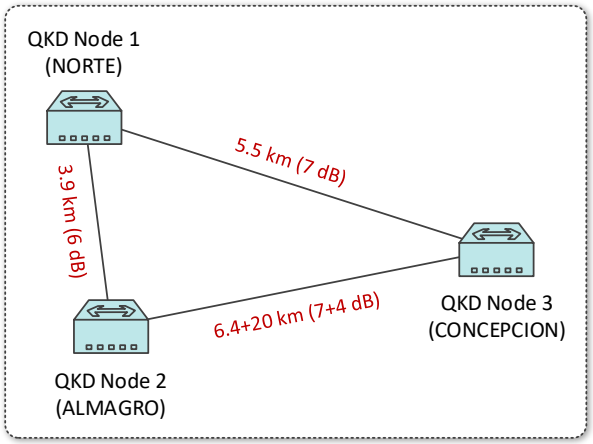

Fig. 11. Illustration of a SDN-enabled CV-QKD metropolitan network in Madrid [126], [163].

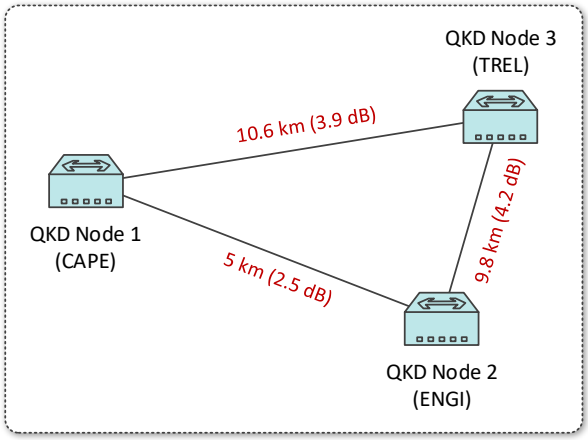

Fig. 12. Illustration of a DV-QKD metropolitan network in Cambridge [47].

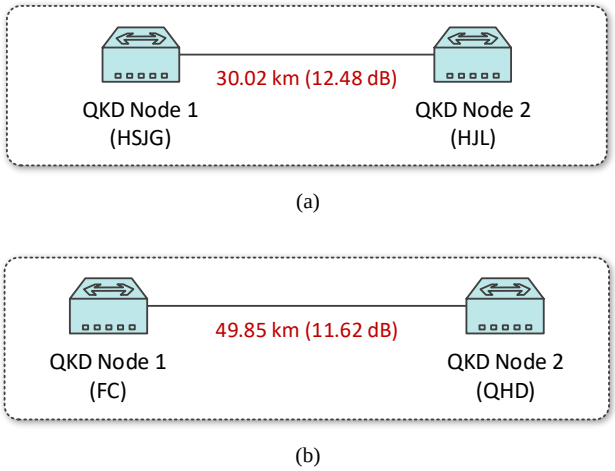

Fig. 13. Illustration of two different CV-QKD metropolitan links in (a) Xi'an and (b) Guangzhou [91].

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]

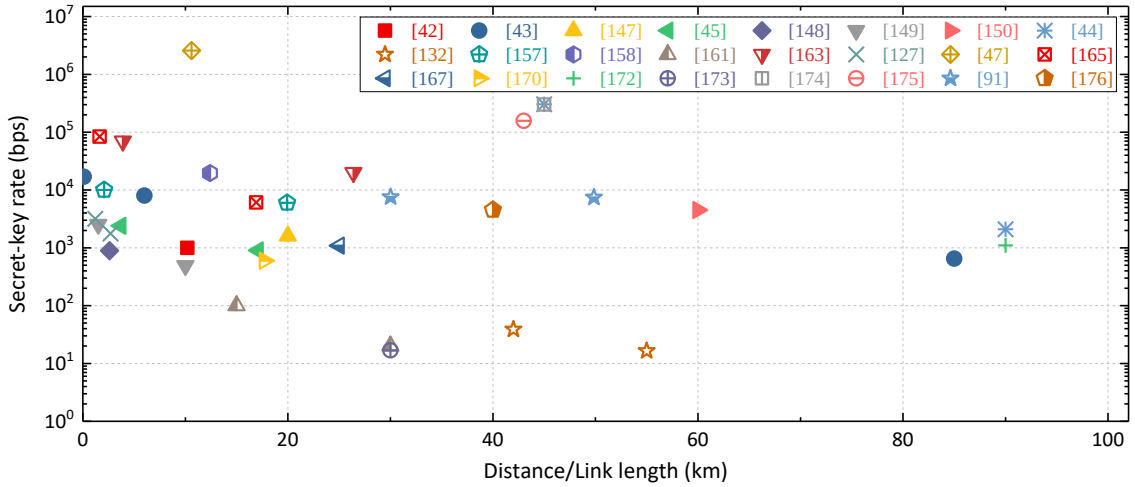

Fig. 14. Secret-key rate versus distance (link length) for different QKD networks/links deployed in various metropolitan areas.

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

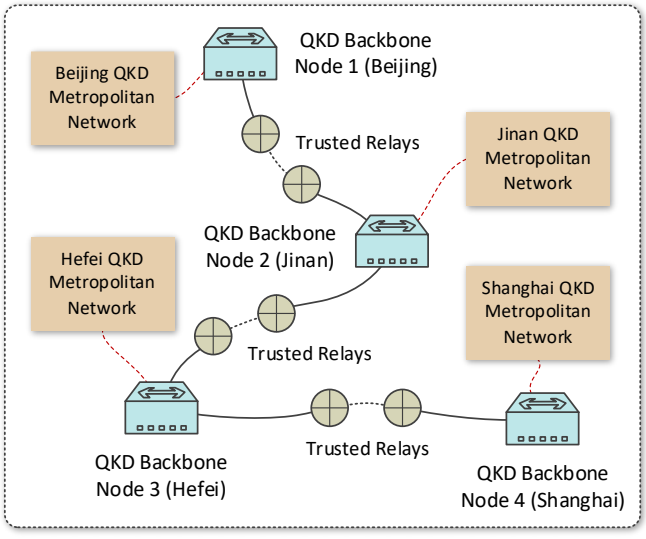

Fig. 15. Illustration of the Beijing-Shanghai QKD backbone network [46].

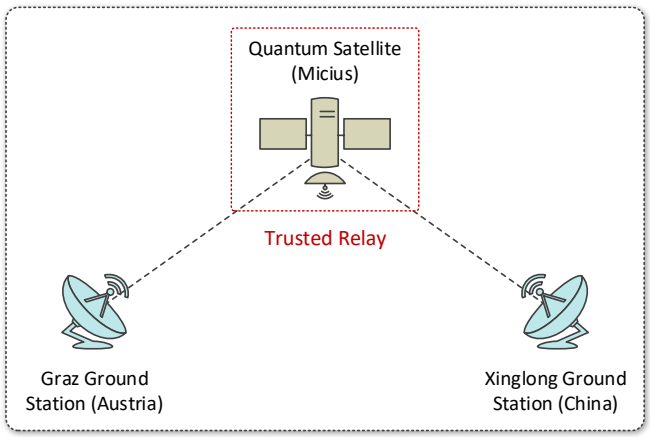

Fig. 16. Illustration of the satellite-based intercontinental QKD network between China and Austria [48].

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

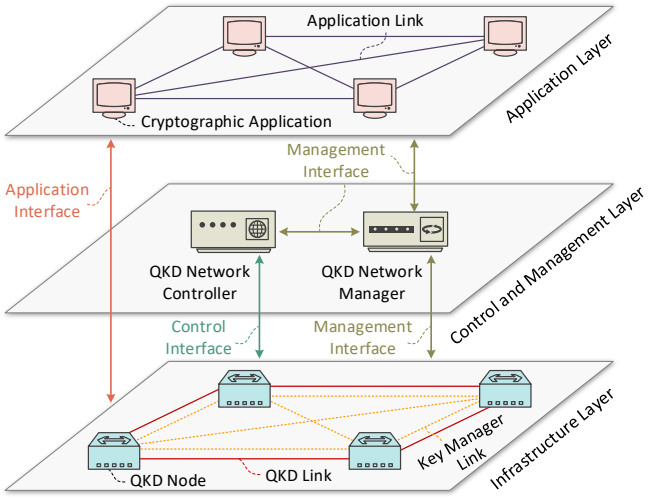

Fig. 17. General architecture of QKD networks.

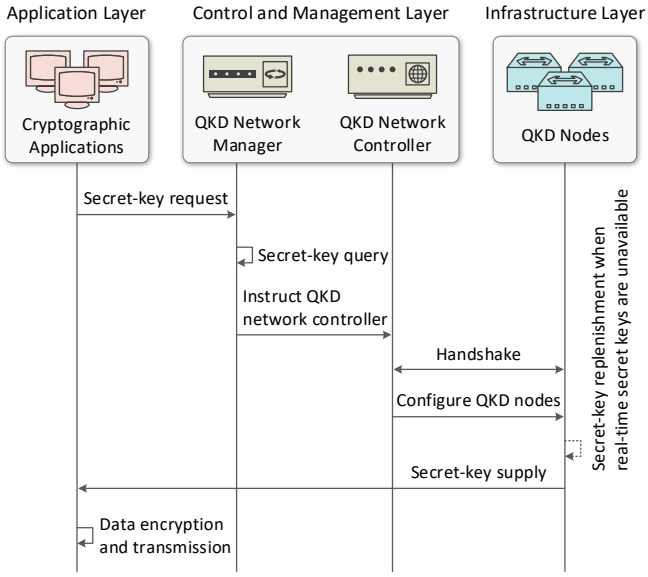

Fig. 18. Illustration of a simple workflow of service provision for cryptographic applications.

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.

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

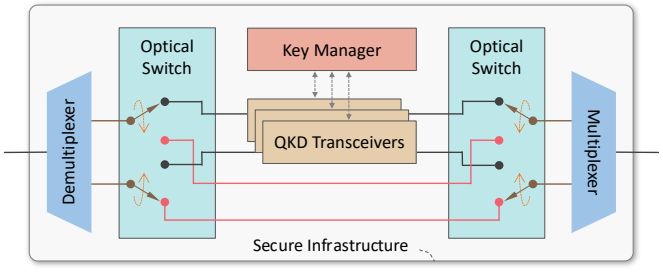

Fig. 19. Illustration of a QKD node structure.

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

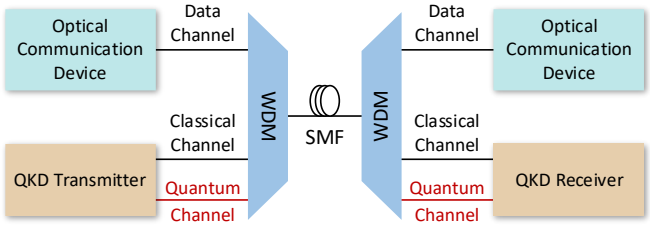

Fig. 20. Illustration of multiplexing quantum and classical (data) channels in a SMF using WDM.

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,

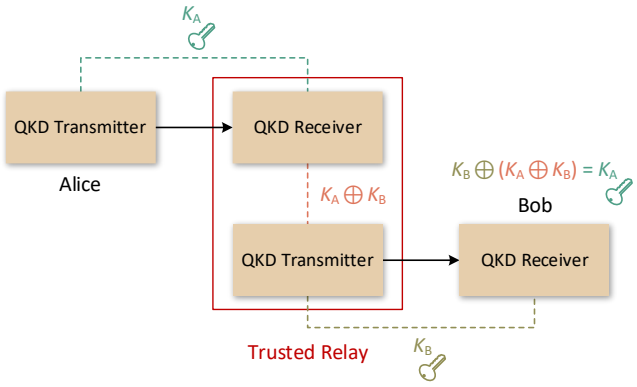

Fig. 21. Illustration of the QKD distance extension via a trusted relay between Alice and Bob.

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 $K_A \oplus K_B$ to Bob. Based on $K_B \oplus (K_A \oplus K_B) = K_A$, 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

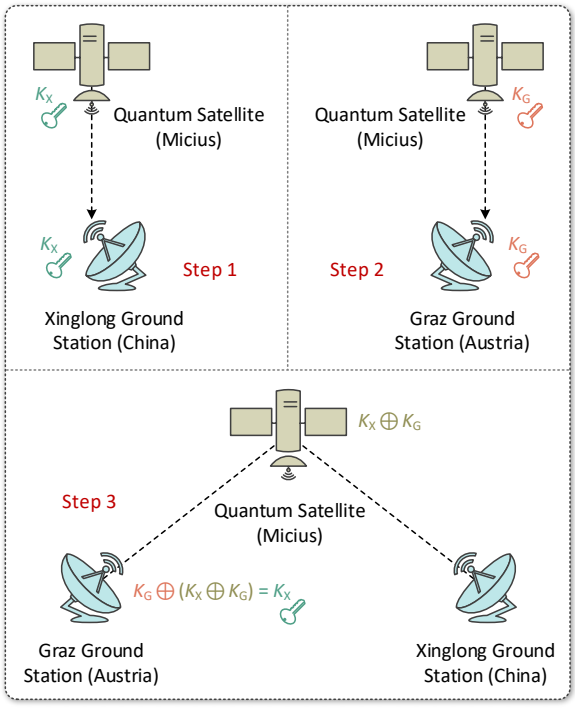

Fig. 22. Illustration of the three steps to enable two ground stations to share a secret key based on the quantum satellite.

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].

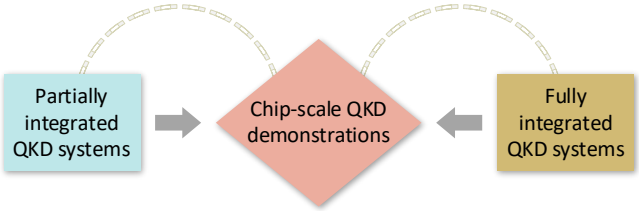

Fig. 23. The evolution of chip-based QKD.

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

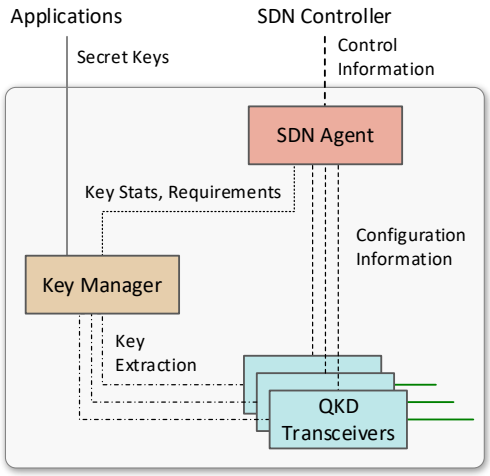

Fig. 24. Abstraction model of a SDN-enabled QKD node [163], [217].

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.

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

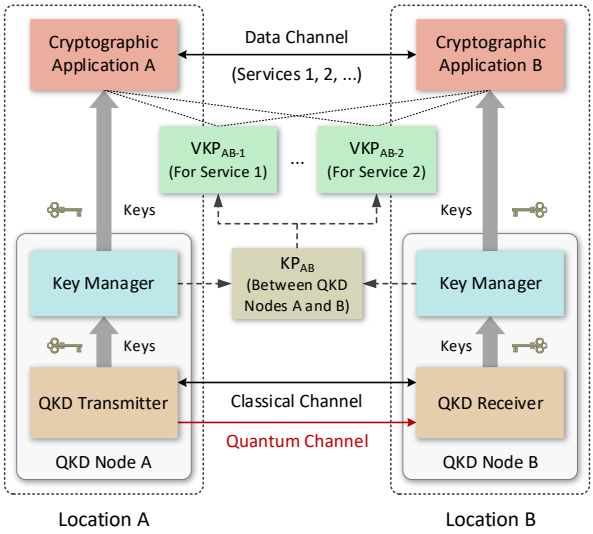

Fig. 25. Illustration of the new concepts of KP and VKP [208].

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.

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

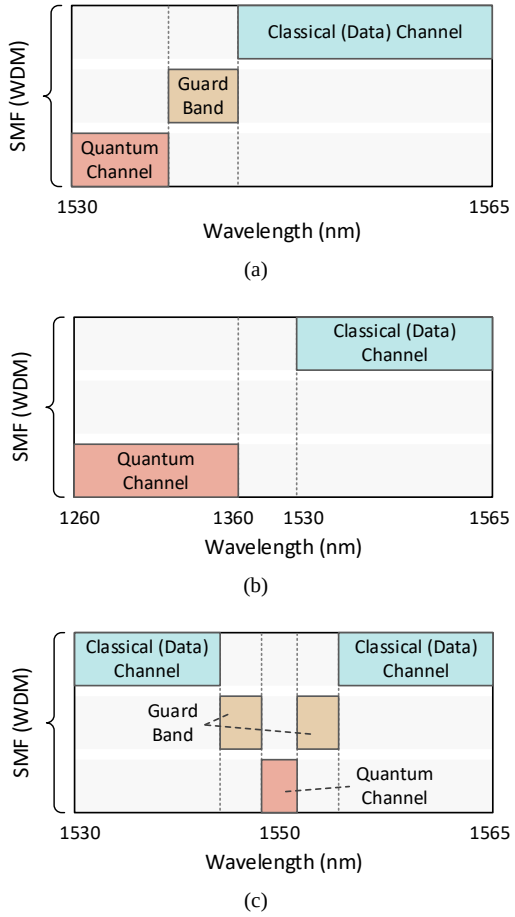

Fig. 26. Three schemes of wavelength allocation for different channels: (a) C-band for both quantum (near 1530 nm) and classical (data) channels [205]; (b) O-band for quantum channels and C-band for classical (data) channels [378]; (c) C-band for both quantum (near 1550 nm) and classical (data) channels.

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

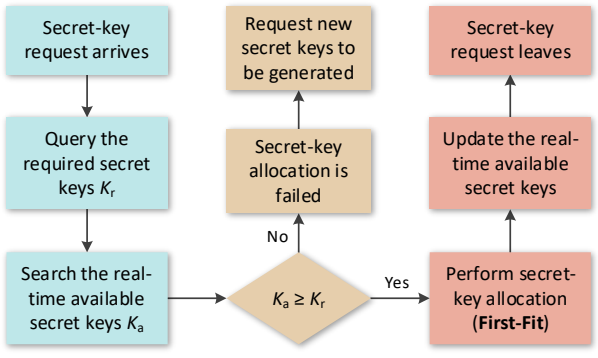

Fig. 27. Illustration of the flowchart of a simple secret-key allocation scheme.

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.

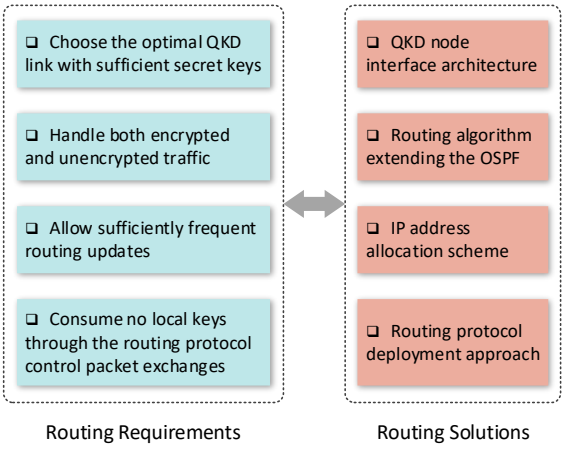

Fig. 28. Routing requirements and bespoke routing solutions for a QKD network [399].

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.

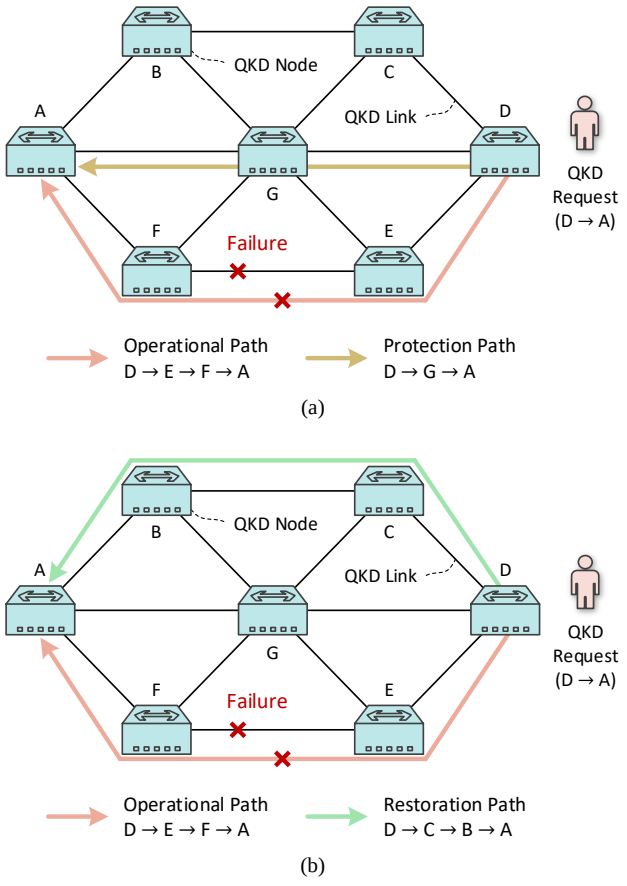

Fig. 29. Illustration of the (a) global path protection scheme and (b) rerouting restoration scheme for QKD networks.

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

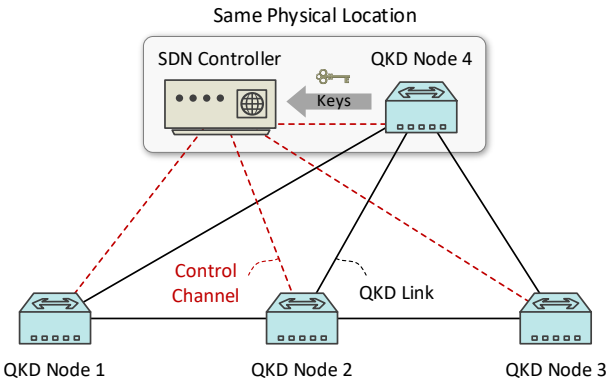

Fig. 30. Illustration of using the QKD-based secret keys to enhance the security of control channels in a SDN-enabled QKD network.

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.

$$N_{\mathrm{T}}^{r}=\left\lceil \frac{L_{sd}}{D}-1 \right\rceil . \quad (3)$$

Then, the total number of QRNs required in a QKD network is

$$N_{\mathrm{T}}^{R}=\sum_{r\in R} N_{\mathrm{T}}^{r} . \quad (4)$$

- *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

$$L_{\mathrm{W}}^{r}=2\frac{v_r}{k}L_{sd} . \quad (5)$$

Then, the total required physical length of QKD links in a QKD network is

$$L_{\mathrm{W}}^{R}=\sum_{r\in R} L_{\mathrm{W}}^{r} . \quad (6)$$

Based on the above formulation, Cao *et al.* [378] defined a cost-oriented model for deploying QKD over a WDM backbone network as follows:

$$C_{\mathrm{Total}}=C_{\mathrm{U}}N_{\mathrm{U}}^{R}+C_{\mathrm{B}}N_{\mathrm{B}}+C_{\mathrm{T}}N_{\mathrm{T}}^{R}+C_{\mathrm{W}}L_{\mathrm{W}}^{R} , \quad (7)$$

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.

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].

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

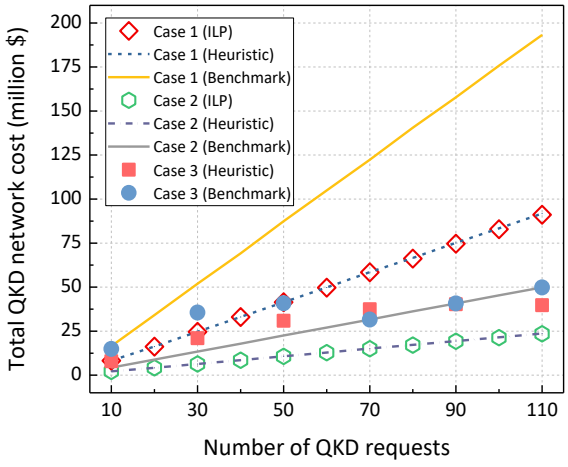

Fig. 31. Illustration of the total QKD network cost versus the number of QKD requests in three cases under the ILP model, heuristic algorithm, and benchmark (14-node 21-link NSFNET topology, $v_r = k$) [378].

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.

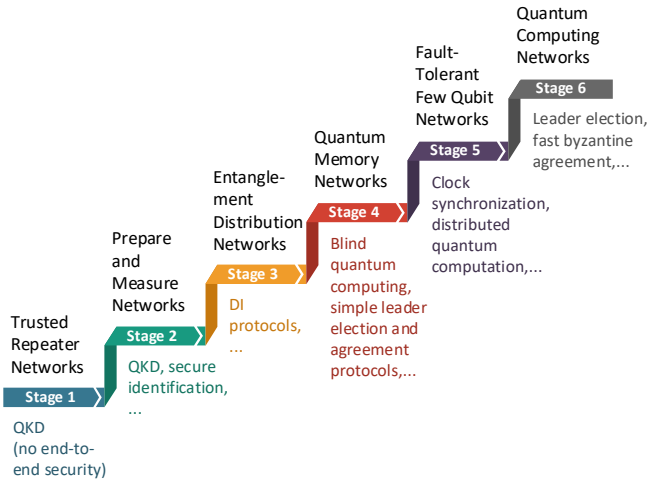

Fig. 32. Stages in the development of a Qinternet [50].

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.

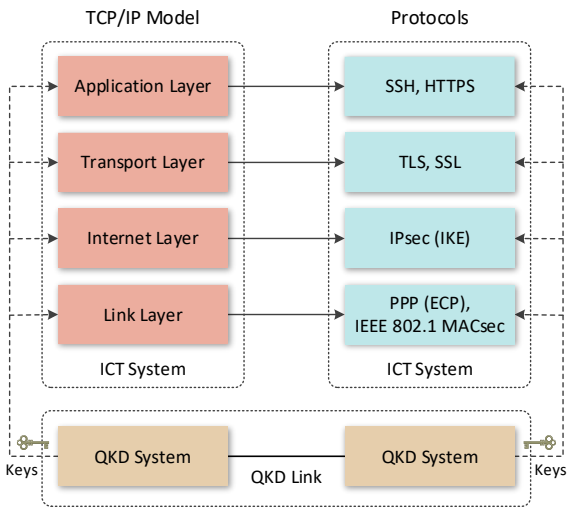

Fig. 33. Application of QKD in ICT systems following the TCP/IP model.

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

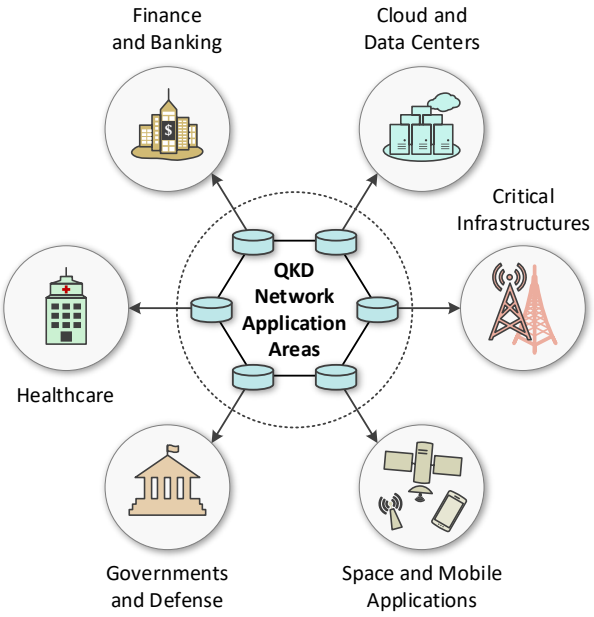

Fig. 34. Various application areas of QKD networks.

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

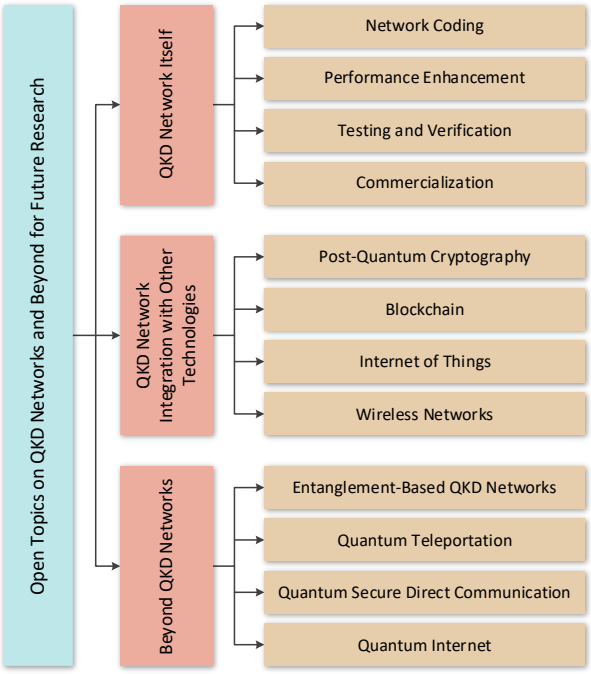

Fig. 35. Open topics on QKD networks and beyond for future research.

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

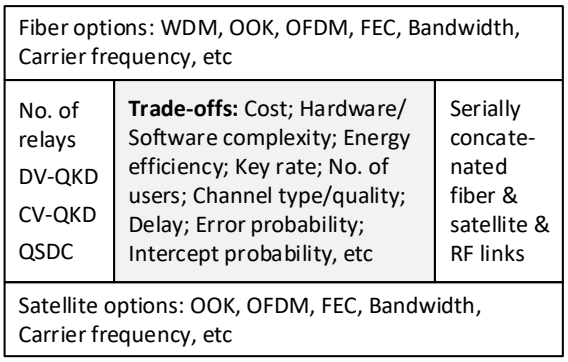

Fig. 37. Design guidelines for QKD networks without quantum repeaters.

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.