This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2021.3106659, IEEE Open Journal of the Communications Society

Quantum Key Distribution Secured Optical Networks: A Survey

Purva Sharma, *Student Member, IEEE,* Anuj Agrawal, *Member, IEEE,* Vimal Bhatia, *Senior Member, IEEE,* Shashi Prakash, *Senior Member, IEEE*, and Amit Kumar Mishra, *Senior Member, IEEE*

Increasing incidents of cyber attacks and evolution of quantum computing poses challenges to secure existing information and communication technologies infrastructure. In recent years, quantum key distribution (QKD) is being extensively researched, and is widely accepted as a promising technology to realize secure networks. Optical fiber networks carry a huge amount of information, and are widely deployed around the world in the backbone terrestrial, submarine, metro, and access networks. Thus, instead of using separate dark fibers for quantum communication, integration of QKD with the existing classical optical networks has been proposed as a cost-efficient solution, however, this integration introduces new research challenges. In this paper, we do a comprehensive survey of the state-of-the-art QKD secured optical networks, which is going to shape communication networks in the coming decades. We elucidate the methods and protocols used in QKD secured optical networks, and describe the process of key establishment. Various methods proposed in the literature to address the networking challenges in QKD secured optical networks, specifically, routing, wavelength and time-slot allocation (RWTA), resiliency, trusted repeater node (TRN) placement, QKD for multicast service, and quantum key recycling are described and compared in detail. This survey begins with the introduction to QKD and its advantages over conventional encryption methods. Thereafter, an overview of QKD is given including quantum bits, basic QKD system, QKD schemes and protocol families along with the detailed description of QKD process based on the Bennett and Brassard-84 (BB84) protocol as it is the most widely used QKD protocol in the literature. QKD system are also prone to some specific types of attacks, hence, we describe the types of quantum hacking attacks on the QKD system along with the methods used to prevent them. Subsequently, the process of point-to-point mechanism of QKD over an optical fiber link is described in detail using the BB84 protocol. Different architectures of QKD secured optical networks are described next. Finally, major findings from this comprehensive survey are summarized with highlighting open issues and challenges in QKD secured optical networks.

***Index Terms*—Quantum-Classical Coexistence; Quantum Key Distribution; Lightpath Attacks; Optical Networks; Routing, Wavelength and Time-slot Allocation; Trusted Repeater Nodes.**

I. INTRODUCTION

QUANTUM KEY DISTRIBUTION (QKD) has emerged as a solution to provide security for the future optical communication networks. Conventional encryption methods enable security against cyber attacks using public-key cryptography [1], [2]. The level of security achieved by such methods is based on the computational complexity of the employed mathematical functions. With the development of faster processing chips, it is becoming easier to compromise the security offered by public-key cryptography. Moreover, the evolution of quantum computers [3], [4], [5], [6], [7], [8], [9] necessitates the need for QKD to secure the information transmitted over communication networks since the existing encryption methods will not be able to provide security in the era of quantum computing [10], [11], [12].

QKD is based on the fundamental principles of quantum mechanics, namely, the Heisenberg's uncertainty principle and the quantum no-cloning theorem [13], [14], [15]. Heisenberg's uncertainty principle states that it is not possible to accurately measure a pair of conjugate properties, i.e., the position and momentum of an object simultaneously [16], [17], [18]. Quantum no-cloning theorem states that it is not possible to exactly replicate the arbitrary unknown quantum states carried by the particles such as photons [19], [20], [21], [22], [23]. The uncertainty principle and the no-cloning theorem imply that a quantum bit (qubit) cannot be copied and any attempt of copying it can be detected by the sender (referred to as 'Alice'), and the receiver (referred to as 'Bob'). QKD generates and distributes secret keys between the sender and the receiver [14], [24]. The generated random secret keys can then be used to encrypt and decrypt the classical data using the conventional encryption algorithms [25] such as one-time pad [26] and advanced encryption standards (AES) [27].

In 1984, Charles H. Bennett and Gilles Brassard developed the first QKD protocol, known as the Bennett and Brassard-84 (BB84) protocol [13], [28], and subsequently, various other QKD protocols were proposed over the years [29], [30], [31], [32], [33], [34], [35], [36], [37]. The schemes and families of QKD protocols are described in Section II along with a detailed description of the first as well as the most widely used BB84 protocol. Most of the QKD protocols employ single-photon sources and detectors for secret key generation and detection. Since the single-photon sources and detectors are still under development, implementation of QKD has been widely done using weak coherent light sources. However, such devices are imperfect for the implementation of QKD and may cause security loopholes in the system, thereby making the QKD system insecure [38], [39], [40]. Thus, to protect the QKD systems from such imperfections, new QKD protocols,

This work was supported in part by the Ministry of Education (MoE) Government of India, in part by the Visvesvaraya Ph.D. scheme, Ministry of Electronics and Information Technology (MeitY).

P. Sharma is with the Signals and Software Group, Department of Electrical Engineering, Indian Institute of Technology Indore, Indore, 453552 India (e-mail: phd1801202007@iiti.ac.in).

A. Agrawal is with the Signals and Software Group, Department of Electrical Engineering, Indian Institute of Technology Indore, Indore 453552, India and Indian Institute of Technology Gandhinagar, Gujarat 382355, India (e-mail: anujagrawal@ieee.org).

V. Bhatia is with the Signals and Software Group, Department of Electrical Engineering, Indian Institute of Technology Indore, Indore 453552, India and UHK FIM, Czech Republic-500 03 (e-mail: vbhatia@iiti.ac.in).

S. Prakash is with Photonics Laboratory, Department of Electronics & Instrumentation Engineering, Institute of Engineering and Technology, Devi Ahilya University, Indore 452017, India (e-mail: spraksh@ietdavv.edu.in).

A.K. Mishra is with Department of Electrical Engineering, University of Cape Town, South Africa (e-mail: amit.mishra@uct.ac.za).

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2021.3106659, IEEE Open Journal of the Communications Society

namely, the decoy-state QKD protocol [41], [42], [43] and the measurement-device-independent QKD (MDI-QKD) protocol [44], [45], [46] have been proposed.

QKD can be realized over both the free-space [47], [48], [49] and the optical fiber [50], [51], [52] media. In this survey, we focus on the optical fiber networks secured by QKD. Optical fiber has been usually considered as a secure mode of transmission due to propagation of optical signals inside the guided medium, however, the increasing incidents of lightpath attacks including jamming, eavesdropping, data interception, among others [53], [54], [55] motivated the research and development of QKD secured optical fiber communication. The initial QKD experiments were conducted over separate dark fibers. However, the dark fibers are neither available in abundance to realize quantum communication globally, nor it is cost-effective to deploy a separate global optical network for this purpose. Since optical fibers carry almost all of the global internet traffic currently, and are deployed widely around the world in the access, metro, terrestrial backbone, and the submarine networks, it is a general consensus to integrate QKD with the existing optical networks. However, since the quantum signals are weak (consisting of few countable photons per pulse) as compared to the classical signals (consisting of millions of photons per pulse), the coexistence of quantum and classical signals in a common optical fiber is challenging. Moreover, the transmission distance of quantum signals is much lower as compared to the classical signals as they are weak. Furthermore, any interaction between the quantum signals and classical signals might further deteriorate the quality of quantum signals and can also alter the quantum states. Thus, to integrate QKD with the existing optical networks, multiplexing techniques, namely, wavelength division multiplexing (WDM) and time division multiplexing (TDM) have been extensively researched in the recent past to share the available optical bandwidth among the quantum and classical signals. WDM is used to transmit multiple optical signals onto a single fiber using multiple wavelengths, whereas TDM is used to transmit multiple data streams over a common communication channel by separating them into multiple segments, where each independent data stream is demultiplexed at the receiving end in the time domain.

In 1997, Townsend demonstrated the first simultaneous transmission of quantum and classical signals over single fiber using WDM, where original (O)-band (1260-1360 nm) was used for the quantum signals, and conventional (C)-band (1530-1565 nm) for the classical signals [56]. Thus, using WDM in the QKD secured optical networks, the quantum and classical signals are spaced apart in wavelength, where the optical band used for the quantum signals is referred to as the quantum signal channel (QSCh), and the optical band used for the transmission of classical signals is referred to as the traditional data channel (TDCh) [12],[24]. Quantum signals are transmitted through the QSCh by using TDM. Besides the QSCh and TDCh, another channel, namely, public interaction channel (PICh) is also required [24] to transmit the quantum bit (qubit) measuring-basis and the information during post-processing between the sender and the receiver [24]. O-band has higher losses as compared to the C-band, hence it restricts the transmission distance of weak quantum signals, and results in lower secret key rate (SKR) [57]. Thus, in the later experiments, all the three types of channels, namely, QSCh, PICh, and TDCh were allocated different wavelengths bands from the C-band, thus bringing the three of them closer. In [58], experimental demonstration of quantum-classical coexistence in C-band was performed using dense WDM (DWDM), where the spacing between the channels was kept as 400 GHz and 800 GHz . This channel spacing is necessary to avoid interaction between the quantum and the classical signals [59], [60]. However, a higher channel spacing results in spectrum wastage. Thus, efforts have been made to further reduce the channel spacing, and an experimental demonstration of quantum-classical coexistence was conducted with 200 GHz channel spacing [52], as shown in Fig. 1. Several other demonstrations of multiplexing QSCh, PICh, and TDCh in a single fiber have been conducted recently [50], [51], [61], [62], [63], [64], [65], [66], [67], [68]. Although several successful demonstrations of quantum-classical coexistence in a single fiber have been conducted for point-to-point links, the QKD secured networks present new challenges to be addressed for practical realization of quantum communication globally over the existing optical networks. Such networking challenges of QKD secured optical networks, the procedure involved, and detailed explanation of Fig. 1, i.e., allocation of channels using WDM are given in Section V.

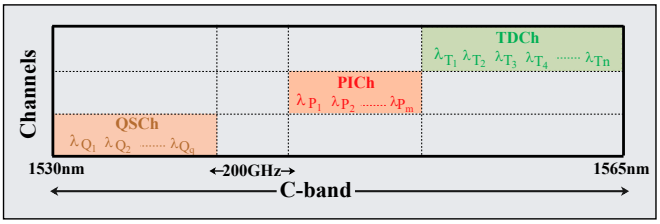


Fig. 1: Types of channels in QKD-secured optical networks [12]

Several QKD networks and testbeds have been established in different part of the world to assess their performance in real environment. The world's first quantum cryptography network, namely, Defense Advanced Research Project Agency (DARPA) quantum network, consisting of 10 nodes was installed between Harvard University, Boston University, and BBN [69], [70]. The European project for Secure Communication based on Quantum Cryptography (SECOQC) combined several QKD systems into a single QKD network considering trusted repeater architecture for long-distance communication in Vienna in 2008 [71]. A QKD network has been established in Tokyo by different organizations of Japan and Europe [72] in 2010. Various long-term performance analyses of QKD networks over the existing regional optical networks have been conducted, namely, the SwissQuantum in Geneva [73] that uses trusted repeaters, the Durban network in South Africa [74], and the Cambridge quantum network [75]. A metropolitan quantum network was demonstrated in Wuhu, China [76]. In 2017, a 2000 km quantum link was established in China, connecting four cities, namely, Beijing, Shanghai, Jinan, and Hefei [77], [78], [79]. Based on the developed

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2021.3106659, IEEE Open Journal of the Communications Society

technology of quantum-classical signal coexistence, a few companies [80], [81], [82], [83] currently provide dedicated QKD services to governments, enterprises, and industrial customers for protection of critical data in transit; and QKD equipments to the research labs. Technological advancements and progress have been made since the beginning of the DARPA quantum network in 2002, and the methods used and the processes involved in the practical QKD test-beds and experiments, such as, key establishment, resource assignment, trusted and untrusted repetition for long-distance communication, among others, are described in Section V along with the proposed schemes in the literature and summarized in Table IV. Moreover, major practical QKD systems involving the optical networking concepts described in Section IV-V, are summarized in Table V.

Despite the successful practical implementation of QKD and performance analyses over testbeds, there are several challenges to be addressed for global deployment of QKD networks over the existing optical fibers used for classical communication in a cost-efficient manner. Almost all the experiments conducted till now for the QKD secured long-haul optical networks are based on the placement of trusted repeater nodes (TRNs) at regular distances to transmit the weak quantum signals over long distances. TRNs increase the cost of the system, and the reliance on TRNs might affect the security of the system as well, hence new QKD secured optical networks are being developed using MDI-QKD [44], [45], [46], [84] and twin-field QKD (TF-QKD) [85], [86], [87] to increase the transmission distance and secret key rate, thus avoiding/reducing the TRNs. Moreover, integration of QKD with the existing optical networks introduce new networking challenges including routing, wavelength, and time-slot allocation (RWTA), resilient QKD, TRN placement, integration with cloud datacenters, among others. Extensive research has been done in the recent years to propose architectures for QKD secured optical networks based on WDM and to address various networking challenges. However, a greater challenge lies ahead to explore integration of QKD with the next-generation optical network technologies to be used for classical communication that provide spectral and spatial flexibility to expand the capacity of optical networks.

Standardization efforts on QKD systems and networks are also in progress by organizations such as International Telecommunication Union (ITU), European Telecommunications Standards Institute (ETSI), International Organization for Standardization/International Electrotechnical Commission (ISO/IEC), Institute of Electrical and Electronics Engineers (IEEE) and Internet Engineering Task Force/Internet Research Task Force (IETF/IRTF) [88]. Standardization of QKD systems and networks is essential to facilitate interoperability of QKD devices in a multi-vendor environment that will make it possible to integrate QKD technology with the communication networks. Documentation related to QKD standards have been released by different standards developing organizations, and some more are still in progress. The ITU-Telecommunications (ITU-T) Study Group 13 (ITU-T SG 13) "Future Networks" [89] is focusing on next-generation networks (NGNs), network aspects of mobile telecommunications, and standardization of QKD networks (QKDN) and have published majority of its standards on QKD in the Y-series of ITU-T recommendations. The ITU-T Y.3800-Y.3804 recommendations cover overview of networks supporting QKD; functional requirements and architecture; key management, quality of service aspect; and control and management [90]. The ITU-T Study Group 17 (ITU-T SG 17) "Security" [91] recently started working on standardization in quantum network security and published its standards in the X-series of ITU-T recommendations. This recommendation series include security considerations [92], security framework, key combination and confidential key supply for QKD networks.

An Industry Specification Group (ISG) on QKD for users at ETSI (ETSI ISG-QKD) [93] is working on various industry specifications and have published several group specification documents on QKD (ETSI GS QKD), such as internal and application interfaces, module security specification, optical characterization of QKD components and QKD system, implementation of security requirements, and a control interface for software-defined networks [94]. A working group-WG3 "Security Evaluation, Testing, and Specification" of ISO and IEC (ISO/IEC Joint Technical Committee (JTC) 1/SC27) is focusing on security requirements, test, and evaluation methods for QKD and have proposed standards for improving the design and implementation security of different QKD devices and evaluating the security of QKD modules [88], [92]. The IEEE P1913 draft standard [95] enables dynamic addition, modification, and removal of quantum protocols or applications by configuring quantum devices in communication networks. In IEEE P1913, a YANG model is presented, whose QKD module, when applied to devices in a communication network, can capture the information such as transceiver rates, QKD protocol, and other QKD-specific characteristics. Although several standardization efforts are ongoing worldwide, consideration of parallel technological advancements in the classical and quantum communication technologies, and harmonization among different standardization organizations is essential to avoid possible contradictions in the standards being published by them.

This survey aims to cover all the relevant aspects of QKD secured optical networks including the motivation behind the necessity of QKD secured optical networks. Thus, the important terminologies and concepts of QKD are described first, such as qubit, a basic QKD system, types of attacks in QKD systems, and different QKD protocols (with detailed description of BB84 protocol since we use it later to explain the process of QKD secured optical communication networks) to develop a basic understanding. However, the readers interested in others important aspects of QKD such as device-level research and protocol-specific studies are encouraged to refer to the corresponding literature. The point-to-point QKD over fiber system; architecture of mesh connected QKD secured optical networks; important networking challenges in QKD secured optical networks and the existing methods to solve them are described next. Furthermore, some of the most relevant challenges and crucial research aspects related to QKD secured optical networks are highlighted. A summary of learnings from this survey is given at the end. To the best

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2021.3106659, IEEE Open Journal of the Communications Society

of authors' knowledge, this is the first survey that covers the networking aspects of QKD secured optical networks. A few survey papers [1],[15], [25], [96], [97], [98], [99], [100] have been published on some specific issues of quantum cryptography and related areas. However, none of them provide a comprehensive survey and discussion covering various aspects that are essential to develop a complete understanding of the QKD secured optical networks. Moreover, discussion on the limitations of the existing technology and important future research directions covering various aspects are essential for a survey article that we provide in this paper.

A. Contributions of this Paper

Main contributions of this survey paper are as follows:

- We provide an overview of the need of QKD in the quantum computing era and the integration of QKD with optical networks.
- A review of the experimental demonstrations conducted till now for QKD secured optical networks and testbeds developed in different parts of the world.
- We provide a review of QKD with relevant examples and the process for secret key generation using BB84 protocol. BB84 protocol has been widely used in the literature as well as in the experimental demonstrations. Thus, in this paper, to describe various concepts and procedures, we use BB84, and hence explain the BB84 protocol in detail in Section II.B.3(a).
- We survey and review different types of quantum hacking attacks, and methods to protect optical networks from such attacks.
- Various architectures of QKD secured optical networks using WDM are explained in detail covering different types of channels and planes.
- Networking aspects and new research challenges in QKD secured optical networks are highlighted and various state-of-the-art methods proposed to address those challenges are elucidated.
- We discuss the limitations of the existing methods, and highlight some of the most relevant open issues and challenges to be addressed in the QKD secured WDM optical network, elastic optical network (EON), and the multicore fiber (MCF) network.

B. Organization of this Paper

In Section II, basics of QKD such as those related to qubits, QKD protocols, the QKD system and its underlying process using the BB84 protocol, quantum hacking attacks and their methods of prevention are reviewed. Section III explains the point-to-point mechanism of quantum-secured optical networks. Section IV describes different architectures of QKD-secured optical networks. Section V elucidates networking aspects of QKD secured optical networks along with the existing methods proposed to solve the key networking challenges. Section VI presents open issues and challenges in QKD secured optical networks. Section VII summarizes the key findings from this survey paper. Finally, Section VIII concludes the paper. A list of abbreviations is given in Appendix A.

II. Overview of Quantum Key Distribution

This section gives an overview of QKD including qubits and its representation, and a basic yet complete QKD system. Subsequently, we describe the underlying QKD process using the BB84 protocol, the schemes for designing QKD protocols, and the quantum hacking attacks along with the method of prevention.

A. Quantum Bits

A classical bit is the basic entity of the classical computation and information systems. Similarly, a qubit coined by Benjamin Schumacher [101] is the basic entity of the quantum information and quantum computation systems [21]. In a classical system, a bit can be in two states, i.e., 0 or 1. In quantum systems, a qubit has two basis states, represented as $|0\rangle$ or $|1\rangle$, where $|\rangle$ is Dirac or bra-ket notation [21], [102]. However, a qubit can be in a quantum superposition of the basis states $|0\rangle$ and $|1\rangle$ simultaneously [5], [8], [103], which is the key difference between a classical bit and a qubit. Bloch sphere is used to graphically represent the possible quantum states of a qubit, as shown in Fig. 2 [21]. Fig. 3 shows the vector representation of the classical bit and the qubit. The representation of qubit states depends on the computational basis. Some examples of qubit states $|\psi\rangle$ in the Bloch sphere are $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$, $|+i\rangle$, and $|-i\rangle$.

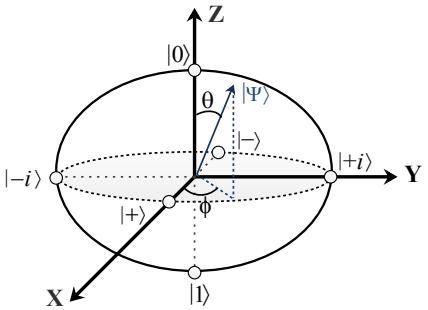


Fig. 2: Bloch Sphere [21], [104]

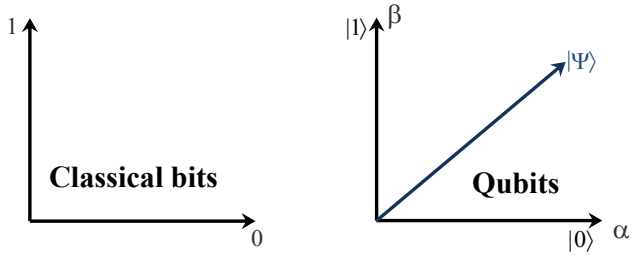


Fig. 3: Vector representation of classical bit and qubit

B. Basic QKD System

This subsection describes a basic QKD system, QKD protocols, and the process of QKD system using BB84 protocol

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2021.3106659, IEEE Open Journal of the Communications Society

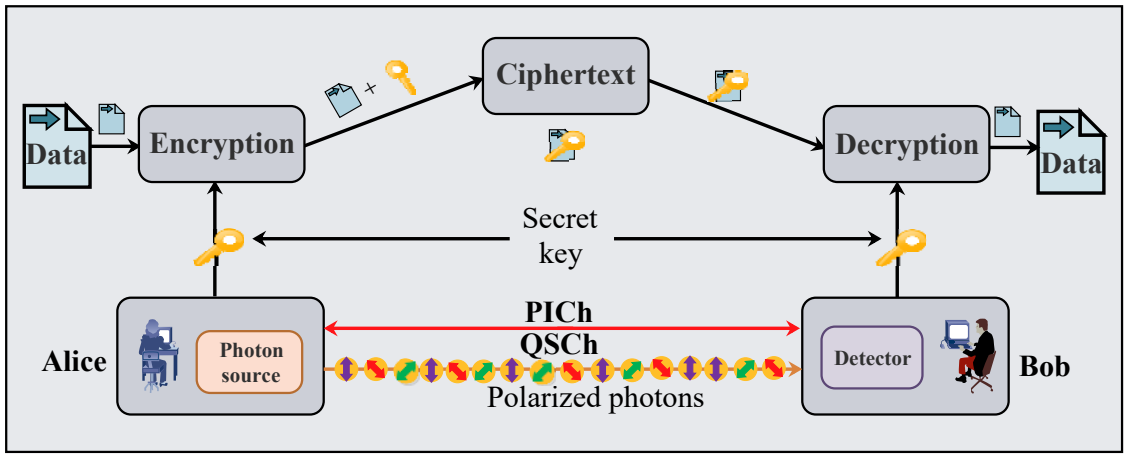


Fig. 4: Basic QKD system [105]

1) Components of a basic QKD system and their functionalities

A QKD system requires two types of channels, viz. QSCh [106] and PICh; a QKD protocol; and encryption/decryption blocks, as shown in Fig. 4.

- QSCh is used to send the quantum states of light (photons) between the nodes, i.e., Alice and Bob.
- PICh is used to transmit the measuring-basis of qubits, and to verify the generated shared secret keys using the post-processing methods [107]. After post-processing, a final random secret key is generated between Alice and Bob.
- A QKD protocol [96] is used in QKD to establish secure connection between Alice and Bob. It generates secret keys and also analyzes the amount of correct information shared between the users during the key generation.
- The encryption and decryption blocks are required to encrypt the information using the secret keys and then to decrypt it back.

2) Quantum key distribution protocols

(a) Schemes of QKD Protocol: The two main schemes used to design QKD protocols are Prepare and Measure (P&M) scheme, and Entanglement-Based (EB) scheme [1], [96], [108].

(i) Prepare and Measure Scheme: In the P&M scheme, Alice *prepares* the information in the form of polarized photons and then sends that information to Bob, which is then *measured* by Bob [96], [108], as shown in Fig. 5. The process of P&M scheme is described in detail in Section II.B.3(a) using BB84 protocol. The P&M scheme is based on two fundamental laws of quantum mechanics, namely, the Heisenberg's uncertainty principle and the quantum no-cloning theorem [105]. Some of the QKD protocols based on this scheme are BB84 [13], Bennett-92 (B92) [30], Six-State protocol (SSP) [32], [33], Scarani Acin Ribordy Gisin-04 (SARG04) [34], Differential Phase Shift (DPS) [36], [37], and others [44], [109].

(ii) Entanglement-Based Scheme: In the EB scheme, a source generates entangled pairs of photons, i.e., the entangled

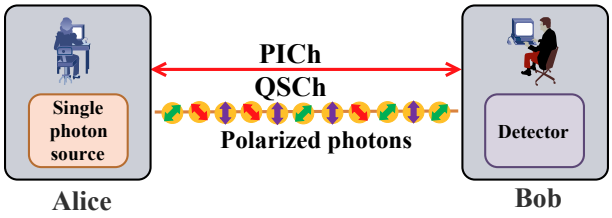


Fig. 5: Concept of prepare and measure scheme [105]

quantum states, and sends them to Alice and Bob [110], as shown in Fig. 6. Alice and Bob then measure the received quantum states. In this scheme, the quantum states of both the sender and receiver are associated in such a way that the measurement on one affects the other, and both can easily detect any attempt of eavesdropping [108]. The QKD protocols based on this scheme are Ekert-91 (E91) [29] and Bennett Brassard Meermin-92 (BBM92) [31].

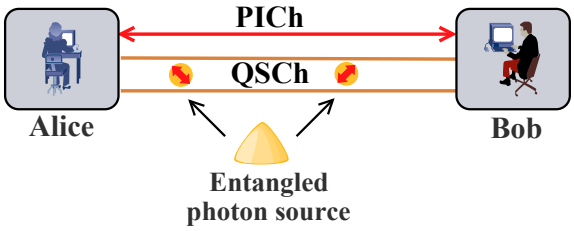


Fig. 6: Concept of entanglement-based scheme [110]

(b) QKD protocol families: The QKD protocols belong to one of the following three families, namely, discrete-variable (DV)-QKD protocols, continuous-variable (CV)-QKD protocols, and distributed-phase-reference (DPR)-QKD protocols [96].

(i) Discrete-Variable QKD Protocols: The DV-QKD protocols generate secret keys between Alice and Bob by using the polarization states of photon or phase to encode the bits. Such protocols utilize the photon counting and post-processing methods for the detection of individual

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2021.3106659, IEEE Open Journal of the Communications Society

TABLE I: Summary of QKD Protocols

Protocol Family	Name and Year of Protocol	Protocol Scheme	Principle	Unique Feature	Innovators and References
DV-QKD	BB84 (1984)	P & M	Heisenberg's uncertainty principle	The first quantum cryptography protocol, uses four polarization states of photon	C. H. Bennett and G. Brassard [13]
	E91 (1991)	EB	Quantum entanglement	The first QKD protocol based on the principle of quantum entanglement	A. Ekert [29]
	B92 (1992)	P & M	Heisenberg's uncertainty principle	Identical to the BB84, however, it uses only two non-orthogonal states	C. H. Bennett [30]
	BBM92 (1992)	EB	Quantum entanglement	The BBM92 protocol is the entangled version of BB84 protocol	C. H. Bennett, G. Brassard, and N. D. Mermin [31]
	SSP (1998 & 1999)	P & M	Heisenberg's uncertainty principle	This protocol uses higher number of polarization states of photon (i.e., six) as compared to the BB84 protocol	D. Bruß [32] and H.B-Pasquinucci and N. Gisin[33]
	SARG04 (2004)	P & M	Heisenberg's uncertainty principle	Only the classical phase of SARG04 is different than the BB84 protocol	V. Scarani, A. Acin, G. Ribordy, and N. Gisin [34]
CV-QKD	Discrete modulation protocol (Squeezed-state BB84 (2000))	P & M	Heisenberg's uncertainty principle	A new version of BB84 protocol with the squeezed-state and discrete modulation	M. Hillery [111]
	Gaussian protocol (Squeezed-state BB84 (2001))	P & M	Heisenberg's uncertainty principle	The squeezed-state based BB84 protocol with the Gaussian modulation	N. J. Cerf, M. Levy, G. Van Assche [112]
DPR-QKD	DPS (2003)	P & M	Heisenberg's uncertainty principle	The first DPR based QKD protocol that uses weak coherent sources, and one bit delay circuit to generate, and measure qubits, respectively	K. Inoue, E. Waks, and Y. Yamamoto [36], [37]
	COW (2004)	P & M	Heisenberg's uncertainty principle	The COW protocol uses weak coherent pulses for photon generation and each bit is encoded in a sequence of one non-empty (μ)-pulses (containing the mean number of photons) and one empty (0)-pulses	N. Gisin, G. Ribordy, H. Zbinden, D. Stucki, N. Burnner, and V. Scarani [109]

photons to generate the secret keys [96]. The first protocol of this family is the BB84 protocol [13].

(ii) Continuous-Variable QKD Protocols About fifteen years after implementation of the first DV-QKD protocol, an alternative approach, namely, the continuous-variable coding, was introduced by Ralph for secure data transmission [35]. DV-QKD protocols require single photon sources and detectors for implementation. However, CV-QKD protocol uses standard telecommunication devices, such as positive-intrinsic-negative (PIN) photo-diode. The major difference between the DV-QKD and CV-QKD protocol lies in their detection method. CV-QKD protocols replaced the photon counting approach of discrete-variable coding with a coherent detection method, i.e., homodyne detection, which is highly efficient, cost-effective, and fast. The first squeezed-state category of BB84 protocol [111], [112], [113] with the discrete and Gaussian modulation was implemented by Hillery [111] and Cerf et al. [112], respectively. Later, experimental demonstrations of various CV-QKD protocols were done to check the practicality of these protocols with the coherent states of light [114], [115], [116], [117], [118], [119], [120].

(iii) Distributed-Phase Reference QKD Protocols: The QKD protocols of this family include DPS-QKD [36], [37], [121] and coherent-one way (COW) protocol [96], [109] which have been developed recently. In DPR-QKD protocols, a sequence of coherent states of weak laser pulses is transmitted from Alice to Bob. In the DPS-QKD protocol, the intensity of the pulses is same; however, their phases modulate. In COW protocol, the phases of all the pulses are same; however, their intensities vary. Table I summarizes all the aforementioned QKD protocols.

3) Basic process of a QKD system

Fig. 4 shows the components of a QKD system [105] and the process of secure information exchange, as described below.

- A secret key is generated and shared between the Alice and the Bob using a QKD protocol. The process of secret key generation using BB84 protocol [13], [28] is described below.
- After secret key generation, the encryption block encrypts information using some conventional encryption algorithms [26], [27], [105]. The encrypted information is known as ciphertext, which is then transmitted by Alice.
- Bob uses the same secret key to decrypt the ciphertext to recover the original information, i.e., convert the ciphertext into plaintext [25].

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2021.3106659, IEEE Open Journal of the Communications Society

(a) Process of secret key generation using BB84 Protocol: The BB84 protocol [13], [28] is based on the basic principles of quantum mechanics and is provably secure. For the generation of photons, the BB84 protocol uses pulses of polarized light, where each pulse contains single photon. Single photon is generated by using a single-photon source which reduces the adverse effects of photon number splitting (PNS) attack [122], [123], [124]. The BB84 protocol uses two bases, namely, a rectilinear basis (R) with two polarization states of photons ($0°$ and $90°$) and a diagonal basis (D) with two polarization states of photons ($45°$ and $135°$), as shown in Fig. 7.

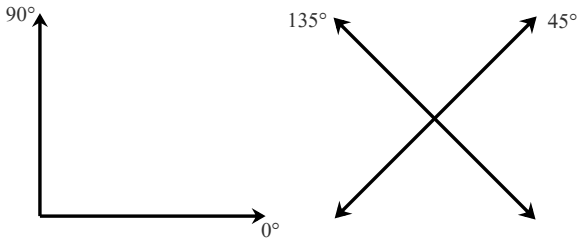


Fig. 7: Photon polarization states in BB84 protocol (R&D bases) [28]

Fig. 8 shows the bit encoding in BB84 protocol according to the original BB84 protocol proposed in [13]. Here, binary 0 is represented by $0°$ or horizontal (H) polarization state in R or a $45°$ polarization state in D. Similarly, binary 1 is represented by a $90°$ or vertical (V) polarization state in R or $135°$ polarization state in D [28]. Table II shows the polarization bases, polarization states, and bit encoding in the BB84 protocol.

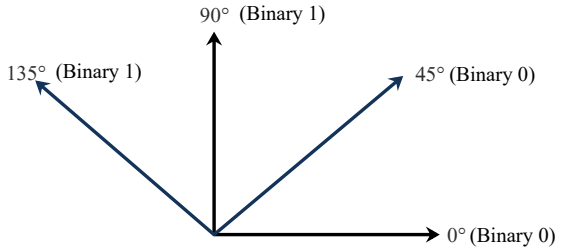


Fig. 8: Bit encoding in BB84 protocol [28]

TABLE II: Polarization bases, states, and bit encoding in BB84 protocol [28]

Polarization basis	Polarization state	Bit Encoding
Rectilinear (+)	$0°$ or H	Binary 0
	$90°$ or V	Binary 1
Diagonal ($\times$)	$45°$	Binary 0
	$135°$	Binary 1

The process of a QKD system is explained in the following phases below. Table III describes the operations involved in different phases with an example as discussed in [13], [28]:

- Quantum Phase: In the quantum phase, Alice communicates with Bob over the quantum channel in the following steps [108]:
  - Alice generates a random string of bits, and for each bit, she choose a measuring basis randomly, either R or D. The random string of bits along with the polarization states, i.e., the string of qubits is then sent to Bob through the quantum channel.
  - Bob also chooses a measuring basis randomly for each of the received qubit, and using the chosen basis, it starts to measure the received bits. For a bit, if the measuring bases of Alice and Bob match, it results in a perfectly correlated result, otherwise, an uncorrelated result. Sometimes, due to errors in detection and/or transmission, Bob does not register anything (as shown by blank entry from 5^{th} row onwards in Table III).
  - After measurement of all the bits, Bob records a string of all the received bits, called as *Raw key (K_{raw})* [14].
- Classical Phase: In the classical phase, Alice communicates with Bob over the classical channel to extract secret keys from the measurement results. The secret key extraction process, as shown in Fig. 9 involves of the following steps [25], [107], [125]:
  - Sifting: In this step, Alice and Bob exchange the information related to the sent/received photons over the classical channel. The random measuring bases chosen by Alice and Bob are compared: the bits corresponding to the same bases are kept, and the bits corresponding to different measuring bases are discarded. The remaining string of bits is known as the *sifted key (K_{sifted})* [14], [126].
  - Error estimation: In order to avoid eavesdropping, Alice and Bob decide a threshold value of quantum bit error rate ($QBER_{th}$), when there is no eavesdropper (Eve) on the communication medium. *QBER* is the ratio of the probability of getting wrong detection to the total probability of detection. Based on that value, they compare a random subset of K_{sifted} bits and calculate the estimated $QBER_{est}$. If $QBER_{est} > QBER_{th}$, the process is terminated and restarted, otherwise continued. [105], [125].
  - Error reconciliation or error correction: This step is used to further remove any chance of error occurred during the sifting process. Different methods of error reconciliation are used to enhance the capability of error correction in the QKD protocols [108]. After this process, the generated key is known as *corrected key ($K_{corrected}$)*
  - Privacy amplification: Privacy amplification is an important step in this phase, which reduces the information of secret key to a negligible amount against an unauthenticated user and produces a new shorter key using the universal hash functions. The generated final key is known as the *Secret key (K_{final})* [107], [125]. Additionally, an authentication process is required to ensure safety of the generated secret key from eavesdropping [14].

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2021.3106659, IEEE Open Journal of the Communications Society

TABLE III: Example of BB84 protocol process [28]

Alice's random bits	1	1	0	1	0	0	1	1	0	1	0	0
Alice's measuring bases	+	×	×	+	+	×	+	×	×	+	+	×
Photon polarization states	V	135°	45°	V	H	45°	V	135°	45°	V	H	45°
Bob's measuring bases	+	+	+	+	+	×	+	+	×	×	+	×
Bob's bits (Raw key)	1	0	0	1	0	0	1		0		0	0
Bob send his measuring bases to Alice	+	+	+	+	+	×	+		×		+	×
Alice confirm the measuring bases	T	F	F	T	T	T	T		T		T	T
Sifted key	1			1	0	0	1		0		0	0
Bob reveals some bits at random				1		0						
Alice confirm the bits				OK		OK						
Secret key	1				0		1		0		0	0

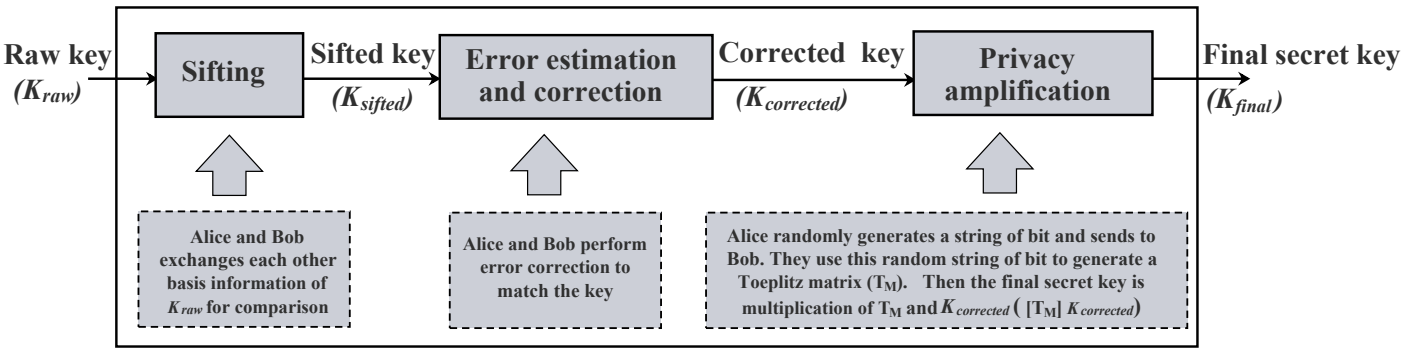


Fig. 9: Post-processing procedure

- Encryption Phase: In this phase, the generated secret key is then used for encryption and decryption of sensitive information between two legitimate end-users. This phase utilizes the one-time pad encryption [26] and symmetric encryption algorithm, i.e., AES [27] to encrypt and decrypt the data, and establish secure communication between the end-users [105], [127].

C. Quantum hacking attacks and their prevention strategies

In this subsection, some of the significant and vulnerable quantum hacking attacks or side-channel attacks at both the source and detector sides are discussed [122], [128], [129]. These attacks can be made in the QKD systems during the secret key generation. The security of QKD systems can be affected by such attacks if the devices at user-ends are imperfect. The practically realizable methods to prevent QKD protocols [41],[44] from side-channels attacks are also discussed.

1) Source side attack and its prevention

(a) Source side attack: BB84 protocol [13], [28] has been widely used to generate secret keys for practical QKD systems, however, this QKD protocol uses single-photon devices (source/detector) at the sender and the receiver side [108]. In practice, it is difficult to design a perfect single-photon transmitter or receiver. Thus, due to device imperfections, side-channel attacks can affect the QKD systems [38], [40]. The most vulnerable attack at the source side is the PNS attack [122], [130]. The PNS attack occurs due to the use of a weak coherent source instead of a single-photon source [131]. For example, when Alice sends single photon to Bob, multiple photons get transmitted instead of single photon due to device imperfections. In the PNS attack, the eavesdropper first measures the number of photons of each transmitted pulse. When s/he notices that multiple photons are being transmitted simultaneously, s/he splits the photons, otherwise, s/he blocks the transmitted pulse. After splitting the photons, the eavesdropper stores one photon and pass the other photons to the Bob via a lossless channel, as shown in Fig. 10. In order to get the complete information of secret key, the eavesdropper listens to the PICh for Alice's and Bob's bases announcement. Once eavesdropper knows the Alice's and Bob's information related to basis measurement, s/he can get the complete information of the secret key by measuring each of the stored photons in the correct measurement basis. In this way, the eavesdropper can perform the PNS attack, without letting either of the Alice or the Bob realizing the attack.

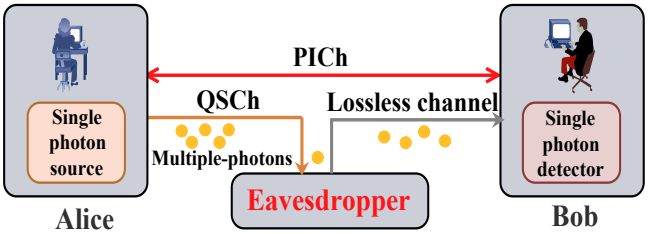


Fig. 10: PNS attack [130]

(b) Decoy-State QKD method To prevent the QKD systems

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2021.3106659, IEEE Open Journal of the Communications Society

from the PNS attacks, a decoy-state method was proposed [41]. This method allows the use of weak laser sources by creating the additional states, known as the decoy states, in place of single-photon sources. In the decoy-state method [39], [130], [132], [133], the sender chooses the intensity for every transmitted pulse at random from a set of available intensities, and reduces the effect of multi-photon transmission (PNS attack). Out of all the available intensities, one corresponds to the signal states (used for secret key generation) and the rest to the decoy states (having different intensity levels than main signal) [25], [42], [43], [134], [135]. After the announcement of Bob that he has received all the transmitted pulses, Alice announces the intensity level used for each transmitted pulse and estimates the *QBER* and yield (it is the conditional probability that the signal will be detected by Bob (the receiver), given that Alice (the sender) transmits it) of decoy states. By monitoring the *QBER* and yield, Alice and Bob can detect the presence of a PNS attack. The decoy states can be created by using variable optical attenuator (VOA) and intensity modulator (IM) [44], which changes the intensity of signals. The original BB84 protocol [13], [28] integrated with the decoy-state technique is known as the decoy-state BB84 protocol. The first experimental demonstration of decoy-state QKD over a 15 km fiber link achieved a secret key generation rate of 165 bps[132]. Various QKD protocols based on this technique have been experimentally implemented to detect the attacks on the source side [39], [133], [136], [137], [138], [139].

2) Detector side attacks and its prevention

(a) Detector side attacks Decoy-state method [41] secures the source side of the QKD system from the PNS attacks, however, this method cannot be applied at the detector side. Several quantum hacking attacks have been proposed and experimentally demonstrated in the literature [38], [128], [140], [141]. Some of the powerful attacks are the detector blinding attacks [129] and time-shift attacks [128], [142]. In the detector blinding attacks, an eavesdropper sends a bright light at the detector side and forces the detector to enter into the linear operation mode (in which detectors are more sensitive to light). The Eve randomly prepares his/her signal and sends a bright trigger pulse towards the Bob. If the measurement bases of Eve and Bob are same, then one of the detector produces a *click*, and the Eve can determine which detector produced the *click*. In this way, he/she can know the information of the secret key without any disturbance [129]. Since QKD protocol consists of at least two single-photon detectors for qubit detection, and the detection efficiency of both the detectors are time-dependent, the detectors may not have the same detection efficiency throughout. By taking advantage of this, Eve can shift the arrival time of each pulse and partially gain knowledge of the secret key without any error. Such type of attack is known as the time-shift attack [128], [142].

(b) Measurement-Device-Independent QKD method Various methods have been proposed to secure the QKD systems against device-imperfection based security loopholes. Some of the methods are slightly complicated [143], [144], and have extremely low key generation rate and transmission reach [145]. Hence, a new MDI-QKD scheme [44] was proposed that removes all the detector side-channel attacks. The initially proposed MDI-QKD relied on the single-photon source, and hence was susceptible the PNS attack [122]. However, the decoy-state method [41] was combined with MDI-QKD to prevent the QKD systems from the imperfect single-photon source based attacks [146], [147]. The idea of decoy-state MDI-QKD has a great importance in the QKD security against all types of device imperfection attacks. Moreover, it improves the transmission distance of quantum signals [46]. In the MDI-QKD method, Alice and Bob (sources) randomly prepare their measurement bases similar to that in the BB84 protocol, and send them to an untrusted node, i.e., Charles (at center) [44], as shown in Fig. 11. Charles performs measurement test on received bases, and after performing the measurement test, he announces the measurement outcome via the public channel. Alice and Bob keep the information of bits corresponding to the Charles's measurement results and discard the remaining. Charles's measurement results are only used to check the parity of both Alice's and Bob's bits, and it does not provide any information related to his/her bits. Similar to the BB84 protocol [13],[28], Alice and Bob perform a post-processing operation, i.e., Alice and Bob announce the randomly selected bases and compare them with Charles's measurement outcomes. At the end, either Alice or Bob performs the bit flip operation to achieve a guarantee correlation between the bit strings, and obtain the final secret key [44]. This method is called as MDI-QKD because the detector at the center has no information about the qubits, i.e., he/she does not know the bases and the polarization states used and to which party they belong. The process of MDI-QKD protocol and other aspects related to implementation, key generation rate, etc., are described in detail in [44], [142].

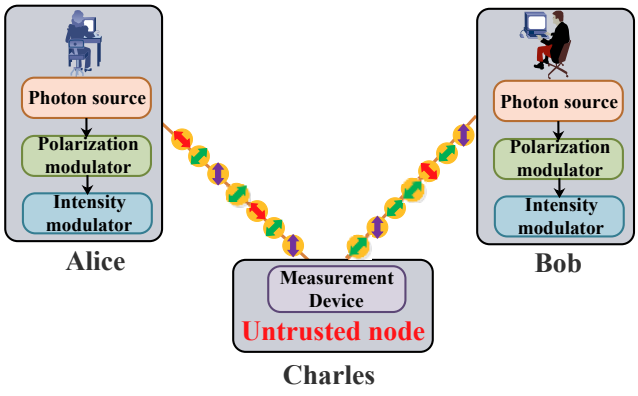


Fig. 11: Generalized MDI-QKD setup [44]

III. Point-to-Point QKD System over an Optical Fiber Link

This section describes the mechanism of secure communication over a point-to-point [148] optical fiber link using the BB84 QKD protocol. A basic point-to-point mechanism of QKD over optical fiber is shown in Fig. 12, as described

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2021.3106659, IEEE Open Journal of the Communications Society

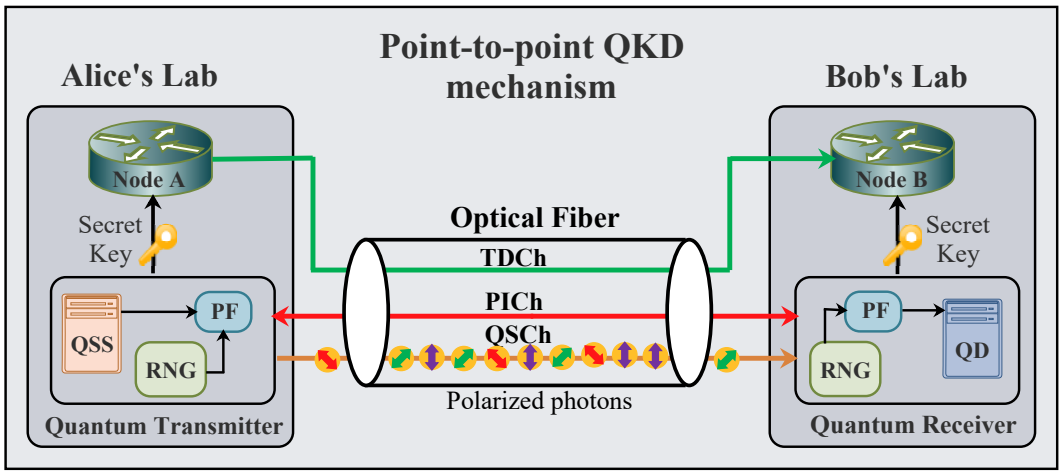


Fig. 12: Point-to-point QKD mechanism [12], [148]

in [12]. Here, Alice's lab consists of a quantum transmitter (quantum signal source (QSS), random number generator (RNG), and polarization filter (PF)) and Bob's lab consists of a quantum receiver (quantum detector (QD), RNG, and PF) [12]. QKD systems consist of various other components and the selection of such components depends on the QKD protocols being used. The steps involved in establishing secure communication between Alice and Bob in Fig. 12 are described as follows [24]:

- In the Alice's lab, the QSS transmits single photons [149] to the PF; and RNG generates random bits and sends them to the PF.
- The single photons are polarized with one of the four polarization states (H, V, 45°, 135°). The bits generated by RNG are encoded with the polarized single photons to obtain qubits.
- Alice sends the qubits to Bob through QSCh, and PICh is required for qubit synchronization between Alice and Bob.
- In Bob's lab, the quantum receiver receives and measures the qubits with randomly selected polarization bases.
- Alice and Bob exchange the measuring bases with each other via PICh and compare them. After comparison, the qubits with the same polarization bases are considered for secret key generation. The sequence of bits obtained after the comparison of bases constitutes the *sifted key*.
- Alice and Bob may not be sure about the correctness of the bits considered for the *sifted key*. Thus, to further ensure the correctness and to improve the safety, error-correction, privacy amplification, and authentication are performed via PICh. The remaining bits obtained after these processes (referred to as post-processing) constitute the *secret key* [125]. Alice uses the generated *secret key* to encrypt the classical data and transmits the encrypted data to Bob through TDCh. Bob uses the same key to decrypt the received data [24].

In the last step, for data encryption, conventional encryption methods, such as one-time pad and AES, are used, however, using the secret key that has been obtained using a QKD protocol via QSCh. A one-time pad encryption method was proposed in [26], however, Shannon [150] found that in this method, the key length has to be at least as long as the data size. Hence, this method is not suitable for high bit rate data encryption as it requires large storage and high execution time, which degrades the performance of the system. To overcome this, an AES algorithm [27] was proposed, where secret keys of different lengths, i.e., 128, 192, and 256 bits are used to encode and decode the data in blocks of 128 bits. AES algorithm can encrypt the data with smaller key size and low execution time [151], [152], however, it is less secure than the one-time pad encryption method [15].

Several experiments have been conducted over point-to-point optical fiber link to assess the performance of the QKD systems as well as to analyze the coexistence of classical and quantum signals in a common fiber. However, to integrate QKD over the existing optical networks, specifically, the backbone mesh optical networks, the existing network architectures need to be modified. Moreover, integration of QKD with the existing optical networks introduces new networking challenges for which the conventional methods (such as routing, resource allocation, network resilience) are not suitable. Thus, new methods need to be developed for the QKD secured optical networks. The network architectures proposed in the literature for QKD secured optical networks are described in the next section.

IV. Network Architectures of QKD Secured Optical Network

In this section, various network architectures of QKD secured optical networks are discussed in detail.

A. Basic Architecture

A basic network architecture of the QKD secured optical network is shown in Fig. 13. This architecture comprises of four planes, namely, application plane, control plane, QKD plane, and data plane [12], [24], [153].

- Application Plane: In the application plane, lightpath requests are generated which include (i) the lightpath

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2021.3106659, IEEE Open Journal of the Communications Society

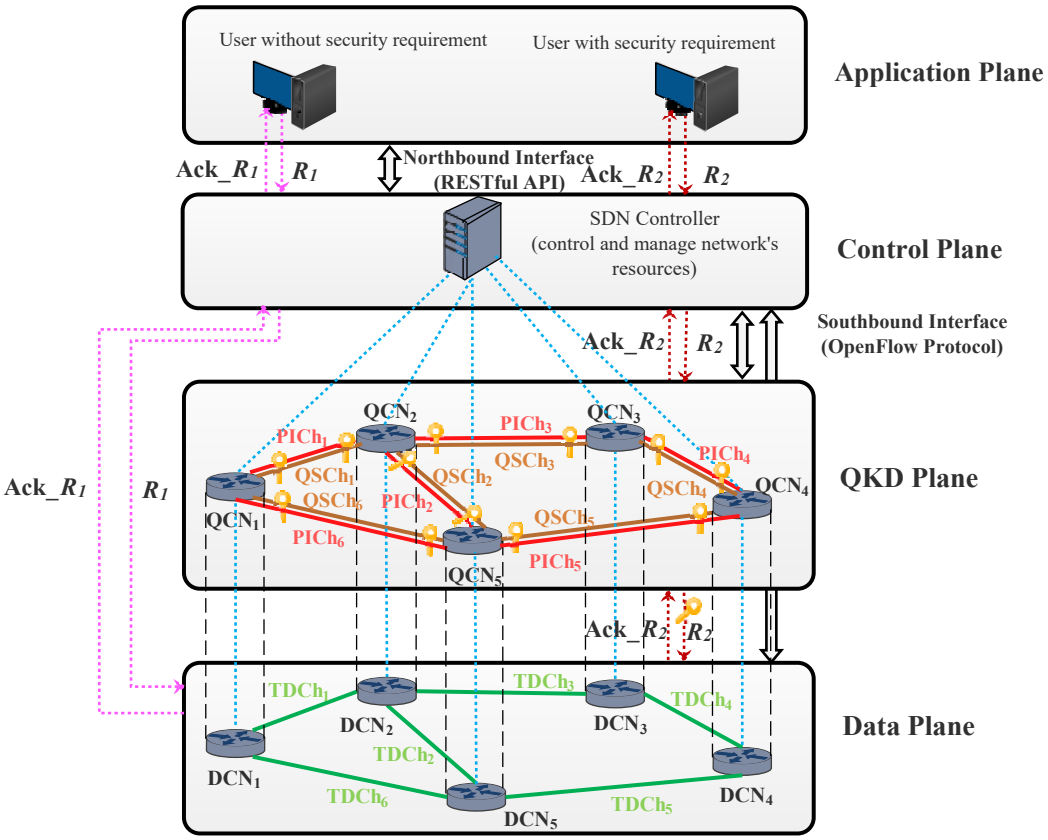


Fig. 13: Basic network architecture [12]

requests that require QKD security (hereafter referred to as QKD secured lightpath (QLP)), and (ii) the typical lightpath (LP) requests without QKD security. Both QLP and LP requests are then transferred to the control plane for further processing. The status of QLP and LP request acceptance/rejection is received at the application plane.

- Control Plane: The control plane consists of the software-defined networking (SDN) controller [154], [155], [156], [157], [158], [159], [160] that controls and manages the network resources. The control plane allocates resources to QLP, and LP requests from the QSCh, and TDCh in the QKD plane, and data plane, respectively.
- QKD plane: The QKD plane consists of quantum communication nodes (QCNs) and the connection among QCNs is established over QSCh and PICh. The implementation of QKD plane is dependent on the QKD protocol being used. The process of secret key generation between each node-pair of the QLP requests takes place in the QKD plane.
- Data plane: The LP requests are transferred to the data plane directly without the involvement of QKD plane and are assigned wavelength/frequency resources. The QLP requests are also assigned the wavelength/frequency resources in the data plane, however, the data to be transmitted over TDCh is encrypted (using the conventional encryption methods) by the secret keys generated at the QKD plane.

To establish communication among the four planes of the network architecture, different protocols are used. For implementing the southbound interface (between control plane and QKD/data plane), OpenFlow protocol (OFP) or Network Configuration (NETCONF) protocol can be used [161]. The southbound interface is used to transmit the control signals corresponding to the QLP, and LP requests from the SDN controller to the QKD plane, and data plane, respectively. The RESTful application program interface (API) is used to implement the northbound interface (between control plane and application plane) through which the properties (such as nodes, bit rate requirement, etc.) and status (acceptance, rejection, etc.) of LP and QLP requests are exchanged [12]. The process of serving LP and QLP requests is shown Fig. 13 for an LP request (R_1, shown in magenta) and a QLP request (R_2, shown in red). On receiving the LP request R_1 from the application plane, the control plane performs routing, and resource allocation from the TDCh, and sends the control directly to the data plane for transmitting the information using the chosen route and the allocated TDCh resources. For the QLP request R_2, the control plane configures the QKD plane to generate the secret keys among the QCNs, i.e., routing, and resource allocation from the QSCh and PICh takes place. It should be noted here that the routes chosen for establishing communication among the QCNs and the DCNs do not need to be the same. The control plane then sends the control to the data plane for encrypting the information to be transmitted using the secret keys generated at the QKD plane, and then transmit it over the chosen route

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2021.3106659, IEEE Open Journal of the Communications Society

and the allocated wavelength/frequency resources from the TDCh. For both the LP and QLP requests, the data plane acknowledges the control plane, where the status of network resources requests is updated accordingly, and the status of QLP/LP acceptance/rejection is forwarded to the application plane.

B. Quantum Key Pools (QKPs) based QKD secured Optical Network Architecture

An advanced architecture of QKD secured optical network has been proposed in [126], [127], where a concept of quantum key pool (QKP) has been devised to manage the secret key resources efficiently. QKP is used for storing the secret keys between each pair of QCNs in QKD network. In this architecture, two types of QKPs are constructed 1) between the SDN controller and each QCN in the network, i.e., QKP_1, QKP_2, QKP_3, QKP_4, and QKP_5 and 2) between the pair of QCNs (QCN_1 and QCN_2) in the network, i.e., $QKP_{1\text{-}2}$, as shown in Fig. 14 and Fig. 15. The network architecture with QKP is shown in Fig. 15 For QKP construction, the synchronized

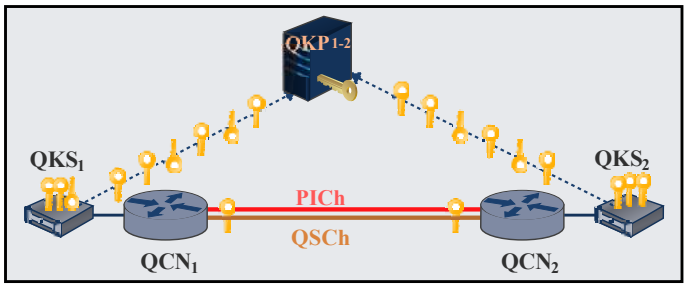


Fig. 14: An example of construction of QKP between QCN_1 and QCN_2 for provisioning of secret [127]

secret keys between various pairs of QCNs in the network are stored in the respective quantum secret key servers (QKSs) of QCNs. The stored synchronized secret keys between various pairs of QKSs can be virtualized into a respective QKP to provide the required secret key on-demand [127]. For example, as shown in Fig. 14, the synchronized secret keys between the QCN_1 and QCN_2 are stored in their respective QKSs, i.e., QKS_1 and QKS_2. The stored secret keys are then virtualized into a QKP, i.e., $QKP_{1\text{-}2}$, that provides the secret keys for data encryption/decryption on-demand based on the different security requirements.

The process of serving a QLP request (R_1, shown in magenta) is shown in Fig. 15. On receiving the QLP request R_1 (QCN_1/DCN_1 to QCN_2/DCN_2) from the application plane, the control plane first computes the path and then performs an OpenFlow handshake on a selected path with corresponding QKPs, i.e., QKP_1 and QKP_2. Then, the control plane configures QKP_1 and QKP_2 to provide secret keys for control messages through the control channel. The control plane then configures $QKP_{1\text{-}2}$ to provide secret keys for a QLP request from DCN_1 to DCN_2 via TDCh. The control plane then sends the control to the data plane for encrypting the information to be transmitted using the secret keys and then transmit it over the chosen route and the allocated wavelength/frequency resources from the TDCh. In the end, the control plane acknowledges the application plane.

C. Key as a Service (KaaS) based QKD secured Optical Network Architecture

Another architecture for QKD secured optical network with a concept of key as a service (KaaS) has been proposed in [162] to jointly solve the problem of efficient deployment and employment of secret keys. The KaaS concept refers to the provision of secret keys as a service to fulfill the security requirements of QLP requests in a timely and precise way. The point-to-point QKD mechanism of QKD-secured optical network with KaaS for securing communication between any pair of nodes is shown in Fig. 16 [162]. Here, the generated secret keys of QCN_1 and QCN_2 are stored in their respective QKS, i.e., QKS_1 and QKS_2. For data encryption/decryption between DCN_1 and DCN_2, the QKSs (QKS_1 and QKS_2) provide secret keys via TDCh. Each QLP request between DCN_1 and DCN_2 can demand any number of secret keys for data encryption/decryption. Therefore, in order to satisfy such requirements of QLP requests between any pair of nodes, secret keys can be provided as a service.

To implement the two functions of KaaS, i.e., employment and deployment of secret keys, two secret key virtualization steps (key pool (KP) assembly and virtual key pool (VKP) assembly) were introduced. In the KP assembly step, i.e., for the deployment of secret keys, the generated secret keys stored in each pair of QKSs (QKS_1 and QKS_2) can be virtualized into a KP ($KP_{1\text{-}2}$) to facilitate the efficient resource management of secret keys. In the VKP assembly step, i.e., for the employment of secret keys, a portion of generated secret keys in a $KP_{1\text{-}2}$ can be virtualized into a VKP ($VKP_{1\text{-}2\text{-}A}$ or $VKP_{1\text{-}2\text{-}B}$) to improve the security of dedicated QLP request ($VKP_{1\text{-}2\text{-}A}$ for QLP request-A and $VKP_{1\text{-}2\text{-}B}$ for QLP request-B) between any pair of DCNs via TDCh.

The KaaS based QKD secured optical network architecture is shown in Fig. 17. Here, on receiving the QLP requests (one (R_1) or more (R_2, R_3, R_4)) from users ($User_1$ and $User_2$) in the application plane, the control plane consisting of an SDN controller performs KaaS. The controller first selects a route and then performs a handshake on a selected path with relevant QCNs/QKSs and DCNs. The control plane configures the relevant QCNs/QKSs and DCNs for KaaS, i.e., for the deployment and employment of secret keys to fulfill the security requirements of each QLP request from the users.

D. QKD secured Optical Network Architecture with SDN and TRN for QKD as a Service (QaaS)

A new architecture of SDN for QKD as a service (QaaS), i.e., SDQaaS framework has been proposed in [163] to accomplish QaaS for multiple users over a QKD network infrastructure, as shown in Fig. 18. The concept of QaaS [164] is that multiple users can apply for different QLP requests in order to obtain their required secret key rates (SKRs) from the same network infrastructure. An example of QaaS to satisfy the SKR requirements of two users is shown in Fig. 19. Let us consider two QCNs (QCN_1 and QCN_3) and a TRN (TRN_2) between

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2021.3106659, IEEE Open Journal of the Communications Society

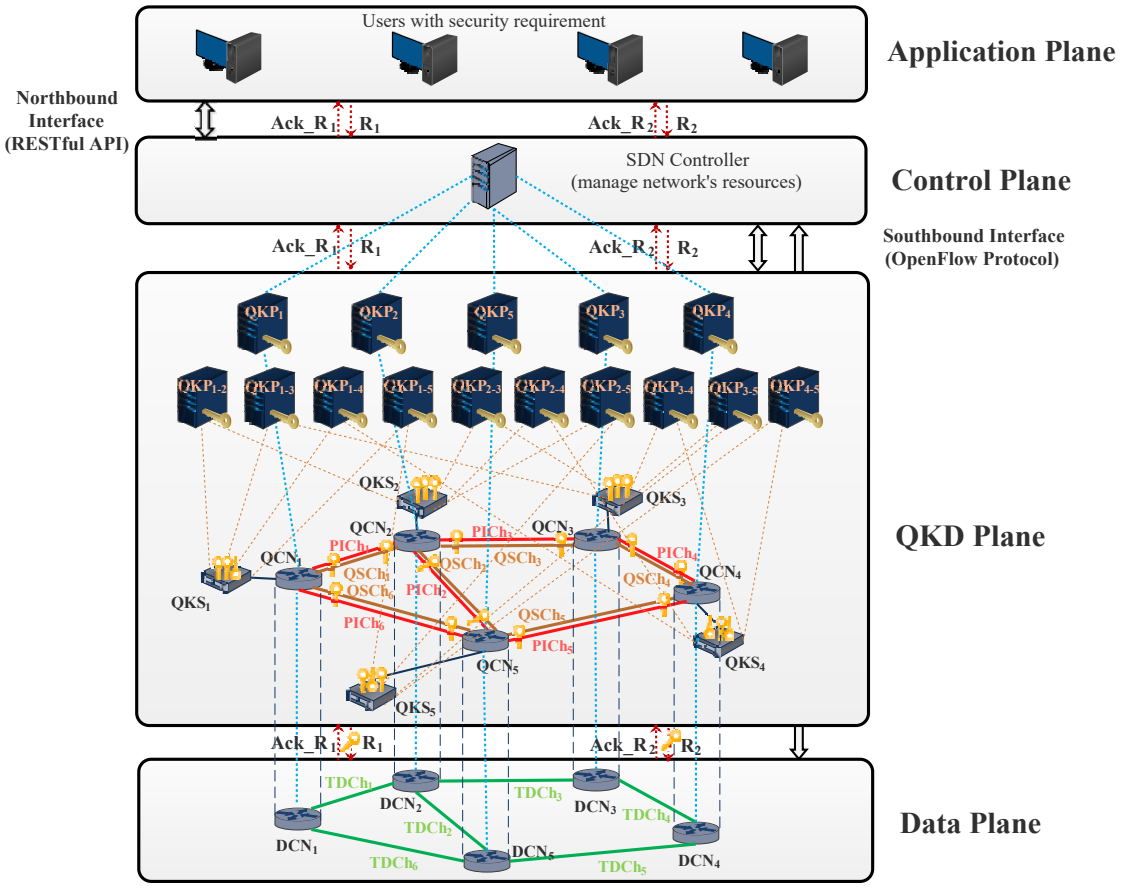


Fig. 15: QKD-secured optical network architecture with quantum key pools (QKPs) [127]

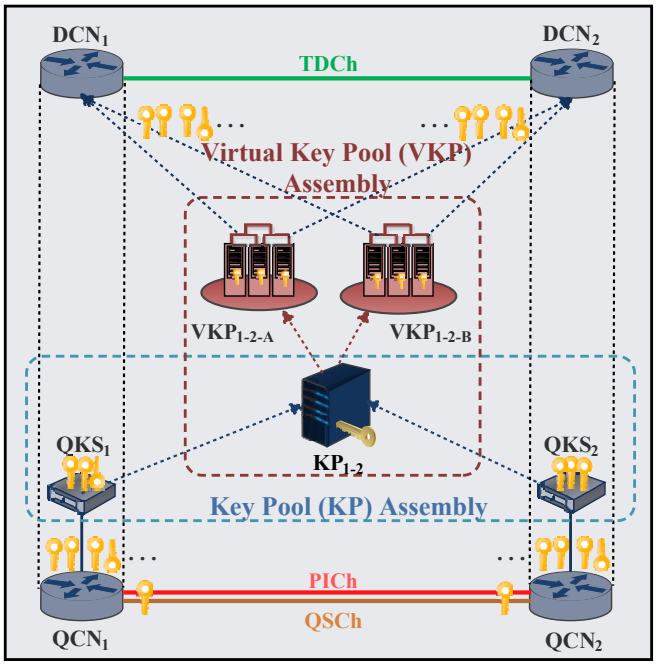


Fig. 16: Point-to-point QKD mechanism with two secret key virtualization steps for KaaS [162]

the two QCNs for long-distance secure communication. The point-to-point QKD mechanism is realized between the QCN_1 and TRN_2, and TRN_2 and QCN_3, respectively, and then on the quantum links (QLs), i.e., QL_1 and QL_2, different SKRs can be obtained, as shown in Fig. 19.

When a user ($User_1$ or $User_2$) requests a QLP to satisfy the required SKR between the QCN_1 and QCN_3, a path is computed between the source QCN (QCN_1) and destination QCN (QCN_2), i.e., QCN_1-TRN_2-QCN_3. Then, the required SKR of QLP request is examined for each user (e.g., $User_1$ requires 3 SKR, and $User_2$ requires 4 SKR). As per the user requirements, the available SKRs are searched on QL_1 and QL_2. If the available SKR on the QL can fulfill the SKR requirements of QLP request, the required SKR from the relevant QL is selected for this QLP request, otherwise, this QLP request is rejected. After SKR selection, TRN_2 uses the obtained secret keys (SKR_{1B} for $User_1$ and SKR_{2B} for $User_2$) on QL_2 to encrypt the obtained secret keys (SKR_{1A} for $User_1$ and SKR_{2A} for $User_2$) on QL_1. Then, TRN_2 relays the encrypted data from QCN_1 to QCN_3. To decrypt the corresponding original data, the QCN_3 can use the obtained secret key on QL_2 and can share the obtained secret key with QCN_1 on QL_1. In the end, the obtained secret keys based on SKR_{1A} (SKR_{2A}) are assigned to $User_1$ ($User_2$).

In this SDQaaS architecture, QaaS includes the creation, modification, and deletion of the QLP requests. On receiving a QLP request creation from the application plane, the control plane first computes and selects a route between the source

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2021.3106659, IEEE Open Journal of the Communications Society

QCN and the destination QCN. After route selection, the availability of SKR slots on each relevant QL is searched, and as per the user requirement, SKR slots are selected. If the available SKR slots can fulfill the SKR requirement of this

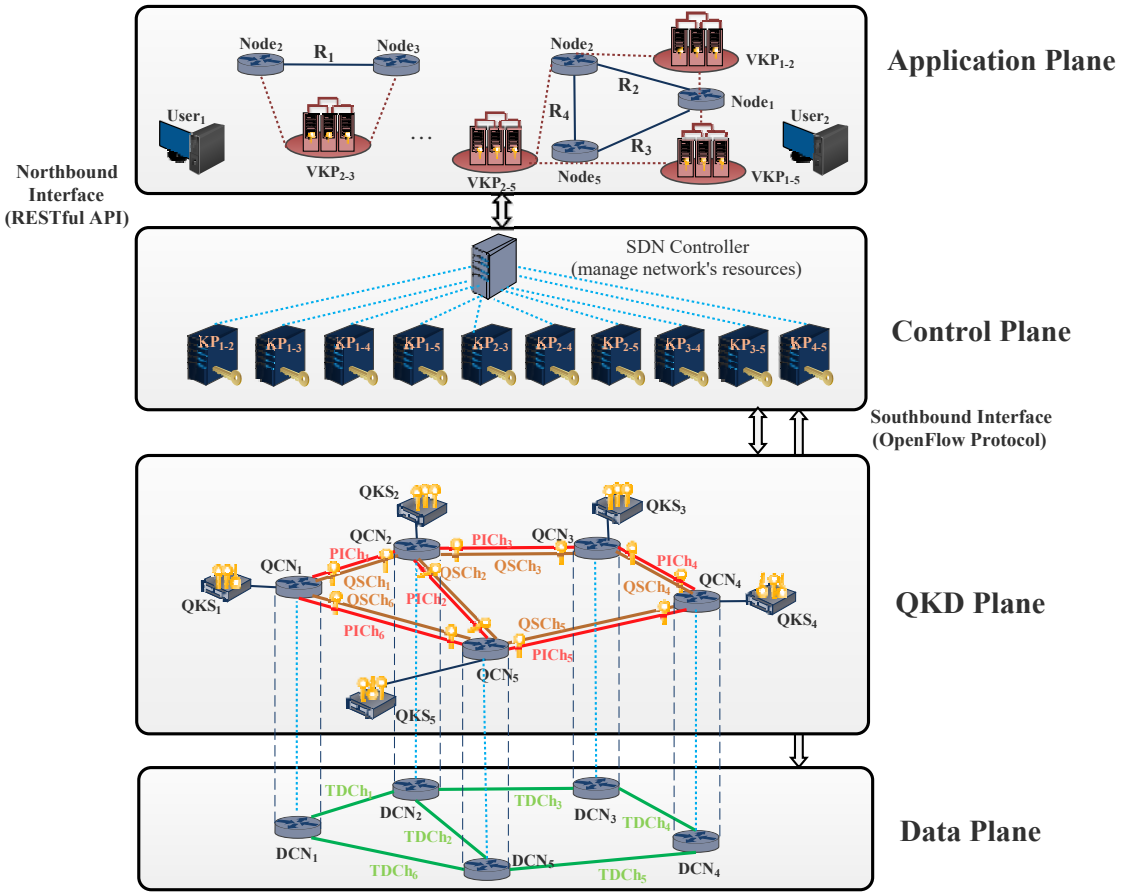


Fig. 17: QKD-secured optical network architecture with key as a service (KaaS) [162]

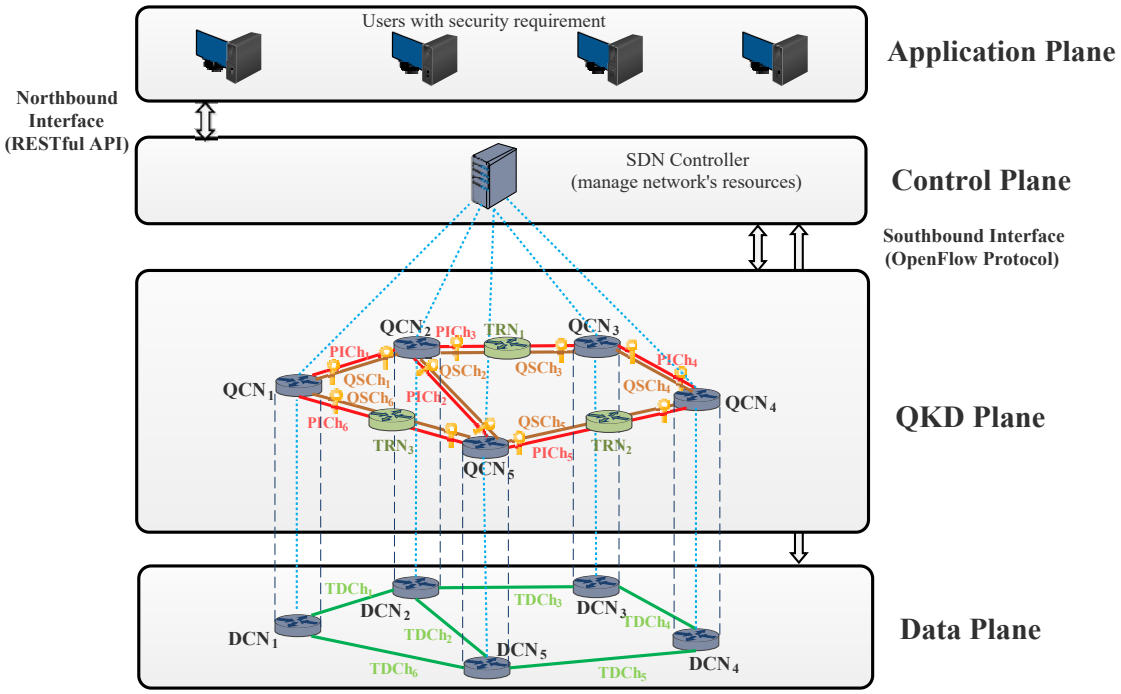


Fig. 18: QKD-secured optical network architecture with SDN and TRN for QKD as a service (QaaS) [163]

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2021.3106659, IEEE Open Journal of the Communications Society

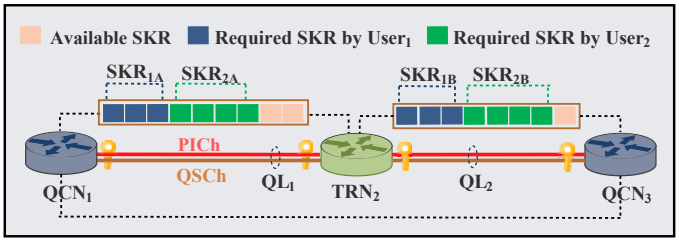


Fig. 19: An example of QaaS [163]

QLP request, the control plane configures the source QCN, TRN (intermediate node), and the destination QCN on the selected route for QLP request creation. Otherwise, the QLP request is rejected. For long-distance secure communication, TRNs can relay the secret keys from source QCN to destination QCN. On successful accomplishment of SKR assignment for QLP request creation, an acknowledgment is sent back to the application plane. Additionally, when the requirement of SKR slots of a user changes, the established QLP request for this user needs to change/update its SKR requirement. On receiving a QLP request modification, for SKR slot reassignment, the control plane performs the same task as discussed above (for SKR slot assignment). If the available SKR slots cannot satisfy the requirements of SKR slots for this QLP request, the QLP request is rejected. Furthermore, when the QLP request is expired, the application plane requests the deletion of this QLP request. On receiving the deletion request, the control plane configures the QCNs/TRNs to stop allocating SKR slots to this QLP request and erase the information of this QLP request.

E. QKD secured Optical Network Architecture with hybrid trusted/untrusted relay based QKD

A new QKD secured optical network architecture with hybrid trusted/untrusted relay based QKD has been introduced in [165], [166], as shown in Fig. 20 for the deployment of large-scale QKD. In this network architecture, three types of nodes are required, i.e., QCNs (act as the end nodes to provide secret keys to its co-located DCNs), TRNs, and the untrusted relay nodes (UTRNs) (act as the intermediated nodes between two QCNs). Fig. 21 illustrates the node structure of TRNs and UTRNs used in this network architecture. A TRN comprises two or more MDI-QKD transmitters (MDI-QTxs), a local key manager (LKM) (that receives, stores, and relays the secret keys), and the security infrastructure. An UTRN contains two or more MDI-QKD receivers (MDI-QRxs).

An example of a hybrid trusted/untrusted relay based QKD chain is shown in Fig. 21. In order to establish secure long-distance communication between two nodes (QCN_1 and QCN_2) using hybrid trusted/untrusted relay based QKD, a string of keys Q_{k1} is shared between QCN_1 and TRN_1, while another string of keys Q_{k2} is shared between TRN_1 and QCN_2. Additional interleaved TRNs/UTRNs can be added to further extend the transmission reach of QKD. In each TRN, the LKM can relay the secret key hop-by-hop along the hybrid QKD chain through a key management link (KML). For instance, in TRN_1, LKM combines Q_{k1} and Q_{k2} of the same string length using the OTP method and then sends $Q_{k1} \oplus Q_{k2}$ to the LKM in QCN_2 via KML. The LKM in QCN_2 can decrypt the key (Q_{k1}) based on Q_{k2} ($Q_{k1} \oplus Q_{k2}$). The LKMs of both the QCNs (QCN_1 and QCN_2) send Q_{k1} to their connected QKS. Hence, Q_{k1} is successfully shared between QCN_1 and QCN_2.

V. Networking Challenges in QKD secured Optical Networks and the Existing Methods

In this section, the new networking challenges that have been introduced due to the integration of QKD with the existing optical networks are described. Significant research has been done on the networking aspects of QKD secured WDM optical networks, and various methods have been proposed to address the networking challenges, as described below.

A. Routing, Wavelength and Time-Slot Assignment

In classical WDM networks, the available optical band is subdivided into a number of fixed wavelengths grids, and for each LP request, after defining a suitable route, wavelength is assigned. This problem is known as routing and wavelength assignment (RWA). However in the QKD secured optical networks, the available optical band is subdivided into QSCh, PICh, and TDCh, as shown in Fig. 1. The wavelengths reserved for TDCh are allocated to the LP/QLP requests for data transmission in the same way as that used for the classical optical networks. However, the wavelengths allocated for QSCh and PICh are utilized employing the optical time-division multiplexing (OTDM) scheme [12], [24]. For establishing QLP requests, after defining the route, wavelength is assigned on the TDCh, and time-slots are assigned on the QSCh/PICh. The modified problem in QKD secured optical networks is known as RWTA [167].

The wavelength resources are limited, and with the integration of QKD, the number of wavelengths available for the classical communication further reduces. Thus, it is necessary to utilize them efficiently such that maximum number of LP/QLP requests can be established with required security levels. Thus, resource (wavelength/time-slot) assignment [24], [168], [169], [170] for the three types of channels is an important problem in QKD secured optical networks [12]. Furthermore, currently, in most of the practical QKD networks, the secret key rate is only about $1 \sim 2$ Mbps for 50 km fiber link distance [63], [66], [127], [171]. The secret key resources (time-slots) are also limited, whose assignment/reassignment depend on the required security levels, and hence they should also be efficiently utilized for QLP requests using OTDM. OTDM is an optical multiplexing technique in which multiple lower bit-rate data streams are combined to form a high bit-rate data stream, and the multiplexed signals are transmitted, and then demultiplexed at the receiver in time-domain [172]. In QKD-secured optical networks, the reserved wavelengths for QSCh and PICh are subdivided into multiple time-slots using OTDM to share the network resources and utilize them efficiently [12], [24]. PICh can reserve the dedicated wavelengths or share the wavelengths with TDCh.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2021.3106659, IEEE Open Journal of the Communications Society

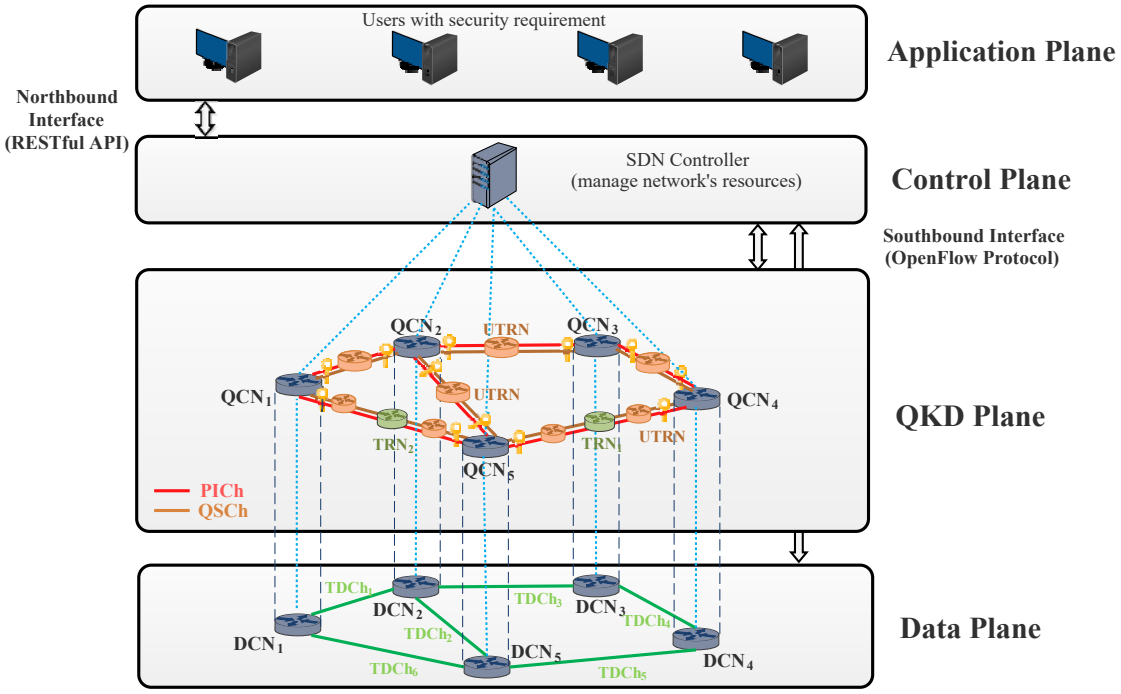


Fig. 20: QKD-secured optical network architecture with hybrid trusted/untrusted relay based QKD [165]

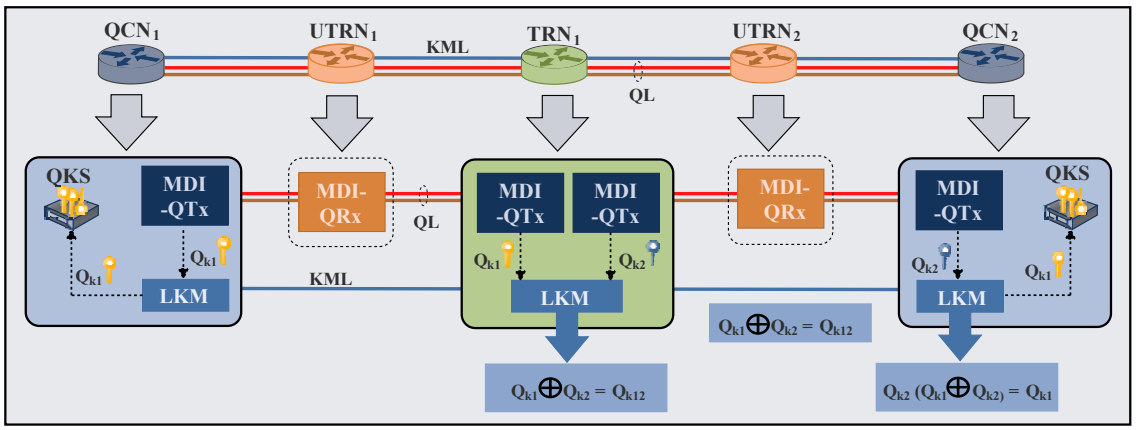


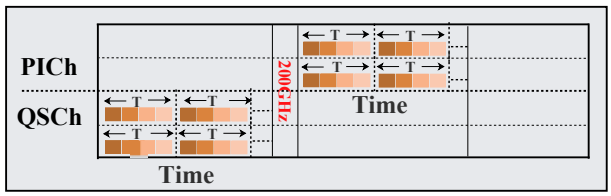
Fig. 21: An example of a hybrid trusted/untrusted relay QKD chain [165]

Various strategies have been proposed in the literature to solve the RWTA problem [173], [174], [175], [176], [177]. Initially, the RWTA problem was investigated in [12], and an RWTA strategy for resource allocation in a static traffic scenario was proposed. In a static traffic scenario, the set of connection requests is known in advance. An integer linear programming (ILP) model was developed and a heuristic algorithm to solve the resource assignment problem was proposed. To enhance the security level of QLPs, a concept of key updating period was introduced. In this, the secret key can be updated periodically for data encryption, thereby making it difficult for the Eve. Fig. 22 shows the time-slot assignment scenario for QLPs with two different security levels that are assigned different key updating periods (T). Fig. 22(a) shows the security-level scheme with fixed T, i.e., T is fixed (does not vary dynamically) and same for all the wavelengths reserved for QSCh and PICh. In the second scheme, as shown in Fig. 22(b), the value of T is fixed, however, it is different for different wavelengths. The security level in the first scheme is lower as compared to that of the second scheme because of fixed T (easier to be cracked). A new metric, referred to as service request security ratio (SRSR) was introduced, which is defined as the ratio of the service requests allocated with QSChs successfully to the total unblocked number of service requests [12].

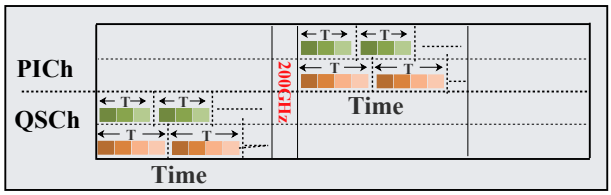
To improve the security level further, a new key updating period scheme with flexible T, i.e., T with some statistical distribution, was introduced in [24]. In this scheme, T is flexible and changes dynamically, thereby increasing the complexity to make it harder for an Eve to crack the key, and hence enhancing the security of the QLPs [178]. In case of dynamic traffic scenario, a time conflict problem arises during resource allocation due to the LP/QLP requests that arrive at the same time in the network. A concept of time-sliding window (TSW)

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2021.3106659, IEEE Open Journal of the Communications Society



(a) Fixed T



(b) Different fixed T

Fig. 22: Types of security levels [12]

was introduced to overcome this problem [24], however, a trade-off exists between the security-level and the resource utilization efficiency in QKD secured optical networks.

To maintain a balance between the security-level and the resource utilization efficiency, a new key on demand (KoD) strategy with the QKP construction technique over a software-defined optical network (SDON) was presented in [127] to secure the control channel (CCh) and the data channel (DCh). The KoD scheme with QKP assigns secret key resources on demand to the QLP requests. To perform KoD jointly for both the channels, a dynamic routing, wavelength and key assignment (RWKA) algorithm was developed. RWKA algorithm consists of three steps 1) routing and wavelength assignment (RWA) for DCh of each request; 2) key assignment (KA) for CCh of each request; 3) KA for requests via the DCh. Two cases were considered for key assignment in the RWKA problem, namely, key updating based on the time-complexity of the attacks, and key updating based on the data-complexity of the attacks.

To provision adequate secret keys over QKD secured optical networks, a time-scheduled scheme with QKP technique was introduced in [126]. In this scheme, the RWTA problem is solved by considering three sub-problems, namely, fixed/flexible secret key consumption, uniform/non-uniform time-slot allocation, and time-slot continuous/discrete QKP construction, for efficient QKP construction. An example of these sub-problems for RWTA in QKD-secured optical networks is shown in Fig. 23. In secret key consumption, the secret keys in different QKPs (e.g., $QKP_{1\text{-}2}$, $QKP_{1\text{-}3}$, and $QKP_{2\text{-}3}$) are constantly consumed, and may be fixed or flexible, depending on the security requirements of confidential information being transmitted between the QCNs (e.g., QCN_1, QCN_2, and QCN_3) in the network. In time-slot allocation, the number of time-slots allocated for different QKPs (e.g., $QKP_{1\text{-}2}$, $QKP_{1\text{-}3}$, and $QKP_{2\text{-}3}$) may be uniform or non-uniform depending on the security (secret key) requirements of QKP construction. For e.g., let us consider the different QKPs (e.g., $QKP_{1\text{-}2}$, $QKP_{1\text{-}3}$, and $QKP_{2\text{-}3}$) are constructed with the same security (secret key) requirement, and for each QKP construction, a uniform time slot (i.e., one time-slot) is allocated (t_1, t_4, and t_3 are allocated for $QKP_{1\text{-}2}$, $QKP_{1\text{-}3}$, and $QKP_{2\text{-}3}$, respectively, shown in Fig. 23 (the brown dash line)). In Fig. 23 (the green dash line), different QKPs (e.g. $QKP_{1\text{-}2}$, $QKP_{1\text{-}3}$, and $QKP_{2\text{-}3}$) are constructed with different security (secret key) requirements, and for each QKP construction, non-uniform time slots (i.e., three (t_1, t_2, t_3), three (t_1, t_3, t_5 on QL_1 and t_4, t_5, t_6 on QL_2), and two time-slots (t_2, t_4) for $QKP_{1\text{-}2}$, $QKP_{1\text{-}3}$, and $QKP_{2\text{-}3}$, respectively) are allocated. The construction of different QKPs may occupy continuous time-slots or discrete time-slots on the intermediate QLs between the two QCNs depending on QCN without/with secret key cache function. For instance, construction of $QKP_{1\text{-}3}$ depends on the construction of $QKP_{1\text{-}2}$ and $QKP_{2\text{-}3}$ with time slot t_4 on the intermediate QLs (QL_1 and QL_2), i.e., for continuous time-slot QKP construction time-slot continuity constraint should be followed. For discrete time-slot QKP construction, the time slot continuity constraint is not necessary. An example of discrete time-slot QKP construction is shown in Fig. 23, where the construction of $QKP_{1\text{-}3}$ depends on the construction of $QKP_{1\text{-}2}$ with time slot (t_1, t_3, t_5) on the intermediate QL_1 and $QKP_{2\text{-}3}$ with time slot (t_4, t_5, t_6) on the intermediate QL_2. Efficient deployment and employment of the secret keys are the two new challenges in such networks. To address these challenges, a concept of key as a service (KaaS) has been introduced in [162] with two secret-key virtualization steps, namely, KP assembly and VKP assembly (as discussed in Section IV.C).

Deployment of a dedicated QKD network for each high-security organization such as banking, finance, and intelligence is expensive. Hence, a multi-tenant QKD network was implemented in [179], [180] where multiple tenants can share a same QKD network infrastructure to satisfy their requirements. However, efficient and flexible provisioning of multiple-tenant over a QKD network is challenging. Generally, multi-tenant provisioning (MTP) can be divided into two problems, i.e., offline (static) MTP (Off-MTP), where tenant requests are known in advance, and online (dynamic) MTP (On-MTP), where tenant requests arrive without any prior knowledge. The Off-MTP problem was addressed in [179] to improve cost efficiency by sharing a QKD network infrastructure among multiple tenant requests. An SDN-enabled metropolitan area QKD network [181] architecture was introduced, and various multi-tenancy operations for establishing multi-tenant requests over the new architecture were experimentally demonstrated. In the laboratory, an experimental testbed was established for demonstrating a workflow, protocol extension, and an on-demand secret key resource allocation strategy for providing multi-tenant services. In QKD secured optical networks, the secret-key resources are limited. Thus, a SKR sharing scheme was presented in [179] for efficient multi-tenant secret-key assignment (MTKA). A new concept of QKD as a service (QaaS) was introduced in [163] (as discussed in Section IV.D) for multiple users to access their required SKRs from the same QKD network infrastructure. In this study, a new architecture of SDN for QaaS (SDQaaS) was developed (as discussed in Section IV.D). Additionally, the protocol extension and intercommunication workflow to create, update, and delete the QKD lightpath requests were presented; and a routing

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2021.3106659, IEEE Open Journal of the Communications Society

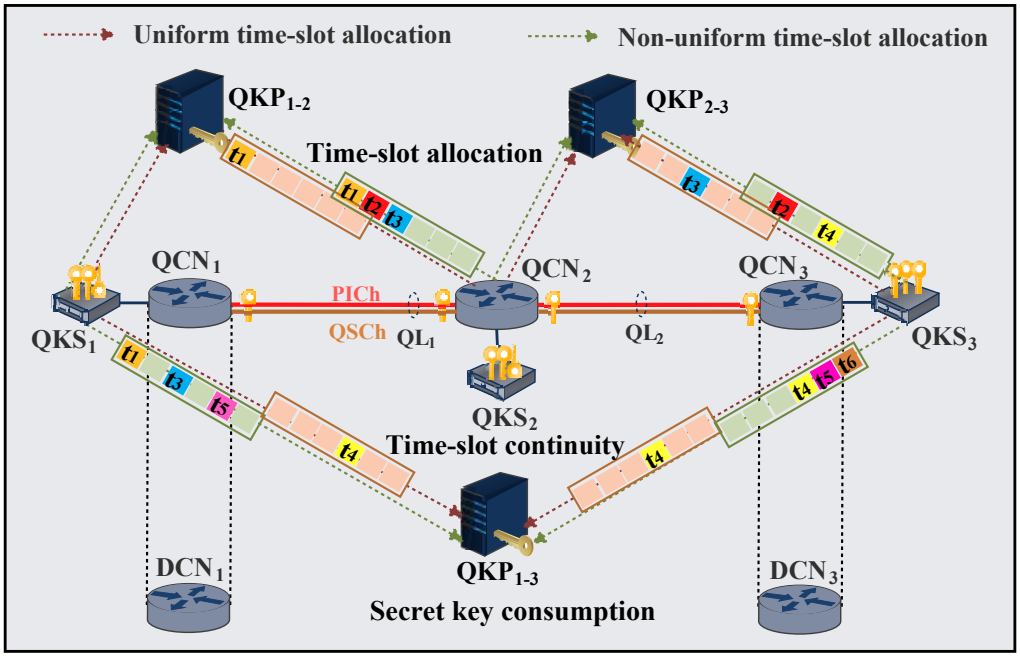


Fig. 23: An example of three sub-problems (fixed/flexible secret key consumption, uniform/non-uniform time-slot allocation, and time-slot continuous/discrete QKP construction) for RWTA [126]

and SKR assignment strategy for implementing QaaS was proposed. In [182], [183], an On-MTP problem was addressed, where the On-MTP includes the scheduling of multiple-tenant requests and assignment of non-reusable secret keys to multiple tenant requests. In [182], a reinforcement learning (RL)-based MTKA strategy was proposed for QKD secured optical networks. Moreover, to implement efficient On-MTP, a comparative analysis of heuristics and an RL-based On-MTP was performed to examine the efficiency of On-MTP [183]. Furthermore, in [184], a problem of efficient distribution of keys over metro-quantum optical networks (MQON) was addressed by designing a novel node structure (discussed in Section V.C). Based on this structure, two new RWTA schemes were proposed for MQON.

B. Resiliency in QKD secured Optical Networks

In the classical optical networks, a network component (node/link) failure causes LP failures or loss of data transmission. However, in QKD secured optical networks, in addition to the typical LP failures, a node/link failure can also affect the security of a working QLP. Moreover, large-scale failures [185] such as those caused by earthquakes, Tsunamis, weapons of mass destruction, etc., can severely compromise the security of QLPs along with the huge amount of data loss in QKD secured optical networks [186]. Therefore, network survivability is a bigger challenge in QKD secured optical networks. In the conventional optical network protection methods, the LPs are protected against failures by reserving alternate resources in advance as the backup resources. However, in QKD-secured optical networks, backup resources need to be reserved for both the LPs and QLPs on the TDCh, QSCh, and PICh. Thus, the existing network survivability strategies cannot be used for the QKD secured optical networks. To apply the existing network survivability strategies in the QKD secured optical networks, these strategies need to be modified as per the two unique characteristics of secret keys, i.e., the key updating process, and generation of sufficient secret keys for backup resources [186]. Fig. 24 explains the concept of survivability in such networks using an example 5-node optical network. Consider a QLP request generated between Node_1 (QCN_1/DCN_1) and Node_2 (QCN_2/DCN_2). For providing survivability (assuming dedicated path protection (DPP)), two paths, i.e., a primary and a backup path are required on both the QKD plane and the data plane. In this case, the primary path, and the backup path on both the planes is same, i.e., 1-2 and 1-5-2, respectively. In the event of link failure (suppose link 1-2), the same backup path can be used for secret key generation in the QKD plane and for data transmission in the data plane. However, if the primary paths on the QKD and data plane are different for a QLP request, and if only the primary path used in the QKP plane fails, the data transmission continues at the data plane with compromised security.

In [186], two new schemes were proposed for designing survivable QKD secured optical networks, namely, a key-volume adaptive dedicated protection scheme, and a key-volume adaptive shared protection scheme. These schemes protect the secret keys in the networks via the QSCh and PICh, and assume that the data services can be protected via the TDCh using the conventional survivability methods. To enhance the security level in the network, three key updating periods were considered. Since the key updating period increases the number of secret keys, hence the blocking probability increases because of the reduced available network resources at each updation. Thus, for a key-volume adaptive shared protection scheme, two key-protection thresholds are set for minimizing the blocking probability. The results show

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2021.3106659, IEEE Open Journal of the Communications Society

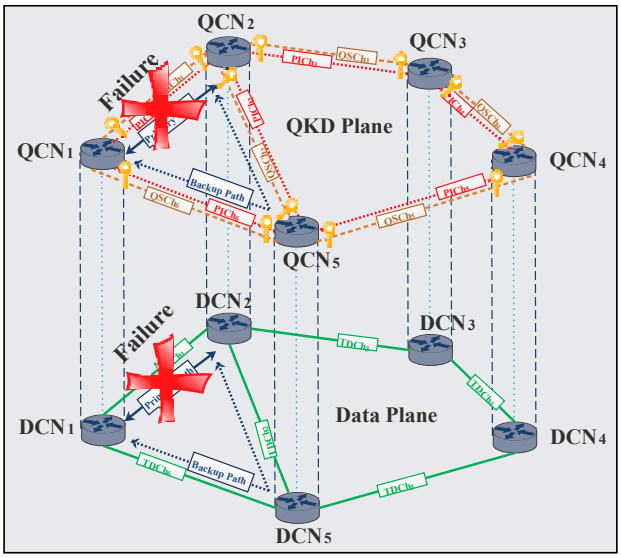


Fig. 24: Resiliency in optical networks integrated with QKD [186]

that a higher threshold value of key protection improves the survivability, and a smaller update period increases the security of the QLPs. Thus, a trade-off exists between the survivability and security of the network [186]. A model for failure affected and unaffected events, namely, the secret key flow model (SKFM), was developed in [187], [188]. In this model, a secret-key recovery strategy (SKRS) was proposed with three algorithms, namely, one path recovery method (OPRM), multi-path recovery method (MPRM), and time window-based recovery method (TWRM) to protect the failure-affected key provisioning services in QKD secured optical networks [188]. Moreover, in order to avoid disruption of information transmission between the nodes in event of failure a novel shared backup path protection (SBPP) scheme based on dynamic time window plane was proposed in TDM based QKD-secured optical networks [189].

In dynamic time window plane based SBPP algorithm, the concepts of time window (having a certain number of continuous time-slots) and time window plane (that reports the status of resource occupancy in the network), were introduced to satisfy the two main constraints needed to be considered during RWTA, namely, the time-slot continuity, and the time-slot consistency, respectively. In the existing backup QKD-secured optical networks, it is important to complete the resource allocation (wavelength and secret key allocation) process for both primary and backup paths. However, due to limited resources in the existing optical network, mixed/hybrid resource allocation is a challenging problem. Therefore, to solve the mixed/hybrid resource allocation problem, a new dynamic wavelength and key resource adjustment algorithm was proposed in [190]. The resource adjustment scheme includes three conditions: 1) If wavelength resources are enough while key resources exceed the threshold (i.e., resources are not enough to satisfy the requirements QLP request), adjust (increase) the storage volume of secret key, or if wavelength resources exceed the threshold while the key resources are enough, then reduce the storage volume of secret key. 2) If wavelength and key resources of QSCh and TDCh exceed the threshold, then add the wavelength of QSCh and TDCh, respectively. 3) In other conditions, no resource adjustment is required.

C. Trusted Repeater Node Placement

In QKD secured optical networks, the weak quantum signals have significantly shorter transmission reach as compared to that of the classical signals. Thus, to integrate QKD with the existing backbone optical networks having link distances ranging from hundreds to thousands of kilometers, several intermediate TRNs need to be placed to achieve long-distance transmission of the quantum signals among the nodes of the backbone optical networks. The TRNs need to be credible since they know the secret keys between various node pairs of the network [126]. Therefore, TRN placement is another important problem in the QKD secured optical networks [24],[126],[191].

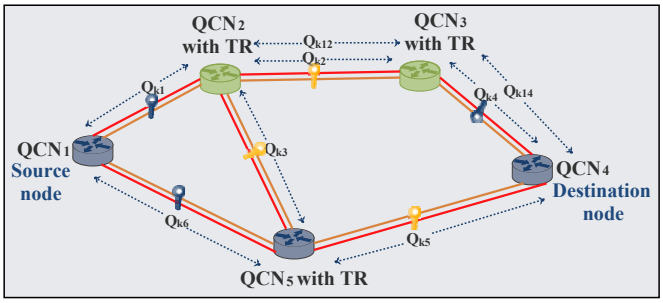


Fig. 25: Trusted repeaters for long-distance transmission [126]

Fig. 25 describes the process of key exchange between a source-destination node-pair through the TRNs, assuming three TRNs co-located at Node-2, Node-3, and Node-5. From source node (QCN_1) to destination node (QCN_4) on the path $QCN_1-QCN_2-QCN_3-QCN_4$, for each intermediate node pair, secret keys of same size, i.e., Q_{k1}, Q_{k2}, and Q_{k3} are generated. The secret key Q_{k1} is encrypted by Q_{k2} at the intermediate node QCN_2, and then the generated encrypted key Q_{k12} is transmitted to the next intermediate node QCN_3. The intermediate node QCN_3 uses secret key Q_{k2} for decryption, and obtains the Q_{k1} secret key. Now, the obtained secret key Q_{k1} at QCN_3 is encrypted by the secret key Q_{k4} at the node QCN_3, and the obtained encrypted key Q_{k14} is transmitted to the destination node QCN_4. Finally, the destination node obtains secret key Q_{k1}. Thus, even after multiple encryption and decryption processes at the intermediate nodes TRNs, the source and destination use the same key Q_{k1} for securing the QLPs. However, for the deployment of MQON, the placement of TRNs at each intermediate node is cost-inefficient. Since the distance between any two nodes in MQON is less, it results in the wastage of huge amount of secret key resources. Fig. 26 shows an example of the wastage of key resources. Therefore, the problem of distribution of secret keys over MQON with lower wastage of secret key resources is critical. This problem was addressed in [175], [184] by designing a novel quantum node structure with the ability of bypass

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2021.3106659, IEEE Open Journal of the Communications Society

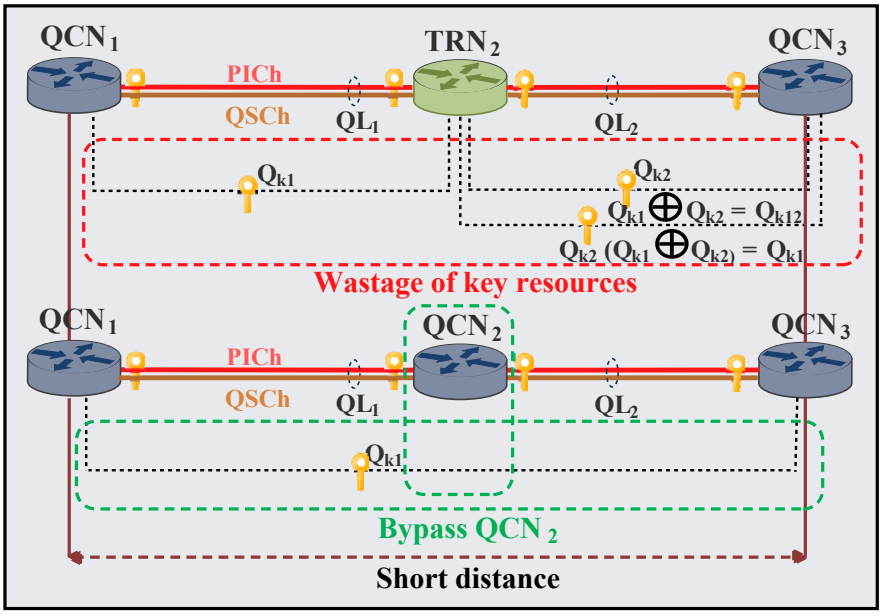


Fig. 26: An example of problem of wastage of key resources and new quantum node structure [184]

itself, if the distance between the two nodes in the network is within a certain range, as shown in Fig. 26. In addition to this, two new heuristic algorithms, namely full-bypassed based RWTA (FB-RWTA) algorithm and partial bypassed based RWTA (PB-RWTA) algorithm, were proposed based on this new node structure and auxiliary graph, in which some TRNs (intermediate nodes) can be bypassed in order to reduce the wastage of key resources [184]. In QKD secured optical networks, three different relay-based solutions are there for long-distance secure communication 1) Quantum repeaters based QKD (Quantum repeaters utilize quantum entanglement principle to create an entangled state between two nodes located at distant places for establishing a secure long-distance communication), 2) TRN based QKD (discussed in Section V.C), and 3) MDI-QKD (discussed in Section II.C.2(b)). However, these three relay-based solutions have their drawbacks. Quantum repeaters are still under development [193], intermediate nodes with the trusted repeaters should be credible because they know the secret-keys between the source node and destination node [126], and MDI-QKD has limitation of safety distance (still limited to ∼500km) [194], [195]. In order to solve the above problem, a new hybrid trusted/untrusted relay based QKD network architecture which consists of trusted relay and un-trusted relay (TRNs/UTRNs) was proposed in [165], [166], [196] (discussed in Section IV.E). In addition to this, four different mixed TRN/UTRN placement strategies were proposed in [166] to improve the security level for the deployment of QKD chain over an existing optical network. The cost optimization problem for the deployment of hybrid trusted/untrusted relay based QKD-secured optical networks was addressed [165]. In order to achieve a cost-optimized design of such a network, an ILP model and a cost-optimized QKD backbone networking algorithms were proposed. The problem of routing in QKD-secured optical network based on hybrid trusted/untrusted relay is a challenging issue. Recently, this problem was addressed in [196] by designing a collaborative routing algorithm.

D. QKD for Multicast Service Scenario

In a multicast service scenario, secure multicast services such as multi-site backup of data centers and video conferences require multicast technology to transmit confidential data from a single node (source node) to multiple nodes (destination nodes). However, QKD has mainly focused on the point(single source node)-to-point(single destination node) distribution of secret keys for establishing a secure connection. Therefore, the efficient distribution of secret keys for multicast services from a single source node to multiple destination nodes is a challenging problem. In order to address this problem a new node structure was designed to support point(single source node)-to-multipoint(multiple destination nodes) relay [176], [192]. An example of quantum key distribution for multicast services with a TRN is illustrated in Fig. 27. For simplicity, let us consider a secret key (Q_k) is distributed between a source QCN (QCN_1) and multiple destination QCNs (QCN_3, QCN_4, and QCN_5). QCN_2 between a QCN_1 and multiple QCNs acts as a TRN, and each node has its own KP to store the secret keys. In this scenario, Q_k is distributed separately through different paths (QCN_1-QCN_2-QCN_3, QCN_1-QCN_2-QCN_4, and QCN_1-QCN_2-QCN_5) from a source QCN to multiple destination QCNs. The steps to share a Q_k between QCN_1 and QCN_3 are as follows: 1) Q_k is encrypted by Q_{k1} obtained by KP and then decrypted at QCN_2, 2) Q_k is again encrypted by Q_{k2} and then decrypted at QCN_3. After multiple encryption/decryption, the Q_k is successfully shared between QCN_1 and QCN_3 by consuming two additional pair of keys. Similarly, Q_k is shared between QCN_1 and QCN_4, and QCN_1 and QCN_5. This process will consume additional pairs of keys (six), and out of six, three pairs of keys are consumed between QCN_1 and QCN_2. In

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2021.3106659, IEEE Open Journal of the Communications Society

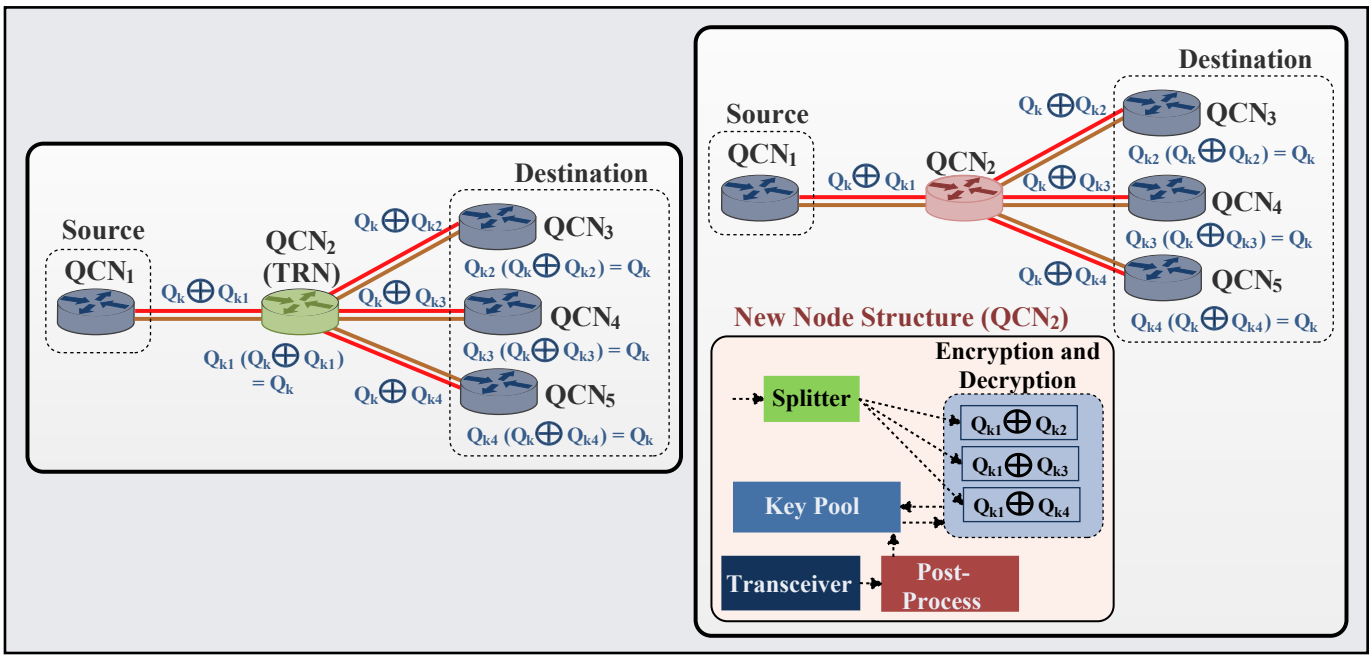


Fig. 27: An example of quantum key distribution for multicast services with a TRN and a MRN structure [192]

order to reduce the wastage of keys, a new node structure (multi-relay node (MRN)) was designed, as shown in Fig. 27 MRN consists of five modules 1) the transceiver module (send and receive quantum signals), 2) the post process module (processing optical-quantum signal), 3) the key pool module (storing keys), 4) the beam splitter (split a beam of light into multiple beams), and 5) the encryption and decryption module (for encryption/decryption). QCN_2 with new MRN, as shown in Fig. 27, follows the different operations: 1) The splitter process the encrypted data ($Q_k \oplus Q_{k1}$) coming from QCN_1, 2) From different KP, Q_{k1}, Q_{k2}, Q_{k3}, and Q_{k4} are taken out, and the Q_{k1} is encrypted with Q_{k2}, Q_{k3}, and Q_{k4} to get $Q_{k1} \oplus Q_{k2}$, $Q_{k1} \oplus Q_{k3}$, and $Q_{k1} \oplus Q_{k4}$, and 3) The encrypted data ($Q_k \oplus Q_{k1}$) coming from QCN_1 is again encrypted with $Q_{k1} \oplus Q_{k2}$, $Q_{k1} \oplus Q_{k3}$, and $Q_{k1} \oplus Q_{k4}$ to get $Q_k \oplus Q_{k2}$, $Q_k \oplus Q_{k3}$, and $Q_k \oplus Q_{k4}$. After this process, a Q_k is successfully shared between a source QCN_1 and multiple destination QCNs (QCN_3, QCN_4, and QCN_5) with less number of key pair, i.e., four, as compared to the conventional scheme with TRN. Furthermore, a novel key-relay-tree based routing and key assignment (KRT-RKA) scheme was designed based on the MRN node structure for efficient distribution of quantum keys as per the user demands in a multicast service scenario [192]. However, these two schemes, i.e., conventional scheme (key distribution with TRN), and KRT-RKA with MRN, have their drawbacks (explained with an example). An example of secret key distribution for multicast services using these schemes is illustrated in Fig. 28.

Let us consider the secret keys are distributed to destination QCNs (QCN_2, QCN_3, and QCN_5) using these scheme. In conventional distribution scheme, a secret key (Q_{k1}) is distributed separately through different routes (QCN_1-QCN_2 and QCN_1-QCN_2-QCN_3) from source QCN (QCN_1) to multiple destination QCNs (QCN_2 and QCN_3) (the detailed steps of this scheme is discussed above). This scheme will consume four keys, i.e., three keys from QCN_1 to QCN_2 and QCN_3, and one from QCN_4 to QCN_5, as shown in Fig. 28. In KRT-RKA with MRN capability (the detailed steps of this scheme is discussed above), will consume two keys from source QCN (QCN_1) to multiple destination QCNs (QCN_2 and QCN_3). However, in this scheme only a single source node (QCN_1) is used to distribute a secret key for multiple destination QCNs (QCN_2, QCN_3, and QCN_5), i.e., QCN_5 also has to obtain the secret key from the QCN_1. Thus, this scheme will consume more (five) secret keys and if distance between the source QCN (QCN_1) and destination node (QCN_5) is large, i.e., QCN_1-QCN_7-QCN_6-QCN_5, then the secret key between QCN_1 and QCN_5 is generated with some delay. In order to overcome the drawbacks of these schemes, a new distributed subkey-relay-tree based secure multicast (DSKRT-SM) scheme was propose in [197]. In this scheme, multiple source node (QCNs)

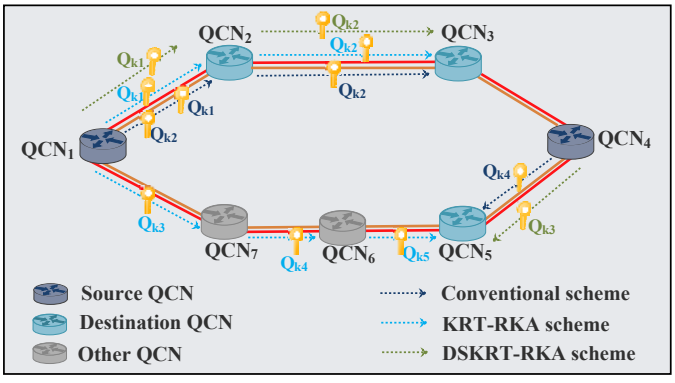


Fig. 28: An example of key distribution using the conventional scheme, KRT-RKA scheme, and DSKRT-RKA scheme

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2021.3106659, IEEE Open Journal of the Communications Society

are used to distribute the secret keys for multicast services. Additionally, this scheme uses the MRN node structure ability for efficient distribution of secret keys between any source QCN and destination QCN. An example of key distribution from source QCNs to destination QCNs using DSKRT-SM is shown in Fig. 28. Since this scheme has MRN capability, it will consume two keys from source QCN (QCN_1) to multiple destination QCNs (QCN_2 and QCN_3), as shown in Fig. 28. Also, this scheme allow QCN_5 to obtain the secret key from nearest source QCN (QCN_4) by finding the shortest path, hence reduces the consumption of keys between the QCNs, i.e., consume only one key. This scheme will consume less number of secret keys (three) as compared to other two key distribution schemes. Moreover, a novel distributed subkey-relay-tree-based secure multicast-routing and key assignment (DSKRT-RKA) algorithm was proposed based on DSKRT-SM scheme for efficient distribution of secret keys for multicast services [197].

E. Quantum Key Recycling

In QKD-secured optical networks, quantum keys are precious because the secret key rate is low. Therefore, to store, allocate, and manage quantum keys effectively, a novel concept of QKP was introduced. However, most of the research on QKP management in the QKD system focuses on the processing of quantum keys that are successfully relayed and not on the key-relay failure scenario. In this scenario, all the quantum keys included in the relay process for establishing secure long-distance communication between the end-users will be destroyed. This will result in the wastage of quantum keys. Fig. 29 explains the key-relay failure scenario, consisting

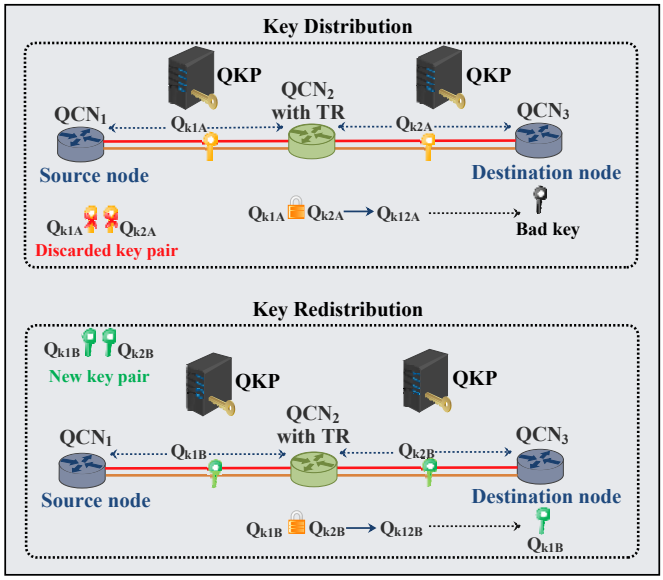


Fig. 29: An example of quantum key distribution and redistribution process [198]

of QCNs, TRNs, and QKPs (keys stored in respective QKP). Let us assume confidential information is transmitted between QCN_1 and QCN_3. A key Q_{K1A} is generated between QCN_1 and the first intermediate node or trusted node (QCN_2), and Q_{K2A} is generated between QCN_2 and QCN_3. If QCN_1 and QCN_3 want to share a key Q_{K1A}, then the secret quantum key Q_{K1A} is encrypted with Q_{K1B} at the intermediate node (QCN_2), and then the generated encrypted key Q_{K12A} is sent to QCN_3. However, because of packet loss and bit error, Q_{K1A} could not be successfully shared between QCN_1 and QCN_3. Therefore, in order to establish a secure connection between QCN_1 and QCN_3, a key redistribution process (similar to the key distribution process) is started by using a new pair of quantum keys (Q_{K1B} and Q_{K2B}), shown in Fig. 29. The key-relay failure may also be caused by an eavesdropper. Therefore, in order to ensure the security of keys (used only once), the old pair of quantum keys (Q_{K1A} and Q_{K2A}) must be discarded. Hence, this increases the wastage of quantum keys. Therefore, for reducing the wastage of quantum keys, a novel concept of quantum key recycling was proposed in [198] that focuses on the processing of failed keys. In [198] quantum key recycling mechanisms, namely, partial recycling, all recycling, and mixed recycling, have been proposed to increase the number of available keys in the QKD system for secure communication. These quantum key recycling and reusing strategies were designed to improve the key-recycling rate and reduce the wastage of quantum keys and QKD service blocking rate. However, few quantum key recycling mechanisms have been proposed till now. Therefore, strategies for quantum key recycling and reuse are required to increase the number of available keys. A summary of various networking challenges addressed in the existing works discussed above, is given in Table IV.

The QKD network test-beds developed and the practical implementations of QKD secured optical networks done since 2002 (as mentioned in Section I) involve the concepts and methods discussed in Section IV-V. The DARPA quantum network, built in 2003 in Boston, USA [69] established entanglement through optical fiber and also introduced the concept of trusted relays (discussed in Section IV.D and Section V.C) for extending the transmission distance [70]. Both the SECOQC quantum network (the European fiber-based quantum network), built in Vienna in 2008 [71], and the SwissQuantum QKD network (the longest-running QKD network installed in a Geneva metropolitan area in a real field environment [73]) used the trusted repeater architecture. The trusted repeaters based architecture and the process of key transmission through TRN are described in Section IV.D, and Section V.C, respectively. Experimental demonstration of the world's first secure TV conferencing was done over a distance of 45 km through GHz-clocked QKD links of the Tokyo QKD network, where six different QKD systems were combined into a mesh network [72]. This secure TV conferencing setup was also based on TRNs to extend the transmission distance. Demonstration of a wide area QKD network was done for more than 5000 hours from 2011 to 2012 in three cities of China, namely, Hefei, Chaohu, and Wuhu [204]. China started to build the longest QKD network over a distance of 2000km from Beijing to Shanghai based on trusted relay in 2013 and successfully established it in 2018 [15], [77], [206]. To circumvent the trust issues involved in the TRN based approach, an MDI-QKD (discussed in Section II.C.2(b)) based network was developed and demonstrated in a real field envi-

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2021.3106659, IEEE Open Journal of the Communications Society

TABLE IV: Summary of existing works that address various networking challenges in QKD-secured optical networks

Networking Challenge	Year, and Ref.	Description
RWTA	2017, [153]	Develops a QKD-secured optical network architecture with SDN, address RWTA problem, and develop a static RWTA strategy
	2017, [12]	Develops an ILP model and a heuristic for RWTA with two security-level providing solutions
	2017, [127]	Introduces a novel concept of KoD for efficient provisioning of network resources with QKP technique
	2017, [173]	Proposes a soft-reservation strategy to avoid time-conflict based on resource allocation
	2018, [178]	Develops RWTA algorithm with flexible key updation period in a dynamic traffic scenario and introduces the concept of TSW to reduce time conflicting
	2018, [126]	Proposes a new time-scheduled scheme to assign resources efficiently for three types of channels with QKP technique
	2018, [199]	Proposes a secret key generation scheme to provide security in the physical layer based on feature extraction of the optical channel and experimentally verified the proposed scheme over 200 km fiber loop
	2019, [162]	Presents the concept of KaaS that provides sufficient secret keys in proper time to satisfy the lightpath requests
	2019, [175]	Proposes an auxiliary graph-based RWTA (AG-RWTA) algorithm to save quantum key resources
	2019, [176]	A new node structure was designed for the distribution of global quantum keys to secure multicast services
	2020, [192]	Proposes a novel KRT-RKA scheme based on the MRN node structure for efficient distribution of quantum keys as per the user demands in a multicast service scenario
	2020, [184]	Two RWTA schemes was designed based on auxiliary graph in MQON with new node structure
	2020, [197]	A novel distributed DSKRT-RKA algorithm was proposed based on DSKRT-SM scheme for efficient distribution of secret keys for multicast services
Multi tenant provisioning problem	2019, [163]	Introduces a new concept of QaaS and develop routing and SKR assignment strategy for multiple users
	2019, [179]	Develops a multi-tenant QKD network in which multiple users can use the same network infrastructure for securing their lightpath requests, proposes a MTKA strategy and experimentally verified the proposed strategy
	2019, [180]	Demonstrates the multi-tenant provisioning over SDN-based metropolitan area network and design an on-demand secret key resource allocation strategy for providing access to multiple users
	2019, [182] and 2020, [183]	The On-MTP problem was addressed and a heuristic and RL-based key assignment strategies were designed for QKD networks
Resiliency	2019, [186]	Focuses on protecting the secret keys against network failure and develop two new survivable schemes
	2019, [188]	A SKFM was constructed to design SKRS to strength the resiliency against failure in QKD network
	2019, [189]	A novel SBPP scheme based on dynamic time window plane was proposed in TDM based QKD-secured optical networks
	2020, [190]	A new dynamic wavelength and key resource adjustment algorithm was proposed to solve the mixed/hybrid resource allocation problem in the existing backup QKD-secured optical networks
Trusted repeater node placement, cost-minimized approach, and key recycling approach	2020, [184]	A novel quantum node structure with the ability of bypass was designed, if the distance between the two nodes in the network is within a certain range
	2020, [166], 2020, [196], and 2021, [165]	A new hybrid trusted/untrusted relay based QKD network architecture which consists of TRNs/UTRNs was proposed
	2019, [200]	The cost minimized problem was addressed, a novel cost-oriented model was constructed and a cost-efficient QKD networking algorithms were designed to solve the cost-minimized problem
	2020, [198]	Quantum key recycling mechanisms, namely, partial recycling, all recycling, and mixed recycling, were proposed to increase the number of available keys in the QKD system for secure communication

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2021.3106659, IEEE Open Journal of the Communications Society

TABLE V: Summary of practical demonstrations of QKD secured optical networks

Year and Ref.	Description
2005, [69]	Reports the status of the world's first quantum cryptography network supported by US DARPA
2009, [71]	Describes the SECOQC prototype of QKD network considering trusted repeater architecture for long-distance communication in Vienna in 2008
2009, [201]	Reports a practical realization of metropolitan QKD network without TRNs in Beijing
2009, [76]	Demonstrates a user-oriented hierarchical quantum network based on technique of TRN in Wuhu, China
2010, [202]	A metropolitan all-pass quantum communication network was successfully demonstrated in 2009 in China
2010, [203]and 2018,[61]	The successful demostration of the co-existence of quantum signal and classical signal using WDM in different cities in China
2010, [74]	A long-term performance analyses of QKD network over the existing regional optical network was conducted in the Durban in South Africa
2011, [73]	Reports the performance of SwissQuantum QKD network in the field environment in Geneva over a metropolitan area
2011, [72]	Demonstration of the quantum secure communication network in Tokyo by integrating six different QKD system into a mesh network
2014, [204]	A successful demonstration of wide area QKD network was conducted for more than 5000 hours from 2011 to 2012 in three cities, namely, Hefei-Chaohu-Wuhu, in China
2016, [45]	Demonstrates a MDI-QKD network in real field environment with three user nodes and one UTRN
2016, [46]	Demonstrates the MDI-QKD with decoy-state technique over ultra-low fiber link of 404 km with key rate of 3.2×10^{-4} bps
2016, [205]	The first commercial QKD network in South Korea was deployed in 2016
2016, [77], 2018, [15], and 2019,[206]	China started to build a longest QKD network over a distance of 2000km from Beijing to Shanghai in 2013 and successful established in 2018
2018, [51]	Experimental demonstration of longest conventional QKD over ultra-low loss fiber achieve 421 km with a secret key rate of 0.25 bps
2018, [85]	A TF-QKD scheme was designed and experimentally demonstrated to solve the rate-distance problem of secure QKD network

ronment in Hefei with three user nodes and one untrusted relay node [45]. Recently, the first entanglement-based multi-node quantum network [207] connecting three quantum processors has been demonstrated in Netherlands, which will be tested further outside the laboratory on the existing optical fiber infrastructure in the future. Several similar efforts are being made worldwide towards the realization of a quantum network that will interconnect countless quantum devices via quantum links in the future. A summary of the practical demonstrations of QKD secured optical networks done in various parts of the world, as discussed above, is given in Table V.

VI. Open Issues and Challenges

Quantum technology is fast evolving and is expected to impact all the communication and secure information systems. Significant research efforts are required at various levels to realize cost-effective global deployment of quantum technology including device-level research, design of new QKD protocols, enhancement of SKR and transmission distance of quantum signals, exploration of new use-cases of quantum technology, development of advanced network architectures, among others, that require interdisciplinary research. We highlight some of the crucial open issues and challenges from the networking perspective that are necessary to be addressed in near-future for integration of QKD with the next-generation optical networks. This section also provides directions for future research in QKD-secured optical networks.

A. Trusted Repeater Node Failure

Most of the existing works on QKD secured WDM optical networks consider TRNs for long-distance communication of quantum signals. The distance among TRNs need to be significantly lesser as compared to the distance among the nodes (ROADM/Optical cross-connect (OXC)) of optical network due to the low transmission reach of weak quantum signals. Thus, in a QKD secured WDM optical network, the number of TRNs will be much higher as compared to the conventional nodes (ROADM/OXC). Such dense deployment of TRNs in core networks require additional cost as well as it is vulnerable to multi-component (node/link) failures. TRN

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2021.3106659, IEEE Open Journal of the Communications Society

failures can affect the SKR and transmission distance as well as it requires development of new survivability schemes. To improve network resiliency, additional fiber might need to be deployed among the TRNs. The geographical placement of TRNs is another crucial aspect since the TRNs share the information of secret keys generated among the end users, as explained in Section V.C. Besides these issues, techno-economic analysis of other schemes that do not require TRNs, such as MDI-QKD and TF-QKD need to be done researched in detail for QKD secured optical networks as an alternative to TRN supported long-distance optical networks secured by QKD.

B. Integration of QKD with EON and multiband transmission

QKD is envisaged to coexist with the global classical optical networks in the future. Most of the work on QKD secured optical networks has been done considering the integration of QKD with the currently deployed WDM optical networks. However, the capacity of WDM optical networks is continuously falling short to accommodate the exponentially increasing bandwidth demands. EON has been proposed as a promising near-term solution to satisfy the increasing bandwidth demands by replacing the currently deployed WDM network technology [208], [209], [210], [211]. EON provides spectral flexibility and dynamicity that improves spectrum utilization, whereas, to further improve the capacity of optical networks, multiband transmission (including other optical bands along with the C-band) is being explored [212]. The spectral expansion and flexibility will provide new challenges for the integration of QKD with the future optical networks, especially, the effect of physical layer impairments and constraints that are necessary to be explored and considered in the networking studies.

C. QKD secured MCF networks

MCFs have been widely accepted as a long-term solution to the capacity crunch in the optical networks. Spectral and spatial expansion and flexibility will increase the capacity of optical networks manifold. Thus, to integrate QKD with the future optical networks, integration of QKD with MCF (or space division multiplexing (SDM)-EON) also need to be explored. Therefore, a bigger challenge lies ahead to investigate the new challenges that will be introduced with the integration of QKD with the next-generation optical network technologies. To this end, few experimental demonstrations have been done recently to analyze the feasibility of quantum-classical coexistence in MCFs. Here, a separate core can be assigned to the quantum signals and hence the available optical band does not need to be divided into QSCh, PICh, and TDCh. However, the presence of inter-core crosstalk (IC-XT) is the main factor of interference between the strong classical signals and the weak quantum signals [213], [214] that need to be addressed. Several other aspects including MCF types, structures, and regions of operation also need to be addressed [215], [216], [217] in the context of MCF networks integrated with QKD, especially, because the MCF technology is also immature currently.

D. Telecom-cloud/fog infrastructure supported by QKD secured optical networks

Optical networks play a major role in cloud computing/storage and act as a substrate for inter-datacenter networking. The quantum computing technology is in infancy and it is expected that at least initially, quantum computing will be provided as a service through the internet, where the users can utilize the quantum computing facilities from a distant co-located quantum computing and cloud datacenter facility, also referred to as quantum datacenter or quantum cloud. The information exchanged between the quantum cloud and the user may not be sensitive and hence might not require QKD secured communication. Conversely, the information to be stored/retrieved from the cloud might be confidential that might not require quantum computing but does need QKD secured communication. Thus, the integration of QKD with the future telecom-cloud/fog infrastructure introduces new networking challenges, especially, the heterogeneity of services, that need to be explored and addressed. Optical networks are also envisaged to enable fog computing and to support networking among the micro datacenters. Thus, with the development of cost-effective quantum computing technology, quantum fog may also be developed similarly for latency-sensitive applications that will introduce new research aspects for metro optical networks.

It may be noted here that in a quantum cloud infrastructure supported by optical network, the quantum computing facilities share the same network that will be used for classical communication (since all the services will not require QKD security). Thus, trust-models need to be developed among the quantum clouds sharing the optical network to ensure security of classical communication. Although telecom and inter-datacenter networking share the same optical network mostly, however, dedicated optical network for quantum cloud or quantum computing only might be deployed in future, for instance, Google's B4 inter-datacenter backbone network dedicated for only interconnecting their datacenters deployed worldwide. Thus, networking aspects with and without integrating cloud and telecom services with QKD also need to be explored.

E. Network topology

The existing core optical networks are mesh-connected and have link distances ranging from hundreds to thousands of kilometers. Several factors of the next-generation optical networks indicate a possible modification in the core optical network technology including wireless network densification (that will require more optical add/drop points per unit area), short reach of higher order modulation formats and MCFs, higher losses in non-C-band transmission, fog-computing/storage supported by optical networks, among others. In this case, a denser core optical network might need to be established, where the TRNs can be co-located with other network equipments and might emerge as a cost-effective solution that provides high SKR. Besides, a mesh inter-TRN optical network can improve the resiliency of QKD secured

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2021.3106659, IEEE Open Journal of the Communications Society

optical network. The topological aspects of QKD secured optical networks have not been addressed yet in the literature.

F. Migration strategies and techno-economic studies

As observed with any other past technology, a gradual migration of classical optical networks to QKD secured optical networks over a long period of time is expected. The services that require QKD are also expected to vary with time and cost. Hence, traffic profiles, traffic forecasting, and evolving network scenarios need to be considered for optimum migration planning. Migration strategies for WDM to EON and EON to SDM-EON have been developed in the literature [218], [219], [220], [221], [222], [223]. Here, both the greenfield and brownfield migration strategies have been developed, where it is ensured that the existing services should not be interrupted during migration. Similarly, gradual migration strategies for integration of QKD with EON, multiband transmission, and MCF networks need to be developed based on service level agreement (SLA) [224] models to conduct techno-economic analyses. Since the current and future technologies coexist during gradual migration, the coexistence of two or more of the WDM, EON, multiband transmission, SDM-EON, and QKD technologies is expected in a network architecture for which new networking algorithms also need to be designed.

G. Other applications and research directions

To address the above-mentioned open issues and networking challenges as well as to improve the performance of the existing approaches discussed in Section V, artificial intelligence (AI), machine learning (ML), deep learning (DL), and optimization methods can play a major role. ML techniques have been used for many communication network applications [225], [226] because they have capability to solve complex problems. Estimation of quality of transmission (QoT) for quantum and classical channels, margin reduction, failure prediction, IC-XT management, device placement, and topology design are some of the approaches that affect optical network planning, which can be efficiently solved using AI/ML/DL. Moreover, network self-configuration, self-optimization, and design of reactive approaches such as restoration and dealing with quantum hacking attacks using AI/ML/DL can also improve the performance of the future QKD-secured optical networks. Recently, a field trial of ML in hybrid quantum-classical network was demonstrated for estimating the quantum channel performance in terms of noise, SKR, and QBER in presence of classical channel in C-band [227]. A draft supplement to ITU-T Y-series recommendations also studied and covered different topics related to application of ML in QKD networks [228]. As observed with any new technology, it is difficult to predict all the possible applications of QKD-secured communication. Some of its possible applications include the realization of quantum sensor networks, fiber-cut monitoring, soft-failure detection, among others. Moreover, QKD is an emerging quantum technology for securing existing and future communication networks. Hence, QKD can be used for providing security in free space optics (FSO) communication systems [229], visible light communications [230], [231], [232], [233], [234], [235], [236], Unmanned Aerial Vehicles (UAVs) communications [237], [238], and THz communications [239], [240].

VII. Summary

This survey paper focuses on the QKD-secured optical networks, and describes procedure of QKD system, basic concepts of qubit, types of attacks, network architectures, and the methods developed for secure communication and to solve the networking problems. QKD distributes random secret keys between the sender and the receiver using different QKD protocols via the QSCh and PICh. The realization of QKD systems mainly depend on the QKD protocol being used. Various QKD protocols have been designed based on the P&M and EB schemes that define the principle on which the QKD system will work. The QKD systems provide security (based on the fundamental laws of quantum mechanics), however, due to the imperfection of practical devices, the quantum hacking attacks may leverage the security loopholes to crack the secure QKD systems. To mitigate the adverse effects of quantum hacking attacks, several methods have been developed, such as decoy-state QKD, MDI-QKD, and TF-QKD.

The QKD systems are expected to be integrated with the existing optical networks. However, this integration that requires two additional channels, namely, QSCh, and PICh, along with the TDCh introduces new challenges to be solved in the QKD secured optical networks. New network architectures have been proposed for QKD secured optical networks. Moreover, various new networking problems have been identified and researched upon in the recent past including the RWTA problem, resiliency of QLPs, TRN placement, among others. Several important and open issues have been identified that need to be addressed in the future.

VIII. Conclusion

This paper provides a comprehensive survey of QKD secured optical networks. All the necessary aspects needed to build an understanding of QKD secured optical networks have been covered, including the basics of qubit, various QKD protocols and procedures, the types of attacks in QKD protocols, network architectures, and state-of-the art methods developed to solve the important networking problems in QKD secured optical networks.

Several unexplored and partially-addressed issues and challenges have been identified that need to be explored further, as highlighted in Section VI. Moreover, efficient methods need to be developed for the already explored networking problems, and new networking challenges might be discovered for successful and efficient integration of QKD with the global optical networks in the future.

Appendix A

A. LIST OF ABBREVIATIONS

AES	Advanced encryption standard
AG-RWTA	Auxiliary graph based-RWTA
AI	Artificial intelligence

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2021.3106659, IEEE Open Journal of the Communications Society

API	Application program interface
B92 protocol	Bennett-92 protocol
BB84 protocol	Bennett and Brassard-84 protocol
BBM92 protocol	Bennett Brassard Meermin-92 protocol
bps	Bit per second
C-band	Conventional band
CCh	Control channel
COW protocol	Coherent one-way protocol
CV-QKD protocol	Continuous-variable QKD protocol
D	Diagonal
DARPA	Defense Advanced Research Project Agency
DCh	Data channel
DCNs	Data communication nodes
DL	Deep learning
DPR-QKD protocol	Distributed-reference QKD protocol
DPS protocol	Differential phase shift protocol
DSKRT-RKA	Distributed subkey-relay-tree-based secure multicast-routing and key assignment
DSKRT-SM	Distributed subkey-relay-tree based secure multicast
DV-QKD protocol	Discrete-variable QKD protocol
DWDM	Dense wavelength division multiplexing
E91 protocol	Ekert-91 protocol
EB scheme	Entanglement based scheme
EONs	Elastic optical networks
ETSI	European Telecommunications Standards Institute
ETSI ISG-QKD	ETSI Industry Specification Group on QKD
FB-RWTA	Full-bypassed RWTA
FSO	Free space optics
H	Horizontal
IC-XT	Inter-core crosstalk
IEEE	Institute of Electrical and Electronics Engineers
IETF/IRTF	Internet Engineering Task Force/Internet Research Task Force
ILP	Integer linear programming
IM	Intensity modulator
ISG	Industry Specification Group
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
ITU	International Telecommunication Union
ITU-T	International Telecommunication Union-Telecommunications
ITU-T SG 13	ITU-T Study Group 13
ITU-T SG 17	ITU-T Study Group 17
JPL-RWTA	Joint-path-and-link-based routing wavelength and time slot assignment
JTC	Joint Technical Committee
KaaS	Key as a service
Km	Kilometer
KML	Key management link
KoD	Key on demand
KP	Key pool
KRT-RKA	Key-relay-tree-based routing and key assignment
LKM	Local key manager
LP	Lightpath
Mbps	Megabits per second
MCF	Multicore fiber
MDI-QKD	Measurement-device-independent QKD
MDI-QRx	MDI-QKD receiver
MDI-QTx	MDI-QKD transmitter
ML	Machine learning
MPRM	Multi-path recovery method
MQON	Metro-quantum optical networks
MRN	Multi relay node
MTKA	Multi-tenant key assignment
MTP	Multi-tenant provisioning
NETCONF protocol	Network configuration protocol
NGNs	Next-generation networks
O-band	Original band
OFP	OpenFlow protocol
Off-MTP	Offline multi-tenant provisioning
On-MTP	Online multi-tenant provisioning
OPRM	Open path recovery method
OTDM	Optical time division multiplexing
OXC	Optical cross-connect
P&M	Prepare and measure
PB-RWTA	Partial-bypassed RWTA
PF	Polarization filter
PICh	Public interaction channel
PIN photo-diode	positive-intrinsic-negative photo-diode
PNS	Photon number splitting
QaaS	QKD as a service
QBER	Quantum bit error rate
QCNs	Quantum communication nodes
QD	Quantum detector
QKD	Quantum key distribution
QKDN	Quantum key distribution network
QKPC	Quantum key pool construction
QKPs	Quantum key pools
QKS	Quantum secret key server
QL	Quantum link
QLP	QKD secured lightpath
QoT	Quality of transmission
QSCh	Quantum signal channel
QSS	Quantum signal source
Qubits	Quantum bits
R	Rectilinear
RL	Reinforcement learning
RNG	Random number generator
ROADMs	Reconfigurable optical add and drop multiplexers
RWA	Routing and wavelength assignment
RWKA	Routing wavelength and key assignment
RWTA	Routing wavelength and time slot assignment

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2021.3106659, IEEE Open Journal of the Communications Society

SARG04 protocol	Scarani Acin Ribordy Gisin-04 protocol
SBPP	Shared backup path protection
SDM	Space division multiplexing
SDN	Software-defined networking
SDON	Software-defined optical network
SDQaaS	Software defined network for QKD as a service
SECOQC	Secure Communication based on Quantum Cryptography
SKFM	Secret key flow model
SKRs	Secret key rates
SKRS	Secret key recovery strategy
SKSR	Service request security ratio
SLA	Service level agreement
SPc	Control channel security probability
SPd	Data channel security probability
SRSR	Service request security ratio
SSP protocol	Six-state protocol
TDCh	Traditional data channel
TDM	Time division multiplexing
TF-QKD	Twin-field QKD
TRNs	Trusted repeater nodes
TSW	Time sliding window
TWRM	Time window-based recovery method
UAVs	Unmanned Aerial Vehicles
UTRNs	Untrusted relay nodes
V	Vertical
VKP	Virtual key pool
VOAs	Variable optical attenuators
WG3	Working group 3
WDM	Wavelength division multiplexing

ACKNOWLEDGMENT

We would like to thank the anonymous reviewers of the IEEE Open Journal of the Communications Society for their valuable suggestions which helped us to enhance the quality of the manuscript. We would also like to thank Prof. Biswanath Mukherjee, University of California, Davis (UC Davis) for his valuable comments and suggestions.

REFERENCES

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

[2] 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.

[3] 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.

[4] M. Caleffi, A. S. Cacciapuoti, and G. Bianchi, "Quantum internet: From communication to distributed computing!" in *Proc. ACM NANOCOM*, Reykjavik, Iceland, 2018, pp. 1–4.

[5] A. S. Cacciapuoti, M. Caleffi, F. Tafuri, F. S. Cataliotti, S. Gherardini, and G. Bianchi, "Quantum internet: networking challenges in distributed quantum computing," *IEEE Netw.*, vol. 34, no. 1, pp. 137–143, Nov. 2019.

[6] M. Caleffi, D. Chandra, D. Cuomo, S. Hassanpour, and A. S. Cacciapuoti, "The rise of the quantum internet," *Computer*, vol. 53, no. 6, pp. 67–72, Jun. 2020.

[7] D. Cuomo, M. Caleffi, and A. S. Cacciapuoti, "Towards a distributed quantum computing ecosystem," *IET Quantum Commun.*, vol. 1, no. 1, pp. 3–8, Jul. 2020.

[8] A. S. Cacciapuoti, M. Caleffi, R. Van 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, Mar. 2020.

[9] N. K. Kundu, S. P. Dash, M. R. McKay, and R. K. Mallik, "MIMO terahertz quantum key distribution," *arXiv preprint arXiv:2105.03642*, 2021.

[10] N. Wolchover, "A tricky path to quantum-safe encryption," *Quanta Mag.*, Sep. 2015.

[11] K. A. Fisher, A. Broadbent, L. Shalm, Z. Yan, J. Lavoie, R. Prevedel, T. Jennewein, and K. Resch, "Quantum computing on encrypted data," *Nat. Commun.*, vol. 5, no. 1, pp. 3074(1–7), Jan. 2014.

[12] Y. Cao, Y. Zhao, X. Yu, and Y. Wu, "Resource assignment strategy in optical networks integrated with quantum key distribution," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 9, no. 11, pp. 995–1004, Nov. 2017.

[13] C. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Computers, Systems & Signal Processing*, Bangalore, India, 1984, pp. 175–179.

[14] Y. Zhao, Y. Cao, X. Yu, and J. Zhang, "Quantum key distribution (QKD) over software-defined optical networks," in *Quantum Cryptography in Advanced Networks*, O. G. Morozov, Ed. Rijeka: IntechOpen, 2019, ch. 2. [Online]. Available: https://doi.org/10.5772/intechopen.80450

[15] Q. Zhang, F. Xu, Y.-A. Chen, C.-Z. Peng, and J.-W. Pan, "Large scale quantum key distribution: Challenges and solutions," *Opt. Express*, vol. 26, no. 18, pp. 24 260–24 273, Sep. 2018.

[16] W. Heisenberg, "The physical content of quantum kinematics and mechanics," in *Quantum Theory and Measurement*, J. A. Wheeler and W. H. Zurek, Eds. Princeton University Press: Princeton, 1927. [Online]. Available: http://www.informationphilosopher.com/solutions/scientists/heisenberg/Heisenberg_Uncertainty.pdf

[17] ——, *Physical principles of the quantum theory*. Dover Publications, Inc., 1930.

[18] C. A. Fuchs and A. Peres, "Quantum-state disturbance versus information gain: Uncertainty relations for quantum information," *Phys. Rev. A*, vol. 53, no. 4, pp. 2038–2045, Apr. 1996.

[19] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, Oct. 1982.

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

[21] M. A. Nielsen and I. L. Chuang, "Fundamental concepts," in *Quantum Computation and Quantum Information*. UK: Cambridge University Press, 2010, ch. 1. [Online]. Available: http://mmrc.amss.cas.cn/tlb/201702/W020170224608149940643.pdf

[22] J. Ortigoso, "Twelve years before the quantum no-cloning theorem," *Am. J. Phys*, vol. 86, no. 3, pp. 201–205, Mar. 2018.

[23] 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.

[24] 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.

[25] H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nat. Photon.*, vol. 8, no. 8, pp. 595–604, Jul. 2014.

[26] G. S. Vernam, "Cipher printing telegraph systems: For secret wire and radio telegraphic communications," *IEEE J. AIEE*, vol. 45, no. 2, pp. 109–115, Feb. 1926.

[27] M. Dworkin, E. Barker, J. Nechvatal, J. Foti, L. Bassham, E. Roback, and J. JFD, "Advanced encryption standard (AES)," *Federal Inf. Process. Stds. (NIST FIPS)*, vol. 197, Nov. 2001. [Online]. Available: https://www.nist.gov/publications/advanced-encryption-standard-aes

[28] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theor. Comput. Sci.*, vol. 560, no. 12, pp. 7–11, 2014.

[29] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, no. 6, pp. 661–663, Aug. 1991.

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

[31] 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.

[32] D. Bruß, "Optimal eavesdropping in quantum cryptography with six states," *Phys. Rev. Lett.*, vol. 81, no. 14, pp. 3018–3021, Oct. 1998.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2021.3106659, IEEE Open Journal of the Communications Society

[33] H. Bechmann-Pasquinucci and N. Gisin, "Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography," *Phys. Rev. A*, vol. 59, no. 6, pp. 4238–4248, Jun. 1999.

[34] V. Scarani, A. Acin, 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, pp. 057 901(1–4), Feb. 2004.

[35] T. C. Ralph, "Continuous variable quantum cryptography," *Phys. Rev. A*, vol. 61, no. 1, pp. 010 303(1–4), Dec. 1999.

[36] K. Inoue, E. Waks, and Y. Yamamoto, "Differential phase shift quantum key distribution," *Phys. Rev. Lett.*, vol. 89, no. 3, pp. 037 902(1–3), Jul. 2002.

[37] ——, "Differential-phase-shift quantum key distribution using coherent light," *Phys. Rev. A*, vol. 68, no. 2, pp. 022 317(1–4), Aug. 2003.

[38] H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth, and H. Weinfurter, "Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors," *New J. Phys.*, vol. 13, no. 7, pp. 073 024(1–10), Jul. 2011.

[39] 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, pp. 022 308(1–9), Aug. 2013.

[40] Z. Yuan, J. Dynes, and A. Shields, "Avoiding the blinding attack in QKD," *Nat. Photon.*, vol. 4, no. 12, pp. 800–801, Dec. 2010.

[41] W.-Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," *Phys. Rev. Lett.*, vol. 91, no. 5, pp. 057 901(1–4), Aug. 2003.

[42] X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," *Phys. Rev. Lett.*, vol. 94, no. 23, pp. 230 503(1–4), Jun. 2005.

[43] H.-K. Lo, "Quantum key distribution with vacua or dim pulses as decoy states," in *Proc. IEEE ISIT*, Chicago, USA, 2004, p. 137.

[44] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 108, no. 13, pp. 130 503(1–5), Mar. 2012.

[45] 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 *et al.*, "Measurement-device-independent quantum key distribution over untrustful metropolitan network," *Phys. Rev. X*, vol. 6, no. 1, pp. 011 024(1–8), Mar. 2016.

[46] 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 *et al.*, "Measurement-device-independent quantum key distribution over a 404 km optical fiber," *Phys. Rev. Lett.*, vol. 117, no. 19, pp. 190 501(1–5), Nov. 2016.

[47] W. Buttler, R. Hughes, P. G. Kwiat, S. Lamoreaux, G. Luther, G. Morgan, J. Nordholt, C. Peterson, and C. Simmons, "Practical free-space quantum key distribution over 1 km," *Phys. Rev. Lett.*, vol. 81, no. 15, pp. 3283–3286, Oct. 1998.

[48] C.-Z. Peng, T. Yang, X.-H. Bao, J. Zhang, X.-M. Jin, F.-Y. Feng, B. Yang, J. Yang, J. Yin, Q. Zhang *et al.*, "Experimental free-space distribution of entangled photon pairs over 13 km: towards satellite-based global quantum communication," *Phys. Rev. Lett.*, vol. 94, no. 15, pp. 150 501(1–4), Apr. 2005.

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

[50] R. J. Hughes, G. L. Morgan, and C. G. Peterson, "Quantum key distribution over a 48 km optical fibre network," *J. Mod. Opt.*, vol. 47, no. 2-3, pp. 533–547, Jul. 2000.

[51] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li *et al.*, "Secure quantum key distribution over 421 km of optical fiber," *Phys. Rev. Lett.*, vol. 121, no. 19, pp. 190 502(1–4), Nov. 2018.

[52] N. Peters, P. Toliver, T. Chapuran, R. Runser, S. McNown, C. Peterson, D. Rosenberg, N. Dallmann, R. Hughes, K. McCabe *et al.*, "Dense wavelength multiplexing of 1550 nm QKD with strong classical channels in reconfigurable networking environments," *New J. Phys.*, vol. 11, no. 4, pp. 045 012(1–17), Apr. 2009.

[53] M. P. Fok, Z. Wang, Y. Deng, and P. R. Prucnal, "Optical layer security in fiber-optic networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 6, no. 3, pp. 725–736, Sep. 2011.

[54] M. Furdek, N. Skorin-Kapov, S. Zsigmond, and L. Wosinska, "Vulnerabilities and security issues in optical networks," in *Proc. IEEE ICTON*, Graz, Austria, 2014, pp. 1–4.

[55] N. Skorin-Kapov, M. Furdek, S. Zsigmond, and L. Wosinska, "Physical-layer security in evolving optical networks," *IEEE Commun. Mag.*, vol. 54, no. 8, pp. 110–117, Aug. 2016.

[56] 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.

[57] S. Bahrani, M. Razavi, and J. A. Salehi, "Optimal wavelength allocation in hybrid quantum-classical networks," in *Proc. IEEE EUSIPCO*, Budapest, Hungary, 2016, pp. 483–487.

[58] T. J. Xia, D. Z. Chen, G. 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. IEEE/OSA OFC*. Optical Society of America, Anaheim, California United States, 2006, p. OTuJ7.

[59] 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.

[60] L. He, J. Niu, Y. Sun, and Y. Ji, "The four wave mixing effects in quantum key distribution based on conventional WDM network," in *Proc. IEEE COIN*, Jeju, South Korea, 2014, pp. 1–2.

[61] Y. Mao, B.-X. Wang, C. Zhao, G. Wang, R. Wang, H. Wang, F. Zhou, J. Nie, Q. Chen, Y. Zhao *et al.*, "Integrating quantum key distribution with classical communications in backbone fiber network," *Opt. Express*, vol. 26, no. 5, pp. 6010–6020, Mar. 2018.

[62] I. Choi, Y. R. Zhou, J. F. Dynes, Z. Yuan, A. Klar, A. Sharpe, A. Plews, M. Lucamarini, C. Radig, J. Neubert *et al.*, "Field trial of a quantum secured 10 Gb/s DWDM transmission system over a single installed fiber," *Opt. Express*, vol. 22, no. 19, pp. 23 121–23 128, Sep. 2014.

[63] K. Patel, J. Dynes, M. Lucamarini, I. Choi, A. Sharpe, Z. Yuan, R. Penty, and A. Shields, "Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks," *Appl. Phys. Lett.*, vol. 104, no. 5, pp. 051 123(1–4), Feb. 2014.

[64] 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, pp. 081 108(1–4), Feb. 2015.

[65] 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," *Nat. Photon.*, vol. 9, no. 3, pp. 163–168, Feb. 2015.

[66] J. F. Dynes, W. W. Tam, A. Plews, B. Fröhlich, A. W. Sharpe, M. Lucamarini, Z. Yuan, C. Radig, A. Straw, T. Edwards *et al.*, "Ultra-high bandwidth quantum secured data transmission," *Sci. Rep.*, vol. 6, pp. 35 149(1–6), Oct. 2016.

[67] J. Dynes, A. Wonfor, W.-S. Tam, A. Sharpe, R. Takahashi, M. Lucamarini, A. Plews, Z. Yuan, A. Dixon, J. Cho *et al.*, "Cambridge quantum network," *npj Quantum Inf.*, vol. 5, no. 101, pp. 1–8, Nov. 2019.

[68] X. Tang, A. Wonfor, R. Kumar, R. V. Penty, and I. H. White, "Quantum-safe metro network with low-latency reconfigurable quantum key distribution," *IEEE/OSA J. Lightw. Technol.*, vol. 36, no. 22, pp. 5230–5236, Nov. 2018.

[69] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, "Current status of the DARPA quantum network," in *Quantum Information and Computation III*, E. J. Donkor, A. R. Pirich, and H. E. Brandt, Eds., vol. 5815, International Society for Optics and Photonics. SPIE, 2005, pp. 138 – 149. [Online]. Available: https://doi.org/10.1117/12.606489

[70] C. Elliott, "Building the quantum network," *New J. Phys.*, vol. 4, no. 1, pp. 46.1–46.12, Jul. 2002.

[71] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. Dynes *et al.*, "The SECOQC quantum key distribution network in Vienna," *New J. Phys.*, vol. 11, no. 7, pp. 075 001(1–37), Jul. 2009.

[72] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka *et al.*, "Field test of quantum key distribution in the Tokyo QKD network," *Opt. Express*, vol. 19, no. 11, pp. 10 387–10 409, May 2011.

[73] D. Stucki, M. Legre, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, P. Monbaron *et al.*, "Long-term performance of the SwissQuantum quantum key distribution network in a field environment," *New J. Phys.*, vol. 13, no. 12, pp. 123 001(1–18), Dec. 2011.

[74] A. Mirza and F. Petruccione, "Realizing long-term quantum cryptography," *J. Opt. Soc. Am. B*, vol. 27, no. 6, pp. A185–A188, Jun. 2010.

[75] Z. Yuan and A. Shields, "Continuous operation of a one-way quantum key distribution system over installed telecom fibre," *Opt. Express*, vol. 13, no. 2, pp. 660–665, Jan. 2005.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2021.3106659, IEEE Open Journal of the Communications Society

[76] F. Xu, W. Chen, S. Wang, Z. Yin, Y. Zhang, Y. Liu, Z. Zhou, Y. Zhao, H. Li, D. Liu *et al.*, "Field experiment on a robust hierarchical metropolitan quantum cryptography network," *Chin. Sci. Bull.*, vol. 54, no. 17, pp. 2991–2997, Aug. 2009.

[77] R. Courtland, "China's 2,000-km quantum link is almost complete [News]," *IEEE Spectr.*, vol. 53, no. 11, pp. 11–12, Nov.2016.

[78] Z. Zhihao, "Beijing-Shanghai quantum link a 'new era'," *China Daily*, Sep. 2017. [Online]. Available: https://www.chinadaily.com.cn/china/2017-09/30/content_32669593.htm

[79] M. Razavi, A. Leverrier, X. Ma, B. Qi, and Z. Yuan, "Quantum key distribution and beyond: introduction," *OSA J. Opt. Soc. Am. B*, vol. 36, no. 3, pp. QKD1–QKD2, Mar. 2019.

[80] "ID Quantique." [Online]. Available: https://www.idquantique.com/

[81] "MagiQ Technologies, Inc." [Online]. Available: https://www.magiqtech.com/

[82] "Quantum Communications Hub." [Online]. Available: https://www.quantumcommshub.net/

[83] "QuintessenceLabs Pty Ltd." [Online]. Available: https://www.quintessencelabs.com/

[84] H. Liu, W. Wang, K. Wei, X.-T. Fang, L. Li, N.-L. Liu, H. Liang, S.-J. Zhang, W. Zhang, H. Li *et al.*, "Experimental demonstration of high-rate measurement-device-independent quantum key distribution over asymmetric channels," *Phys. Rev. Lett.*, vol. 122, no. 16, pp. 160 501(1–6), Apr. 2019.

[85] 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.

[86] 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, pp. 021 046(1–9), Jun. 2019.

[87] M. Minder, M. Pittaluga, G. Roberts, M. Lucamarini, J. Dynes, Z. Yuan, and A. Shields, "Experimental quantum key distribution beyond the repeaterless secret key capacity," *Nat. Photonics*, vol. 13, no. 5, pp. 334–338, Mar. 2019.

[88] M. Loeffler, T. Länger, A. Neumann, M. Legré, I. Khan, C. Chunnilall, D. López, M. Lucamarini, and V. Martin, "Current Standardisation Landscape and existing Gaps in the Area of Quantum Key Distribution," *OpenQKD*, Dec. 2020. [Online]. Available: https://openqkd.eu/wp-content/uploads/2021/03/OPENQKD_CurrentStandardisationLandscapeAndExistingGapsInTheAreaOfQuantumKeyDistribution.pdf

[89] "ITU-T Study Group 13 - Future networks, with focus on IMT-2020, cloud computing and trusted network infrastructure," *International Telecommunication Union*. [Online]. Available: https://www.itu.int/en/ITU-T/about/groups/Pages/sg13.aspx

[90] ITU-T Recommendation Y.3804, "Quantum key distribution networks-Control and management," *International Telecommunication Union*, Geneva, Switzerland, Sep. 2020. [Online]. Available: https://www.itu.int/rec/T-REC-Y.3804-202009-I/en

[91] "ITU-T Study Group 17 – Security," *International Telecommunication Union*. [Online]. Available: https://www.itu.int/en/ITU-T/about/groups/Pages/sg17.aspx

[92] ITU-T XSTR-SEC-QKD, "Security consideration for quantum key distribution," *International Telecommunication Union*, Mar. 2020. [Online]. Available: https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-QKD-2020-1-PDF-E.pdf

[93] "ETSI Quantum Key Disrtibution," *European Telecommunications Standards Institute*. [Online]. Available: https://www.etsi.org/technologies/quantum-key-distribution

[94] "Industry Specification Group (ISG) on Quantum Key Distribution Key (QKD) for Users ," *European Telecommunications Standards Institute*. [Online]. Available: https://www.etsi.org/committee/1430-qkd

[95] P1913 - Software-Defined Quantum Communication [Online]. Available: https://standards.ieee.org/project/1913.html.

[96] 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, Sep. 2009.

[97] N. Jain, B. Stiller, I. Khan, D. Elser, C. Marquardt, and G. Leuchs, "Attacks on practical quantum key distribution systems (and how to prevent them)," *Contemp. Phys.*, vol. 57, no. 3, pp. 366–387, Jul. 2016.

[98] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," *npj Quantum Inf.*, vol. 2, no. 1, pp. 1–12, Nov. 2016.

[99] A. Bahrami, A. Lord, and T. Spiller, "Quantum key distribution integration with optical dense wavelength division multiplexing: a review," *IET Quantum Commun.*, vol. 1, no. 1, pp. 9–15, Jul. 2020.

[100] 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, p. 025002, May 2020.

[101] B. Schumacher, "Quantum coding," *Phys. Rev. A*, vol. 51, no. 4, pp. 2738–2747, Apr. 1995.

[102] D. Bouwmeester and A. Zeilinger, "The physics of quantum information: Basic concepts," in *The physics of quantum information*. Springer, 2000, pp. 1–14.

[103] R. Van Meter, "Quantum Background," in *Quantum Networking*. Hoboken, NJ, USA: Wiley, 2014, ch. 2.

[104] S. Wehner and N. Ng, "edX Quantum Cryptography: Week 0," 2016. [Online]. Available: http://users.cms.caltech.edu/~vidick/notes/QCryptoX/LN_Week0.pdf

[105] L. O. Mailloux, M. R. Grimaila, D. D. Hodson, G. Baumgartner, and C. McLaughlin, "Performance evaluations of quantum key distribution system architectures," *IEEE Secur. Priv.*, vol. 13, no. 1, pp. 30–40, Jan.-Feb. 2015.

[106] L. Gyongyosi, S. Imre, and H. V. Nguyen, "A survey on quantum channel capacities," *IEEE Commun. Surv. Tuts.*, vol. 20, no. 2, pp. 1149–1205, 2nd Quart. 2018.

[107] C.-H. F. Fung, X. Ma, and H. Chau, "Practical issues in quantum-key-distribution postprocessing," *Phys. Rev. A*, vol. 81, no. 1, pp. 012 318(1–15), Jan. 2010.

[108] M. Mafu and M. Senekane, "Security of quantum key distribution protocols," in *Advanced Technologies of Quantum Key Distribution*, S. Gnatyuk, Ed. Rijeka: IntechOpen, 2018, ch. 1. [Online]. Available: https://doi.org/10.5772/intechopen.74234

[109] N. Gisin, G. Ribordy, H. Zbinden, D. Stucki, N. Brunner, and V. Scarani, "Towards practical and fast quantum cryptography," *arXiv preprint quant-ph/0411022*, Nov. 2004.

[110] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, "Quantum cryptography with entangled photons," *Phys. Rev. Lett.*, vol. 84, no. 20, pp. 4729–4732, May 2000.

[111] M. Hillery, "Quantum cryptography with squeezed states," *Phys. Rev. A*, vol. 61, no. 2, pp. 022 309(1–8), Jan. 2000.

[112] N. J. Cerf, M. Levy, and G. Van Assche, "Quantum distribution of Gaussian keys using squeezed states," *Phys. Rev. A*, vol. 63, no. 5, pp. 052 311(1–5), Apr. 2001.

[113] M. D. Reid, "Quantum cryptography with a predetermined key, using continuous-variable Einstein-Podolsky-Rosen correlations," *Phys. Rev. A*, vol. 62, no. 6, pp. 062 308(1–6), Nov. 2000.

[114] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Phys. Rev. Lett.*, vol. 88, no. 5, pp. 057 902(1–4), Jan. 2002.

[115] F. Grosshans, G. Van 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.

[116] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, "Quantum cryptography without switching," *Phys. Rev. Lett.*, vol. 93, no. 17, pp. 170 504(1–4), Oct. 2004.

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

[118] T. Wang, P. Huang, Y. Zhou, W. Liu, H. Ma, S. Wang, and G. Zeng, "High key rate continuous-variable quantum key distribution with a real local oscillator," *Opt. Express*, vol. 26, no. 3, pp. 2794–2806, Feb. 2018.

[119] D. Huang, P. Huang, D. Lin, and G. Zeng, "Long-distance continuous-variable quantum key distribution by controlling excess noise," *Sci. Rep.*, vol. 6, no. 1, pp. 19 201(1–9), Jan. 2016.

[120] D. B. Soh, C. Brif, P. J. Coles, N. Lütkenhaus, R. M. Camacho, J. Urayama, and M. Sarovar, "Self-referenced continuous-variable quantum key distribution protocol," *Phys. Rev. X*, vol. 5, no. 4, pp. 041 010(1–15), Oct. 2015.

[121] K. Inoue, "Differential phase-shift quantum key distribution systems," *IEEE J. Sel. Top. Quantum Electron.*, vol. 21, no. 3, pp. 109–115, Sep. 2014.

[122] 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.

[123] A. Acin, N. Gisin, and V. Scarani, "Coherent-pulse implementations of quantum cryptography protocols resistant to photon-number-splitting attacks," *Phys. Rev. A*, vol. 69, no. 1, pp. 012 309(1–16), Jan. 2004.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2021.3106659, IEEE Open Journal of the Communications Society

[124] A. Gleim, V. Egorov, Y. V. Nazarov, S. Smirnov, V. Chistyakov, O. Bannik, A. Anisimov, S. Kynev, A. Ivanova, R. Collins *et al.*, "Secure polarization-independent subcarrier quantum key distribution in optical fiber channel using BB84 protocol with a strong reference," *Opt. Express*, vol. 24, no. 3, pp. 2619–2633, Feb. 2016.

[125] E. Kiktenko, A. Trushechkin, Y. Kurochkin, and A. Fedorov, "Post-processing procedure for industrial quantum key distribution systems," in *J. Phys. Conf. Ser.*, vol. 741, no. 1. IOP Publishing, 2016, pp. 012 081(1–6).

[126] Y. Cao, Y. Zhao, Y. Wu, X. Yu, and J. Zhang, "Time-scheduled quantum key distribution (QKD) over WDM networks," *IEEE/OSA J. Lightw. Technol.*, vol. 36, no. 16, pp. 3382–3395, Aug. 2018.

[127] 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. 26 453–26 467, Oct. 2017.

[128] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, "Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems," *Phys. Rev. A*, vol. 78, no. 4, pp. 042 333(1–5), Oct. 2008.

[129] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination," *Nat. photonics*, vol. 4, no. 10, pp. 686–689, Aug. 2010.

[130] L. O. Mailloux, D. D. Hodson, M. R. Grimaila, R. D. Engle, C. V. Mclaughlin, and G. B. Baumgartner, "Using modeling and simulation to study photon number splitting attacks," *IEEE Access*, vol. 4, pp. 2188–2197, May 2016.

[131] B. Huttner, N. Imoto, N. Gisin, and T. Mor, "Quantum cryptography with coherent states," *Phys. Rev. A*, vol. 51, no. 3, pp. 1863–1869, Mar. 1995.

[132] 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, pp. 070 502(1–4), Feb. 2006.

[133] M. Lucamarini, K. Patel, J. Dynes, B. Fröhlich, A. Sharpe, A. Dixon, Z. Yuan, R. Penty, and A. Shields, "Efficient decoy-state quantum key distribution with quantified security," *Opt. Express*, vol. 21, no. 21, pp. 24 550–24 565, Oct. 2013.

[134] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Phys. Rev. Lett.*, vol. 94, no. 23, pp. 230 504(1–4), Jun. 2005.

[135] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," *Phys. Rev. A*, vol. 72, no. 1, pp. 012 326(1–15), Jul. 2005.

[136] F. Grünenfelder, A. Boaron, D. Rusca, A. Martin, and H. Zbinden, "Simple and high-speed polarization-based QKD," *Appl. Phys. Lett.*, vol. 112, no. 5, pp. 051 108(1–3), Jan. 2018.

[137] D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt, "Long-distance decoy-state quantum key distribution in optical fiber," *Phys. Rev. Lett.*, vol. 98, no. 1, pp. 010 503(1–4), Jan. 2007.

[138] Y. Liu, T.-Y. Chen, J. Wang, W.-Q. Cai, X. Wan, L.-K. Chen, J.-H. Wang, S.-B. Liu, H. Liang, L. Yang *et al.*, "Decoy-state quantum key distribution with polarized photons over 200 km," *Opt. Express*, vol. 18, no. 8, pp. 8587–8594, Apr. 2010.

[139] C.-Z. Peng, J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, H.-P. Zeng, T. Yang, X.-B. Wang, and J.-W. Pan, "Experimental long-distance decoy-state quantum key distribution based on polarization encoding," *Phys. Rev. Lett.*, vol. 98, no. 1, pp. 010 505(1–4), Jan. 2007.

[140] A. Lamas-Linares and C. Kurtsiefer, "Breaking a quantum key distribution system through a timing side channel," *Opt. Express*, vol. 15, no. 15, pp. 9388–9393, Jul. 2007.

[141] M.-S. Jiang, S.-H. Sun, G.-Z. Tang, X.-C. Ma, C.-Y. Li, and L.-M. Liang, "Intrinsic imperfection of self-differencing single-photon detectors harms the security of high-speed quantum cryptography systems," *Phys. Rev. A*, vol. 88, no. 6, pp. 062 335(1–5), Dec. 2013.

[142] 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, pp. 148–158, Dec. 2014.

[143] Ø. Marøy, L. Lydersen, and J. Skaar, "Security of quantum key distribution with arbitrary individual imperfections," *Phys. Rev. A*, vol. 82, no. 3, pp. 032 337(1–7), Sep. 2010.

[144] T. F. da Silva, G. B. Xavier, G. P. Temporão, and J. P. von der Weid, "Real-time monitoring of single-photon detectors against eavesdropping in quantum key distribution systems," *Opt. Express*, vol. 20, no. 17, pp. 18 911–18 924, Aug. 2012.

[145] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, "Device-independent security of quantum cryptography against collective attacks," *Phys. Rev. Lett.*, vol. 98, no. 23, pp. 230 501(1–4), Jun. 2007.

[146] X.-B. Wang, "Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors," *Phys. Rev. A*, vol. 87, no. 1, pp. 012 320(1–8), Jan. 2013.

[147] X.-L. Hu, Y. Cao, Z.-W. Yu, and X.-B. Wang, "Measurement-device-independent quantum key distribution over asymmetric channel and unstable channel," *Sci. Rep.*, vol. 8, no. 1, pp. 1–7, Dec. 2018.

[148] 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, pp. 063 027(1–15), Jun. 2010.

[149] A. Beveratos, R. Brouri, T. Gacoin, A. Villing, J.-P. Poizat, and P. Grangier, "Single photon quantum cryptography," *Phys. Rev. Lett.*, vol. 89, no. 18, pp. 187 901(1–4), Oct. 2002.

[150] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[151] M. Taha and P. Schaumont, "Key updating for leakage resiliency with application to AES modes of operation," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 3, pp. 519–528, Mar. 2015.

[152] P. Derbez, P.-A. Fouque, and J. Jean, "Improved key recovery attacks on reduced-round AES in the single-key setting," in *Advances in Cryptology – EUROCRYPT 2013*, T. Johansson and P. Q. Nguyen, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 371–387.

[153] Y. Cao, Y. Zhao, X. Yu, H. Wang, C. Liu, B. Li, and J. Zhang, "Resource allocation in software-defined optical networks secured by quantum key distribution," in *Proc. IEEE OECC/PGC*, Singapore, 2017, pp. 1–3.

[154] M. Channegowda, R. Nejabati, and D. Simeonidou, "Software-defined optical networks technology and infrastructure: enabling software-defined optical network operations," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 5, no. 10, pp. A274–A282, Oct. 2013.

[155] D. B. Rawat and S. R. Reddy, "Software defined networking architecture, security and energy efficiency: A survey," *IEEE Commun. Surv. Tuts.*, vol. 19, no. 1, pp. 325–346, 1st Quart. 2017.

[156] 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 *et al.*, "Secure NFV orchestration over an SDN-controlled optical network with time-shared quantum key distribution resources," *IEEE/OSA J. Lightw. Technol.*, vol. 35, no. 8, pp. 1357–1362, Apr. 2017.

[157] 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," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 9, no. 10, pp. 819–825, Oct. 2017.

[158] Y. Zhao, Y. Cao, X. Yu, and J. Zhang, "Software defined optical networks secured by quantum key distribution (QKD)," in *Proc. IEEE/CIC ICCC*, Qingdao Shi, Shandong Sheng, China, 2017, pp. 1–4.

[159] 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," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 11, no. 2, pp. A209–A218, Feb. 2019.

[160] S. Gringeri, N. Bitar, and T. J. Xia, "Extending software defined network principles to include optical transport," *IEEE Commun. Mag.*, vol. 51, no. 3, pp. 32–40, Mar. 2013.

[161] 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," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 10, no. 4, pp. 421–430, Apr. 2018.

[162] 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.

[163] ——, "SDQaaS: Software defined networking for quantum key distribution as a service," *Opt. Express*, vol. 27, no. 5, pp. 6892–6909, Mar. 2019.

[164] J. Y. Cho, T. Szyrkowiec, and H. Griesser, "Quantum key distribution as a service," *Proc. QCrypt*, Cambridge, United Kingdom, 2017.

[165] 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.*, Mar. 2021.

[166] ——, "Mixed relay placement for quantum key distribution chain deployment over optical networks," in *Proc. ECOC*. IEEE, 2020, pp. 1–4.

[167] B. Wen and K. M. Sivalingam, "Routing, wavelength and time-slot assignment in time division multiplexed wavelength-routed optical WDM networks," in *Proc. IEEE INFOCOM*, vol. 3, New York, NY, USA, 2002, pp. 1442–1450.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2021.3106659, IEEE Open Journal of the Communications Society

[168] S. Bahrani, M. Razavi, and J. A. Salehi, "Wavelength assignment in hybrid quantum-classical networks," *Sci. Rep.*, vol. 8, no. 1, pp. 3456(1–13), Feb. 2018.

[169] Y. Zhao, Z. Chen, J. Zhang, and X. Wang, "Dynamic optical resource allocation for mobile core networks with software defined elastic optical networking," *Opt. Express*, vol. 24, no. 15, pp. 16 659–16 673, Jul. 2016.

[170] D. Banerjee and B. Mukherjee, "A practical approach for routing and wavelength assignment in large wavelength-routed optical networks," *IEEE J. Sel. Areas Commun.*, vol. 14, no. 5, pp. 903–908, Jun. 1996.

[171] A. R. Dixon, Z. Yuan, J. Dynes, A. Sharpe, and A. Shields, "Continuous operation of high bit rate quantum key distribution," *Appl. Phys. Lett.*, vol. 96, no. 16, pp. 161 102(1–3), Apr. 2010.

[172] R. S. Tucker, G. Eisenstein, and S. K. Korotky, "Optical time-division multiplexing for very high bit-rate transmission," *IEEE/OSA J. Lightw. Technol.*, vol. 6, no. 11, pp. 1737–1749, Nov. 1988.

[173] 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. OSA ACP*, Guangzhou, Guangdong China, 2017, pp. Su2A–66.

[174] W. Yu, B. Zhao, and Z. Yan, "Software defined quantum key distribution network," in *Proc. IEEE ICCC*, Chengdu, China, 2017, pp. 1293–1297.

[175] K. Dong, Y. Zhao, X. Yu, J. Zhang, H. Yu, and Z. Li, "Auxiliary graph based routing, wavelength and time-slot assignment in metro quantum optical networks," in *Proc. IEEE OECC/PSC*, Fukuoka, Japan, 2019, pp. 1–3.

[176] K. Dong, Y. Zhao, X. Yu, J. Zhang, H. Yu, and Y. Zhang, "Auxiliary topology based global quantum key distribution for secure multicast service," in *Proc. IEEE OECC/PSC*, Fukuoka, Japan, 2019, pp. 1–3.

[177] X. Yu, X. Ning, Q. Zhu, J. Lv, Y. Zhao, H. Zhang, and J. Zhang, "Multi-dimensional routing, wavelength, and timeslot allocation (RWTA) in quantum key distribution optical networks (QKD-ON)," *Appl. Sci.*, vol. 11, no. 1, pp. 348(1–14), 2021.

[178] 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.

[179] 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.

[180] Y. Cao, Y. Zhao, X. Yu, and J. Zhang, "Multi-tenant provisioning over software defined networking enabled metropolitan area quantum key distribution networks," *OSA J. Opt. Soc. Am. B*, vol. 36, no. 3, pp. B31–B40, Mar. 2019.

[181] 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. 10 359–10 373, Apr. 2015.

[182] Y. Cao, Y. Zhao, J. Li, R. Lin, J. Zhang, and J. Chen, "Reinforcement learning based multi-tenant secret-key assignment for quantum key distribution networks," in *Proc. IEEE/OSA OFC*, San Diego, CA, USA, 2019, pp. M2A–7.

[183] ——, "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, Jan. 2020.

[184] 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.

[185] A. Agrawal, V. Bhatia, and S. Prakash, "Network and risk modeling for disaster survivability analysis of backbone optical communication networks," *IEEE/OSA J. Lightw. Technol.*, vol. 37, no. 10, pp. 2352–2362, May 2019.

[186] 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)," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 11, no. 3, pp. 67–78, Mar. 2019.

[187] H. Wang, Y. Zhao, X. Yu, B. Chen, and J. Zhang, "Resilient fiber-based quantum key distribution (QKD) networks with secret-key re-allocation strategy," in *Proc. IEEE/OSA OFC*, San Diego, California United States, 2019, pp. W2A–25.

[188] W. Hua, 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. 60 079–60 090, May 2019.

[189] 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. OSA ACP*, Chengdu, China, 2019, pp. M4C–6.

[190] L. Lu, X. Yu, Y. Zhao, and J. Zhang, "Dynamic wavelength and key resource adjustment in wdm based QKD optical networks," in *Proc. OSA ACP*, Beijing, China, 2020, pp. M4A–184.

[191] 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," *arXiv preprint arXiv:1810.03857*, Oct. 2018.

[192] 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," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 12, no. 5, pp. 120–132, Apr. 2020.

[193] D. Elkouss, J. Martinez-Mateo, A. Ciurana, and V. Martin, "Secure optical networks based on quantum key distribution and weakly trusted repeaters," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 5, no. 4, pp. 316–328, Apr. 2013.

[194] X.-T. Fang, P. Zeng, H. Liu, M. Zou, W. Wu, Y.-L. Tang, Y.-J. Sheng, Y. Xiang, W. Zhang, H. Li *et al.*, "Implementation of quantum key distribution surpassing the linear rate-transmittance bound," *Nat. Photon.*, vol. 14, no. 7, pp. 422–425, Jul. 2020.

[195] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W. Zhang, X.-L. Hu, J.-Y. Guan, Z.-W. Yu, H. Xu, J. Lin *et al.*, "Sending-or-not-sending with independent lasers: Secure twin-field quantum key distribution over 509 km," *Phy. Rev. Lett.*, vol. 124, no. 7, p. 070501, Feb. 2020.

[196] 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. OSA OFC*. Optical Society of America, San Diego, California, USA, 2020, pp. M3K–4.

[197] K. Dong, Y. Zhao, A. Nag, X. Yu, and J. Zhang, "Distributed subkey-relay-tree-based secure multicast scheme in quantum data center networks," *Opt. Eng.*, vol. 59, no. 6, pp. 065 102(1–11), Jun. 2020.

[198] X. Li, Y. Zhao, A. Nag, X. Yu, and J. Zhang, "Key-recycling strategies in quantum-key-distribution networks," *Appl. Sci.*, vol. 10, no. 11, pp. 3734(1–19), Jan. 2020.

[199] X. Yang, Y. Li, G. Gao, Y. Zhao, H. Zhang, and J. Zhang, "Demonstration of key generation scheme based on feature extraction of optical fiber channel," in *Proc. IEEE ACP*, Hangzhou, China, 2018, pp. 1–3.

[200] Y. Cao, Y. Zhao, J. Wang, X. Yu, Z. Ma, and J. Zhang, "Cost-efficient quantum key distribution (QKD) over WDM networks," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 11, no. 6, pp. 285–298, Jun. 2019.

[201] 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 *et al.*, "Field experiment on a "star type" metropolitan quantum key distribution network," *IEEE Photon. Technol. Lett.*, vol. 21, no. 9, pp. 575–577, Feb. 2009.

[202] T.-Y. Chen, J. Wang, H. Liang, W.-Y. Liu, Y. Liu, X. Jiang, Y. Wang, X. Wan, W.-Q. Cai, L. Ju *et al.*, "Metropolitan all-pass and inter-city quantum communication network," *Opt. Express*, vol. 18, no. 26, pp. 27 217–27 225, Dec. 2010.

[203] S. Wang, W. Chen, Z.-Q. Yin, Y. Zhang, T. Zhang, H.-W. Li, F.-X. Xu, Z. Zhou, Y. Yang, D.-J. Huang *et al.*, "Field test of wavelength-saving quantum key distribution network," *Opt. Lett.*, vol. 35, no. 14, pp. 2454–2456, Jul. 2010.

[204] 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 *et al.*, "Field and long-term demonstration of a wide area quantum key distribution network," *Opt. Express*, vol. 22, no. 18, pp. 21 739–21 756, Sep. 2014.

[205] "SK Telecom." [Online]. Available: https://www.fiercewireless.com/wireless/sk-telecom-develops-advanced-quantum-repeater

[206] 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, pp. 040 503(1–7), Nov. 2019.

[207] M. Pompili, S. L. Hermans, S. Baier, H. K. Beukers, P. C. Humphreys, R. N. Schouten, R. F. Vermeulen, M. J. Tiggelman, L. dos Santos Martins, B. Dirkse *et al.*, "Realization of a multinode quantum network of remote solid-state qubits," *Science*, vol. 372, no. 6539, pp. 259–264, 2021.

[208] M. Jinno, H. Takara, B. Kozicki, Y. Tsukishima, Y. Sone, and S. Matsuoka, "Spectrum-efficient and scalable elastic optical path network: architecture, benefits, and enabling technologies," *IEEE communications magazine*, vol. 47, no. 11, pp. 66–73, 2009.

[209] A. Lord, P. Wright, and A. Mitra, "Core networks in the flexgrid era," *Journal of Lightwave Technology*, vol. 33, no. 5, pp. 1126–1135, 2015.

[210] H. Saarnisaari, S. Dixit, M.-S. Alouini, A. Chaoub, M. Giordani, A. Kliks, M. Matinmikko-Blue, N. Zhang, A. Agrawal, M. Andersson, V. Bhatia *et al.*, "A 6G White Paper on Connectivity for Remote Areas," *arXiv preprint arXiv:2004.14699*, 2020.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2021.3106659, IEEE Open Journal of the Communications Society

[211] A. Agrawal, V. Bhatia, and S. Prakash, "Spectrum efficient distance-adaptive paths for fixed and fixed-alternate routing in elastic optical networks," *Optical Fiber Technology*, vol. 40, pp. 36–45, 2018.
[212] N. Sambo, A. Ferrari, A. Napoli, N. Costa, J. Pedro, B. Sommerkorn-Krombholz, P. Castoldi, and V. Curri, "Provisioning in multi-band optical networks," *Journal of Lightwave Technology*, vol. 38, no. 9, pp. 2598–2605, 2020.
[213] J. Dynes, S. Kindness, S.-B. Tam, A. Plews, A. Sharpe, M. Lucamarini, B. Fröhlich, Z. Yuan, R. Penty, and A. Shields, "Quantum key distribution over multicore fiber," *Opt. Express*, vol. 24, no. 8, pp. 8081–8087, Apr. 2016.
[214] 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.
[215] A. Agrawal, V. Bhatia, and S. Prakash, "Low-crosstalk-margin routing for spectrally-spatially flexible optical networks," *IEEE Commun. Lett.*, vol. 24, no. 4, pp. 835–839, Apr. 2020.
[216] A. Sano *et al.*, "409-Tb/s+ 409-Tb/s crosstalk suppressed bidirectional MCF transmission over 450 km using propagation-direction interleaving," *Opt. Express*, vol. 21, no. 14, pp. 16 777–16 783, Jul. 2013.
[217] A. Agrawal, V. Bhatia, and S. Prakash, "Towards zero-crosstalk-margin operation of spectrally-spatially flexible optical networks using heterogeneous multicore fibers," in *Proc. IEEE/OSA OFC*, San Diego, California United States, 2020, pp. W2A–23.
[218] X. Yu, M. Tornatore, M. Xia, Y. Zhao, J. Zhang, and B. Mukherjee, "Brown-field migration from fixed grid to flexible grid in optical networks," in *Proc. IEEE/OSA OFC*, Los Angeles, California United States, 2015, pp. W1I–4.
[219] Y. Zhang, Y. Zhang, S. K. Bose, and G. Shen, "Migration from fixed to flexible grid optical networks with sub-band virtual concatenation," *IEEE/OSA J. Lightw. Technol.*, vol. 35, no. 10, pp. 1752–1765, Mar. 2017.
[220] X. Yu, M. Tornatore, M. Xia, J. Wang, J. Zhang, Y. Zhao, J. Zhang, and B. Mukherjee, "Migration from fixed grid to flexible grid in optical networks," *IEEE Commun. Mag.*, vol. 53, no. 2, pp. 34–43, Feb. 2015.
[221] M. Ruiz, L. Velasco, A. Lord, D. Fonseca, M. Pioro, R. Wessaly, and J. P. Fernandez-Palacios, "Planning fixed to flexgrid gradual migration: drivers and open issues," *IEEE Commun. Mag.*, vol. 52, no. 1, pp. 70–76, Jan. 2014.
[222] P. Lechowicz, R. Goscien, R. Rumipamba-Zambrano, J. Perello, S. Spadaro, and K. Walkowiak, "Greenfield gradual migration planning toward spectrally-spatially flexible optical networks," *IEEE Commun. Mag.*, vol. 57, no. 10, pp. 14–19, Oct. 2019.
[223] P. Lechowicz, R. Rumipamba-Zambrano, J. Perelló, S. Spadaro, and K. Walkowiak, "Inter-core crosstalk impact on migration planning from elastic optical networks to spectrally-spatially flexible optical networks," in *Proc. IEEE/OSA OFC*, San Diego, California United States, 2019, pp. M4J–6.
[224] A. Agrawal, U. Vyas, V. Bhatia, and S. Prakash, "SLA-aware differentiated qos in elastic optical networks," *Optical Fiber Technology*, vol. 36, pp. 41–50, 2017.
[225] S. Ali, W. Saad, N. Rajatheva, K. Chang, D. Steinbach, B. Sliwa, C. Wietfeld, K. Mei, H. Shiri, H.-J. Zepernick *et al.*, "6G White Paper on machine learning in wireless communication networks," *arXiv preprint arXiv:2004.13875*, 2020.
[226] A. Chaoub, M. Giordani, B. Lall, V. Bhatia, A. Kliks, L. Mendes, K. Rabie, H. Saarnisaari, A. Singhal, N. Zhang *et al.*, "6G for bridging the digital divide: Wireless connectivity to remote areas," *IEEE Wirel. Commun.*, pp. 1–9, Jul. 2021.
[227] 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 *IEEE ECOC*. IEEE, Rome, Italy, 2018, pp. 1–3.
[228] Draft Supplement ITU-T Y.supp.QKDN-mla, "Quantum Key Distribution Networks - Applications of Machine Learning," *International Telecommunication Union*, 2021.
[229] P. K. Singya, N. Kumar, V. Bhatia, and M.-S. Alouini, "On the performance analysis of higher order QAM schemes over mixed RF/FSO systems," *IEEE Trans. Veh. Technol.*, vol. 69, no. 7, pp. 7366–7378, Apr. 2020.
[230] S. Jain, R. Mitra, and V. Bhatia, "Kernel MSER-DFE based post-distorter for VLC using random Fourier features," *IEEE Trans. Veh. Technol.*, vol. 69, no. 12, pp. 16 241–16 246, Nov. 2020.
[231] R. Mitra, S. Jain, and V. Bhatia, "Least minimum symbol error rate based post-distortion for VLC using random Fourier features," *IEEE Commun. Lett.*, vol. 24, no. 4, pp. 830–834, Jan. 2020.
[232] R. Mitra, F. Miramirkhani, V. Bhatia, and M. Uysal, "Mixture-kernel based post-distortion in RKHS for time-varying VLC channels," *IEEE Trans. Veh. Technol.*, vol. 68, no. 2, pp. 1564–1577, Dec. 2018.
[233] R. Mitra and V. Bhatia, "Precoded chebyshev-NLMS-based pre-distorter for nonlinear LED compensation in NOMA-VLC," *IEEE Trans. Commu.*, vol. 65, no. 11, pp. 4845–4856, Aug. 2017.
[234] ——, "Adaptive sparse dictionary-based kernel minimum symbol error rate post-distortion for nonlinear LEDs in visible light communications," *IEEE Photonics J.*, vol. 8, no. 4, pp. 1–13, Jun. 2016.
[235] V. Bhatia, S. Jain, K. Garg, and R. Mitra, "Performance analysis of RKHS based detectors for nonlinear NLOS ultraviolet communications," *IEEE Trans. Veh. Technol.*, vol. 70, no. 4, pp. 3625–3639, Mar. 2021.
[236] R. Mitra, G. Kaddoum, and V. Bhatia, "Hyperparameter-free transmit-nonlinearity mitigation using a Kernel-width sampling technique," *IEEE Trans. Commun.*, vol. 69, no. 4, pp. 2613–2627, Dec. 2020.
[237] C. Stefanovic, S. Panic, V. Bhatia, and N. Kumar, "On second-order statistics of the composite channel models for UAV-to-ground communications with UAV selection," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 534–544, Mar. 2021.
[238] D. Dixit, N. Kumar, S. Sharma, V. Bhatia, S. Panic, and C. Stefanovic, "On the ASER performance of UAV-based communication systems for QAM schemes," *IEEE Commun. Lett.*, vol. 25, no. 6, pp. 1835–1838, June, 2021.
[239] A. S. Cacciapuoti, K. Sankhe, M. Caleffi, and K. R. Chowdhury, "Beyond 5G: THz-based medium access protocol for mobile heterogeneous networks," *IEEE Commun. Mag.*, vol. 56, no. 6, pp. 110–115, 2018.
[240] V. Sharma, S. Sharma, and V. Bhatia, "Design and analysis of low-complexity terahertz receiver," in *Proc. IEEE TENCON*, Osaka, Japan, 2020, pp. 297–302.

Purva Sharma is currently pursuing Ph.D. in Electrical Engineering at the Indian Institute of Technology (IIT) Indore, India. Her research interests include WDM optical networks, elastic optical networks, quantum key distribution, and optical network security.

Anuj Agrawal has recently submitted Ph.D. thesis on optical networks at the Indian Institute of Technology (IIT) Indore, India. Currently, he is a Postdoctoral Researcher (Early Career Fellow) at IIT Gandhinagar. He was the recipient of Best Paper Award (Ph.D. Student Forum) at the 12th IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS) in 2018 for his work on multicore fiber networks. He was a visiting researcher at the Centre for Wireless Communications, University of Oulu, Finland in 2019. His research interests include optical networks, multicore fiber, quantum-classical coexistence, physical layer impairments, network resilience, network planning, routing, optical-wireless convergence, and optical backhaul/backbone for B5G/6G communication networks. He is a reviewer for IEEE, OSA, Elsevier, Springer, and Wiley.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2021.3106659, IEEE Open Journal of the Communications Society

Vimal Bhatia (SM'12) is currently working as a Professor with the Indian Institute of Technology (IIT) Indore, India, and is an adjunct faculty at IIT Delhi and IIIT Delhi, India. He received Ph.D. degree from Institute for Digital Communications with The University of Edinburgh, Edinburgh, U.K., in 2006. During Ph.D. he also received the IEE fellowship for collaborative research at the Department of Systems and Computer Engineering, Carleton University, Canada, and is Young Faculty Research Fellow from MeitY (2016-2021), Govt of India. He is also a recipient of Prof SVC Aiya Memorial Award (2019). He has worked with various IT companies for over 11 years both in India and the UK. He is a PI/co-PI/coordinator for external projects with funding of over USD 18 million from MeitY, DST, UKIERI, MoE, AKA, IUSSTF and KPMG. He has more than 285 peer reviewed publications and has filed 13 patents. His research interests are in the broader areas of communications, non-Gaussian nonparametric signal processing, machine/deep learning with applications to communications and photonics. He is a reviewer for IEEE, Elsevier, Wiley, Springer, and IET. He is currently Senior Member of IEEE, Fellow IETE and certified SCRUM Master. He was also the General Co-Chair for IEEE ANTS 2018, and General Vice-Chair for IEEE ANTS 2017. He has served as founder head of Center for Innovation and Entrepreneurship, Associate Dean R& D and Dean, Academic Affairs at IIT Indore. He has delivered many talks, tutorials and conducted faculty development programs for the World Bank's NPIU TEQIP-III programs. He is currently Associate Editor for IETE Technical Review, Frontiers in Communications and Networks, Frontiers in Signal Processing, and IEEE Wireless Communications Letters.

Shashi Prakash is Professor in Department of Electronics and Instrumentation, Institute of Engineering & Technology (IET), Devi Ahilya University, Indore, India since 2007. He joined Devi Ahilya University in 1992. He received his M.Tech. and Ph.D. degree from Indian Institute of Technology Delhi, New Delhi, India in 1992 and 2003, respectively. He was Visiting Foreign Researcher in Department of Electrical and Electronics Engineering, Niigata University, Niigata, Japan for about a year in 2009. He has published more than 125 journal and conference papers. His research focuses on optical communication networks, optical metrology, and laser-based instrumentation.

Amit Kumar Mishra received the Ph.D.degree from the University of Edinburgh, Edinburgh, U.K., in 2006. He is currently a Professor with the Department of Electrical Engineering, University of Cape Town, Cape Town, South Africa. His research interests include sensor design, radar, applied machine learning, quantum key distribution, and frugal innovation. His Google-Scholar based H-index is 14. He has more than 150 peer-reviewed publications and five patents.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/