

Multi-protocol relay chaining for large-scale quantum key distribution networks

Yuan Cao(曹原), Xiaosong Yu(郁小松), Yongli Zhao(赵永利), Chunhui Zhang(张春辉), Xingyu Zhou(周星宇), Jie Zhang(张杰), and Qin Wang(王琴)

Citation: Chin. Phys. B, 2025, 34 (**1**): 010310. DOI: 10.1088/1674-1056/ad9018
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Fast implementation of length-adaptive privacy amplification in quantum key distribution

Zhang Chun-Mei (张春梅), Li Mo (李默), Huang Jing-Zheng (黄靖正), Patcharapong Treeviriyanupab, Li Hong-Wei (李宏伟), Li Fang-Yi (李芳毅), Wang Chuan (王川), Yin Zhen-Qiang (银振强), Chen Wei (陈巍), Keattisak Sripimanwat, Han Zhen-Fu (韩正甫)
Chin. Phys. B, 2014, 23 (**9**): 090310. DOI: 10.1088/1674-1056/23/9/090310

Performance of entanglement-assisted quantum codes with noisy ebits over asymmetric and memory channels

Ji-Hao Fan(樊继豪), Pei-Wen Xia(夏沛文), Di-Kang Dai(戴迪康), and Yi-Xiao Chen(陈一骁)
Chin. Phys. B, 2023, 32 (**12**): 120304. DOI: 10.1088/1674-1056/acf492

Short-wave infrared continuous-variable quantum key distribution over satellite-to-submarine channels

Qingquan Peng(彭清泉), Qin Liao(廖骎), Hai Zhong(钟海), Junkai Hu(胡峻凯), and Ying Guo(郭迎)
Chin. Phys. B, 2022, 31 (**6**): 060306. DOI: 10.1088/1674-1056/ac490a

Hybrid linear amplifier-involved detection for continuous variable quantum key distribution with thermal states

Yu-Qian He(贺宇千), Yun Mao(毛云), Hai Zhong(钟海), Duang Huang(黄端), Ying Guo(郭迎)
Chin. Phys. B, 2020, 29 (**5**): 050309. DOI: 10.1088/1674-1056/ab8216

Finite-size analysis of continuous-variable quantum key distribution with entanglement in the middle

Ying Guo(郭迎), Yu Su(苏玉), Jian Zhou(周健), Ling Zhang(张玲), Duan Huang(黄端)
Chin. Phys. B, 2019, 28 (**1**): 010305. DOI: 10.1088/1674-1056/28/1/010305

SPECIAL TOPIC — Quantum communication and quantum network

Multi-protocol relay chaining for large-scale quantum key distribution networks

Yuan Cao(曹原)[1,†], Xiaosong Yu(郁小松)[2], Yongli Zhao(赵永利)[2], Chunhui Zhang(张春辉)[1], Xingyu Zhou(周星宇)[1], Jie Zhang(张杰)[2], and Qin Wang(王琴)[1]

[1] *Institute of Quantum Information and Technology, Nanjing University of Posts and Telecommunications, Nanjing* 210003, *China*

[2] *State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*

(Received 27 September 2024; revised manuscript received 6 November 2024; accepted manuscript online 8 November 2024)

As the first stage of the quantum Internet, quantum key distribution (QKD) networks hold the promise of providing long-term security for diverse users. Most existing QKD networks have been constructed based on independent QKD protocols, and they commonly rely on the deployment of single-protocol trusted relay chains for long reach. Driven by the evolution of QKD protocols, large-scale QKD networking is expected to migrate from a single-protocol to a multi-protocol paradigm, during which some useful evolutionary elements for the later stages of the quantum Internet may be incorporated. In this work, we delve into a pivotal technique for large-scale QKD networking, namely, multi-protocol relay chaining. A multi-protocol relay chain is established by connecting a set of trusted/untrusted relays relying on multiple QKD protocols between a pair of QKD nodes. The structures of diverse multi-protocol relay chains are described, based on which the associated model is formulated and the policies are defined for the deployment of multi-protocol relay chains. Furthermore, we propose three multi-protocol relay chaining heuristics. Numerical simulations indicate that the designed heuristics can effectively reduce the number of trusted relays deployed and enhance the average security level versus the commonly used single-protocol trusted relay chaining methods on backbone network topologies.

Keywords: quantum communications, quantum networks, trusted relay, untrusted relay

PACS: 03.65.–w, 03.67.Hk, 42.50.Ex, 42.79.Sz

DOI: 10.1088/1674-1056/ad9018 **CSTR:** 32038.14.CPB.ad9018

1. Introduction

In numerous fields of defense, finance, telecom, etc., massive confidential data is exchanged among diverse users across the classical Internet. These data are typically secured using cryptographic algorithms belonging to the family of classical cryptography. However, the classical cryptographic algorithms built on computational complexities may be compromised by the emerging powerful quantum computers.[1,2] By contrast, quantum cryptography holds the promise of providing information-theoretic security even in the presence of quantum computers. As one of the most popular applications belonging to the family of quantum cryptography, quantum key distribution[3,4] (QKD) is expected to open up a bright prospect for network and information security.

The basic functionality of QKD is negotiating secret keys between a pair of authorized users. Thus, QKD is essentially a key negotiation method, whose counterpart in the classical cryptography family may be exemplified by the Diffie–Hellman algorithm.[5] QKD also belongs to the branch of quantum communications, hence its basic elements are the QKD transmitter (QTx) and the QKD receiver (QRx) connected via a QKD link. In order to support key negotiation for numerous user pairs, QKD is required to be extended to network settings beyond a single link, ultimately resulting in a QKD network paradigm.[6] In recent years, a growing number of QKD networks have been deployed in both metropolitan[7–13] and backbone[14–16] by relying on optical fiber networks. Furthermore, an integrated space-to-ground QKD network has been constructed by relying on the optical fiber metropolitan and backbone networks as well as satellite–terrestrial free-space links.[17]

Given that the quantum no-cloning theorem prohibits quantum signals from being amplified, long-distance QKD has to rely on the aid of relays, especially in large-scale QKD networks. The end-to-end secret keys (also known as global secret keys) are generated by placing relays between the source and destination QKD nodes as well as chaining them together to form a so-called relay chain. The most cutting-edge relay is the quantum repeater,[18,19] but it is not yet mature enough to be employed in a real-world environment. As a compromise solution, trusted relays are commonly used to extend the relay chain to an arbitrary distance.[6] The trusted relay stores the local secret keys and forwards the global secret keys from source to destination QKD nodes in a segment-by-segment fashion. In practice, single-protocol trusted relay chains have been established relying on the QTx–QRx connectivity pattern

[†]Corresponding author. E-mail: yuancao@njupt.edu.cn

© 2025 Chinese Physical Society and IOP Publishing Ltd. All rights, including for text and data mining, AI training, and similar technologies, are reserved.

belonging to the family of single-point-to-point (SP2P) QKD protocols.[14–17] However, the trusted relays may be vulnerable to eavesdropping since they have knowledge of the global secret keys, hence they might become the weak points of security in a realistic QKD network.

To date, significant technical advances have been made in QKD protocols, while bringing additional connectivity patterns such as QTx–QRx–QTx and QRx–QTx–QRx belonging to the families of measurement-device-independent[20,21] (MDI) and entanglement-based[22,23] (EB) protocols, respectively. An MDI-QKD or EB-QKD protocol relies on an untrusted relay (containing the MDI-QRx or the EB-QTx) to considerably extend its secure distance. For example, the twin-field (TF) protocols belonging to MDI-QKD have reached the long distance of 833.8 km[24] and even 1002 km[25] in the laboratory. However, the nature of MDI and EB protocols does not allow the direct connection of two untrusted relays, hence the untrusted relay may need to be used together with the trusted relay for extending the end-to-end distance without limitations.

The existing QKD networks constitute the first stage of the quantum Internet (Qinternet).[26] More concretely, the Qinternet interconnects quantum devices relying on quantum communications for delivering new Internet techniques beyond the classical Internet. However, the single-protocol solution used in existing QKD networks can hardly fulfill the varying requirements originating from numerous users. Driven by the development of advanced QKD protocols, large-scale QKD networking is expected to evolve from a single-protocol to a multi-protocol paradigm, during which the appropriate QKD protocols can be deployed on demand. The optimal deployment problems of both single-protocol trusted relay chains[27] and single-protocol hybrid relay chains[28] have been addressed for single-protocol QKD networking. However, large-scale QKD networking originates a new research problem: multi-protocol relay chaining. In this context, how to optimize the deployment of multi-protocol relay chains and what benefits can be gained compared to the deployment of single-protocol relay chains need to be explored.

This paper aims to provide a comprehensive analysis of the multi-protocol relay chaining problem as well as perform a detailed comparison and evaluation for the deployment of multi-protocol and single-protocol relay chains. The major contributions of this work are summarized below. (i) We describe the structures of multi-protocol relay chains relying on independent or hybrid SP2P-QKD, MDI-QKD, and EB-QKD. (ii) We delve into the multi-protocol relay chain deployment problem, formulate the network model for QKD backbone networks with upgrading or construction purposes, as well as define the associated objective and policies. (iii) We propose three heuristics to facilitate the deployment of multi-protocol relay chains for QKD backbone networks, aiming for achieving the maximum end-to-end security level. (iv) We conduct a comparative evaluation of the proposed heuristics and the commonly used single-protocol trusted relay chaining methods under different circumstances in terms of deployment success probability, trusted relay quantity, and average security level.

The remainder of this paper is outlined as follows. Section 2 reviews the related work. Section 3 details the multi-protocol relay chain structures. The problem of multi-protocol relay chaining and the associated policies are formally elaborated in Section 4. The three heuristic algorithms for multi-protocol relay chain deployment are presented in Section 5. The performance evaluation and discussion are carried out in Section 6. Finally, Section 7 concludes this work.

2. Related work

This section briefly reviews the related work on QKD protocols and networks, with a special emphasis on the network layer perspective.

Since the pioneering QKD protocol (known as BB84 protocol) devised by Bennett and Brassard in 1984,[29] more and more advanced protocols have been invented. The QKD protocols can be grouped into different categories according to their specific physical characteristics. For example, the protocols are typically classified into the families of discrete-variable (DV) QKD and continuous-variable (CV) QKD based on encoding schemes. When it comes to the connectivity patterns of QTx and QRx, QKD protocols can be divided into three families, namely, SP2P-QKD, MDI-QKD, and EB-QKD, corresponding to the QTx–QRx, QTx–QRx–QTx, and QRx–QTx–QRx patterns, respectively. More concretely, the SP2P-QKD protocol family includes protocols such as BB84,[29] Grosshans-Grangier-2002 (GG02),[30] and coherent-one-way (COW),[31] which have been widely employed in realistic QKD systems. Furthermore, the family of MDI-QKD protocols comprises the original MDI[20] and TF[21] protocols, while the family of EB-QKD protocols can be exemplified by the Ekert-91[22] (E91) and Bennett-Brassard-Mermin-1992[23] (BBM92) protocols.

In reality, the available QKD protocols are not limited to the above-mentioned typical protocols and they are not equivalent in terms of realistic security, but that is not our focus in this work. A comprehensive overview of diverse QKD protocols and their realistic security can be found in Ref. [4]. Furthermore, advanced quantum secure direct communication (QSDC) protocols[32,33] can be incorporated in multi-protocol quantum networks to provide information security, which requires further investigations. Notably, the internet-working of multiple QKD protocols has become a valuable research topic

and is still in its infancy. In Ref. [34], the agile switching between BB84-QKD and MDI-QKD in a reconfigurable network was demonstrated. Guccione *et al.*[35] implemented the connection of nodes with mixed CV and DV encoding schemes by relying on an entanglement swapping protocol. Hence, the incorporation of multiple protocols in a QKD network is feasible. Furthermore, ITU-T has recently initiated several work items intending to specify the protocol framework as well as the interworking framework and requirements for QKD networks. For a realistic QKD backbone network reported in Ref. [17], the secret key rates of 28.1–235.4 kbps were attained over an average fiber length of 63.8 km.

In recent years, many QKD networks have been constructed based on independent QKD protocols. For example, the QKD metropolitan networks reported in Refs. [7–13] were deployed in the field relying on independent protocols belonging to MDI, SP2P, or EB QKD. As a result, the feasibility of deploying QKD networks based on independent connectivity patterns has been validated in real-world environments. On the other hand, the 2000 km Beijing–Shanghai (China)[16,17] and 121 km Cambridge–Ipswich (UK)[15] QKD backbone networks were constructed with the aid of trusted relay chains. In Ref. [36], a field trial of TF-QKD relying on an untrusted relay was realized over a 511 km fiber trunk connecting two non-adjacent metropolitan areas of Jinan and Qingdao, China. Additionally, significant experimental progress has been made in satellite-relayed QKD networks by exploiting the satellite as a trusted relay[37] and an untrusted relay,[38] but the focus of this paper is on fiber-based QKD networks.

To elaborate a little further, in addition to dark fiber-based QKD networks, several practical QKD networks have realized the coexistence of QKD and classical data signals by employing wavelength-division multiplexing (WDM) techniques.[8–11,15] Given that using dark fibers or installing new fibers may significantly increase costs, combining QKD with classical communications in existing optical networks holds the promise of facilitating the widespread deployment of QKD networks. To date, numerous network layer research efforts dedicating to the integration of QKD into existing optical fiber networks have been carried out,[39–43] aiming for empowering the compatibility and complementarity of QKD and optical networks.

With special respect to the relay chain deployment for QKD networks, the cost optimization for the optimal deployment of single-protocol trusted relay chains[27] and single-protocol hybrid trusted/untrusted relay chains[28] was investigated by developing the integer linear programming (ILP) models and the heuristics. However, to the best of the authors' knowledge, there is almost no research delving into the deployment of multi-protocol relay chains, which is potentially a pivotal challenge on the road to the large-scale QKD networks and the Qinternet.

3. Multi-protocol relay chain structures

In this section, we describe the structures of multi-protocol relay chains. Given that each connectivity pattern corresponds to multiple QKD protocols, the multi-protocol relay chains can be established relying on independent or hybrid connectivity patterns.

Figure 1 depicts the structures of multi-protocol relay chains based on independent SP2P-QKD, MDI-QKD, and EB-QKD. We define a chain segment as QTx–QRx, QTx–(QRx)–QTx, and QRx–(QTx)–QRx for SP2P, MDI, and EB QKD, respectively. A multi-protocol relay chain is established by connecting a set of chain segments, hence it can be extended segment-by-segment without constraints. In practice, a relay may require additional auxiliary equipments such as the key manager and optical switch,[27,28,44] but we only display the core components (i.e., QTx and QRx) essential for a relay chain in Fig. 1. Furthermore, the examples shown in Fig. 1 can be used to depict the single-protocol relay chains, where only one QKD protocol is employed in the relay chain.

The key negotiation mechanisms of the QKD protocols belonging to SP2P-QKD, MDI-QKD, and EB-QKD are outlined as follows.

SP2P-QKD: The protocols belonging to SP2P-QKD agree on the local secret keys between a pair of connected SP2P-QTx and SP2P-QRx, as exemplified by K_{A}, K_{B}, and K_{C} in Fig. 1(a). More concretely, the SP2P-QTx prepares the quantum states and sends them to the SP2P-QRx for measurement through a unidirectional quantum channel. Subsequently, the SP2P-QRx and SP2P-QTx perform key distillation (including sifting and post-processing)[44] by exchanging classical information via a bidirectional classical channel to generate the final secret keys. A QKD link covers the above-mentioned quantum and classical channels. More details of the associated SP2P-QKD protocols can be found in Refs. [29–31].

MDI-QKD: The protocols belonging to MDI-QKD agree on the local secret keys between a pair of connected MDI-QTxs with an MDI-QRx placed in the middle, as exemplified by K_{D} and K_{E} in Fig. 1(b). Typically, the MDI-QTxs are in symmetric locations to their connected MDI-QRx, that is, the distances from two MDI-QTxs to the MDI-QRx are symmetric with similar channel losses. However, the channel asymmetry may be remedied by adding a tailored length of fiber to the shorter channel or by emerging asymmetric protocols.[28,45,46] Both MDI-QTxs produce quantum signals and send them to the MDI-QRx via the quantum channels. The MDI-QRx then carries out an interference measurement on the incoming quantum signals and publicly declares the measurement results to MDI-QTxs. The two MDI-QTxs exchange

classical information to distill the final secret keys. More details of the associated MDI-QKD protocols can be found in Refs. [20,21,47,48].

EB-QKD: The protocols belonging to EB-QKD agree on the local secret keys between a pair of connected EB-QRxs with an intermediate EB-QTx, as exemplified by K_{F} and K_{G} in Fig. 1(c). Similar to the MDI-QRx, the EB-QTx can be placed symmetrically to its connected EB-QRxs for achieving better secret key rates, while allowing asymmetric channels as well. The EB-QTx prepares the entangled states (i.e., entangled photon pairs) and distributes them to the EB-QRxs via the quantum channels. Each EB-QRx then measures its received photons belonging to the entangled photon pairs. After classical information processing and interaction, the final secret keys are shared between the two connected EB-QRxs. More details of the associated EB-QKD protocols can be found in Refs. [22,23].

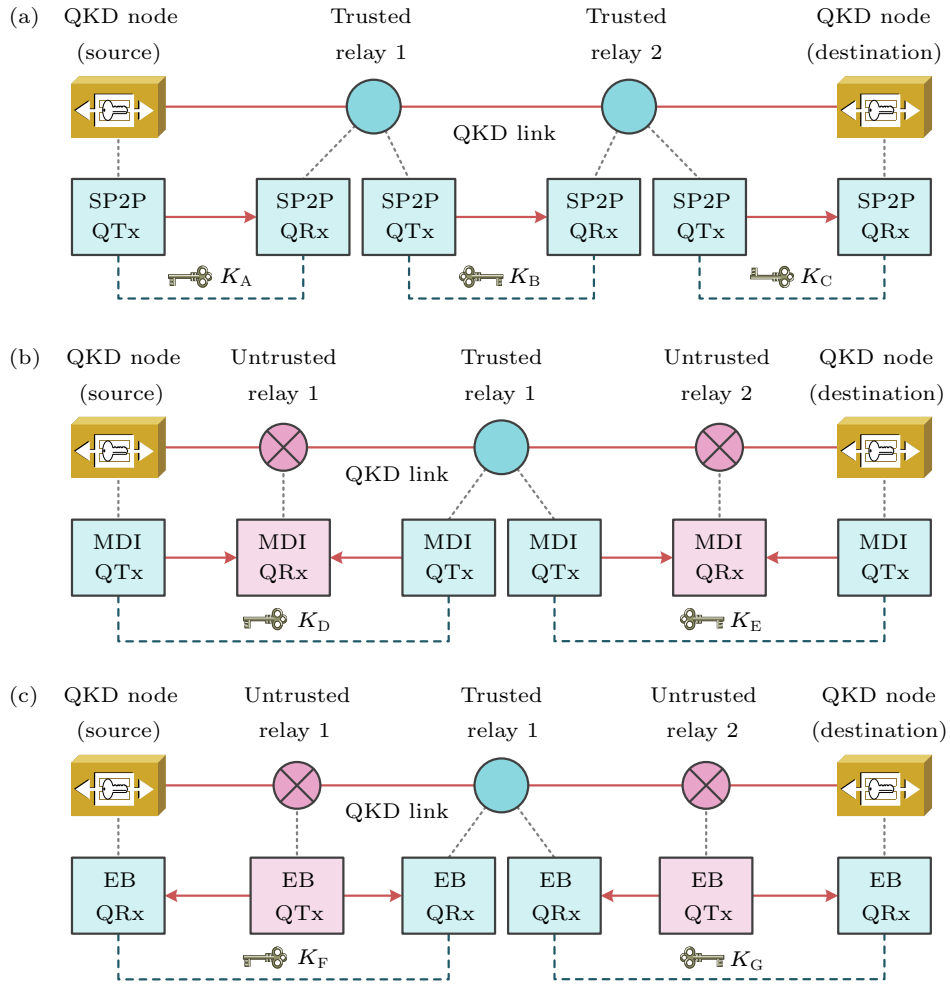


Fig. 1. Illustration of the structures of multi-protocol relay chains based on independent (a) SP2P-QKD; (b) MDI-QKD; and (c) EB-QKD.

As illustrated in Fig. 1, a SP2P-QKD-based multi-protocol relay chain involves QKD nodes and trusted relays, whereas a multi-protocol relay chain relying on MDI-QKD or EB-QKD involves QKD nodes, trusted relays, and untrusted relays. The QKD node can serve as a terminal node (e.g., source or destination node) for a relay chain. In particular, the global secret keys are shared between a pair of QKD nodes and supplied to the users co-located with the corresponding QKD nodes for securing their end-to-end communications.

Again, the trusted relay is used to forward the global secret keys from the source QKD node to the destination QKD node in a segment-by-segment fashion. An example of the trusted relay chain is shown in Fig. 1(a), while the relaying process performed at each node is explained as follows:

1. Source QKD node encrypts the global secret key K_{X} using K_{A} and sends the ciphertext $K_{\mathrm{A}} \oplus K_{\mathrm{X}}$ to trusted relay 1.

2. Trusted relay 1 decrypts K_{X} based on $K_{\mathrm{A}} \oplus (K_{\mathrm{A}} \oplus K_{\mathrm{X}}) = K_{\mathrm{X}}$, then encrypts K_{X} using K_{B} and sends the ciphertext $K_{\mathrm{B}} \oplus K_{\mathrm{X}}$ to trusted relay 2.

3. Trusted relay 2 decrypts K_{X} based on $K_{\mathrm{B}} \oplus (K_{\mathrm{B}} \oplus K_{\mathrm{X}}) = K_{\mathrm{X}}$, then encrypts K_{X} using K_{C} and sends the ciphertext $K_{\mathrm{C}} \oplus K_{\mathrm{X}}$ to destination QKD node.

4. Destination QKD node decrypts K_X based on $K_C \oplus (K_C \oplus K_X) = K_X$. Accordingly, the global secret key K_X is shared between the source and destination QKD nodes.

In the above steps, the one-time pad algorithm[49] has to be used for encryption and decryption, which conducts a bitwise XOR operation ($\oplus$) between the secret keys of the same string length, aiming for maintaining the information-theoretic security of secret keys. Some other optional relaying schemes based on the trusted relay can be found in the ITU-T Y.3803 recommendation.[50] The security of trusted relays relies on an idealized assumption that the relays are trustable (i.e., inaccessible to eavesdroppers), hence they may constitute the weak security points in practice.

By contrast, the untrusted relay has to rely on specific protocols belonging to MDI-QKD or EB-QKD, which contains either the MDI-QRx or the EB-QTx. The untrusted relay has better security than the trusted relay, because it does not rely on any security assumptions and its security is not compromised even in the presence of an eavesdropper. Hence, MDI-QKD and EB-QKD close the security loopholes on the detector and source sides, respectively. Given the fact that the direct linking of two untrusted relays based on MDI/EB-QKD is not allowed, the untrusted relay is required to be employed in conjunction with the trusted relay to extend the end-to-end distance, as depicted in Figs. 1(b) and 1(c). Additionally, a special relay chain relying on only one untrusted relay can only implement MDI-QKD or EB-QKD within a limited distance between a pair of connected MDI-QTxs or EB-QRxs.

On the other hand, several examples of the structures of multi-protocol relay chains based on hybrid SP2P/MDI, SP2P/EB, MDI/EB, and SP2P/MDI/EB based QKD are shown in Figs. 2(a)–2(d), respectively. The SP2P-QKD, MDI-QKD, and EB-QKD are compatible in a multi-protocol relay chain, since each chain segment used for producing the local secret keys is independent. Notably, the blending of SP2P-QKD, MDI-QKD, and EB-QKD may result in various combinations of the chain segments for a multi-protocol relay chain, which may be influenced by the number of relays required. Furthermore, the combination of chain segments based on hybrid connectivity patterns facilitates the accommodation of diverse networking environments. As an example, when MDI-QKD or EB-QKD encounters an even number of relays for establishing a relay chain, the last chain segment can be implemented by SP2P-QKD since it cannot fully exploit the merits of MDI/EB-QKD.

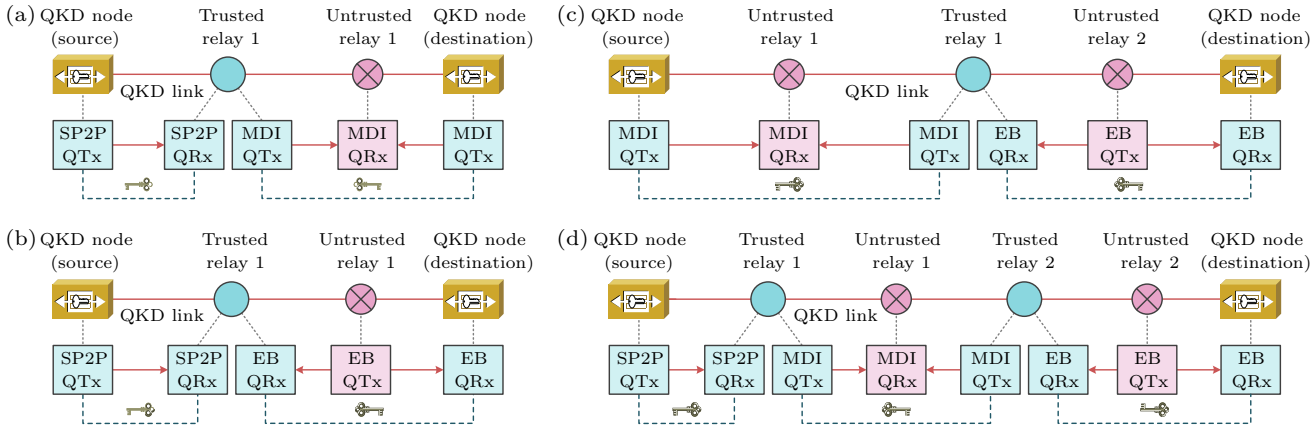


Fig. 2. Illustration of the structures of multi-protocol relay chains based on hybrid (a) SP2P/MDI; (b) SP2P/EB; (c) MDI/EB; and (d) SP2P/MDI/EB QKD.

4. Problem formulation and policy description

In this section, we discuss the multi-protocol relay chaining problem, with a focus on the relatively large QKD network relying on trusted/untrusted relays, especially on the QKD backbone network. We formulate the associated network model, provide the definitions, as well as describe the objective and policies.

4.1. Network model

We model a backbone network topology as $G(V, E)$, where V and E denote the sets of backbone nodes and physical links, respectively. The length of a physical link $e \in E$ is denoted by d_e. The backbone node is a terminal node that can act as a QKD node or an optical backbone node. A physical link connects two adjacent backbone nodes. The backbone network is the infrastructure over which the multi-protocol relay chains are planned to be deployed. Based on the status of the backbone network in different periods, we consider the following two network paradigms.

1) The $G(V, E)$ represents the existing QKD backbone network: The motivation for deploying multi-protocol relay chains is to upgrade the existing QKD backbone network to improve its performance. The set of relays in the existing QKD backbone network is denoted by N, where each relay always has a fixed location known in advance without being altered during the upgrade phase. The set of QKD links in

the existing QKD backbone network is denoted by L, where a QKD link connects two adjacent relays.

2) The $G(V, E)$ represents the existing optical fiber backbone network: The motivation for deploying multi-protocol relay chains is to construct a new QKD backbone network over the existing optical fiber backbone network. The relay location can be flexible without pre-knowledge, while the topology of the QKD backbone network is the same as that of the existing optical fiber backbone network.

The set of wavelength channels reserved for QKD on each physical link is denoted by W, which is predetermined to avoid the wavelength overlapping usage between QKD and classical data communications. It is important to note that both the commonly used dark fibers and WDM techniques are assumed to be available for multi-protocol relay chain deployment. Hence, the wavelength channels reserved for QKD may belong to a single fiber or a group of fibers. The set of available QKD protocols is denoted by P, which may consist of SP2P-QKD, MDI-QKD, and EB-QKD protocols.

A multi-protocol relay chain is established between a pair of QKD nodes. We model a multi-protocol relay chain request as $r(s_r, d_r, w_r)$, where s_r and d_r denote the source and destination QKD nodes of r, respectively, and w_r denotes the number of wavelength channels required for r. Let R denote the set of all multi-protocol relay chain requests to be deployed.

4.2. Definitions

Definition 1 (end-to-end security level of a relay chain): The end-to-end security level of a relay chain is directly affected by the number of trusted relays, which decreases as the quantity of its owned trusted relays increases. Given that a trusted relay may be either risky or risk-free in pessimistic realistic scenarios, in this work we assume a fixed potential risk probability of m for each trusted relay under certain safeguard countermeasures. Then, we define the end-to-end security level of a multi-protocol relay chain request r as

$$\eta_r = (1-m)^{N_{\mathrm{TR}}^r}, \tag{1}$$

where N_{TR}^r denotes the number of trusted relays deployed for r.

Definition 2 (deployment success probability): The success probability of multi-protocol relay chain deployment may be limited by the wavelength resources and requirements. We define the deployment success probability as

$$Z = \frac{|F|}{|R|}, \tag{2}$$

where F is the set of successfully deployed multi-protocol relay chain requests (i.e., the requests successfully allocated with their required wavelength channels).

Definition 3 (average security level of a QKD backbone network): The QKD backbone network consists of the successfully deployed multi-protocol relay chains. The average number of trusted relays for each successfully deployed multi-protocol relay chain is formulated as

$$N_{\mathrm{AVG}}^F = \frac{\sum_{r\in F} N_{\mathrm{TR}}^r}{|F|}. \tag{3}$$

Based on Definition 1 and Eq. (3), we define the average security level of a QKD backbone network as

$$S_F = (1-m)^{N_{\mathrm{AVG}}^F}. \tag{4}$$

It is important to note that the security level defined and discussed in this paper is characterized in the network layer of the QKD network, which is only used as the metric for comparing the end-to-end security performance of single-protocol and multi-protocol relay chains, and it is not equivalent to the security considered in other domains. Indeed, how to test and examine the value of m is still an open issue. For example, the value of m may be characterized by the proportion of the vulnerable components to all components enclosed in the trusted relay. The ideal value of m should be 0, which can be achieved with the untrusted relays relying on MDI/EB-QKD.

In order to achieve a preferable secret key rate for each multi-protocol relay chain, the direct connection of non-adjacent relays relying on intermediate relay bypass is not allowed. In addition, the QKD node has to be a trusted node protected against any intrusion or attack, since it has knowledge of the real secret keys. Hence, the relays in the QKD nodes are not involved in the multi-protocol relay chain deployment. We assume that the desired secret key rate can be achieved for each chain segment by choosing the suitable QKD protocol. Furthermore, multiple QKD protocols can be flexibly deployed to fit various special circumstances, such as SP2P-QKD without relay between source and destination QKD nodes, MDI/EB-QKD over asymmetric channels, as well as the last chain segment with a fiber length less than half of the achievable distance of MDI-QKD or EB-QKD.

4.3. Objective and policies

In contrast to minimizing the deployment cost addressed in Refs. [27,28], the objective considered in the multi-protocol relay chaining problem for large-scale QKD networks is to minimize the number of trusted relays deployed for each multi-protocol relay chain, ultimately resulting in the maximum end-to-end security level. Given the fact that directly connecting two untrusted relays is not allowed, we present an interleaving scheme for deploying trusted and untrusted relays, aiming for the maximum usage of untrusted relays. As illustrated in Fig. 3, we introduce two policies (named trusted relay first and untrusted relay first) for deploying

trusted/untrusted relays based on the interleaving scheme. The trusted relay first and untrusted relay first policies deploy the trusted relay and the untrusted relay as the first relay connected to the source QKD node of the multi-protocol relay chain, respectively.

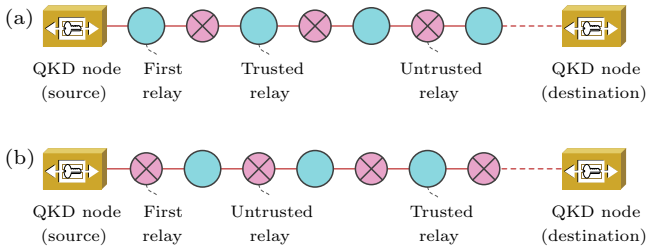


Fig. 3. Illustration of (a) trusted relay first and (b) untrusted relay first policies for deploying trusted/untrusted relays based on the interleaving scheme.

Let N_r represent the total number of relays deployed for a multi-protocol relay chain request r, which can be either an odd or an even number. Then, the numbers of trusted relays deployed for r using the untrusted relay first policy and the trusted relay first policy based on the interleaving scheme are respectively formulated as

$$N^r_{\mathrm{URF}} \leq \lfloor N_r/2 \rfloor, \tag{5}$$

$$N^r_{\mathrm{TRF}} \geq \lceil N_r/2 \rceil. \tag{6}$$

In view of $N^r_{\mathrm{URF}} \leq N^r_{\mathrm{TRF}}$, for each multi-protocol relay chain request that relies on an interleaving scheme to deploy its required trusted and untrusted relays, the number of trusted relays deployed with the untrusted relay first policy is no larger than that with the trusted relay first policy. Notably, this is applicable to both manners for passing the intermediate QKD nodes defined in subsequent paragraphs.

As a result, the untrusted relay first policy based on the interleaving scheme is utilized in this work to achieve a higher security level, where the set P is assumed to cover at least one SP2P-QKD protocol as well as one protocol belonging to MDI-QKD or EB-QKD. Furthermore, the number of trusted relays deployed for a multi-protocol relay chain request is directly associated with the network model, as formulated below.

1) Number of trusted relays deployed for a multi-protocol relay chain request over the existing QKD backbone network: Let N_e denote the number of relays on a physical link e in the existing QKD backbone network. The minimum number of trusted relays deployed on a physical link e is formulated as

$$N^e_{\mathrm{TR}} = \lfloor N_e/2 \rfloor. \tag{7}$$

Based on Eq. (7), the number of trusted relays deployed for a multi-protocol relay chain request r over the existing QKD backbone network is formulated as

$$N^r_{\mathrm{TR}} = \sum_{e \in E} x^r_e N^e_{\mathrm{TR}}, \tag{8}$$

where x^r_e is a Boolean variable that equals 1 if link e is occupied by the multi-protocol relay chain request r, and 0 otherwise.

2) Number of trusted relays deployed for a multi-protocol relay chain request over the existing optical fiber backbone network: Given the location of each relay is not identified in advance, we define the distance between two adjacent relays belonging to an interval $[d_{\min}, d_{\max}]$, which can cover both fixed and flexible distances for a more general consideration. In practice, there may exist intermediate QKD nodes between the source and destination QKD nodes of a multi-protocol relay chain. We define two manners for passing the intermediate QKD nodes, namely, transparent and opaque, as depicted in Fig. 4. More concretely, the intermediate QKD nodes are bypassed by relying on optical switching techniques in the former one, while the QKD links are terminated at the intermediate QKD nodes equipped with trusted relays in the latter one.

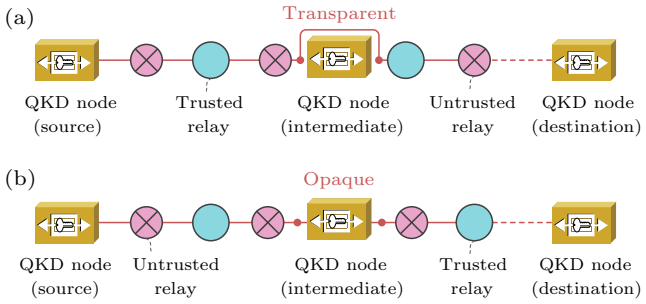


Fig. 4. Illustration of (a) transparent and (b) opaque manners for passing the intermediate QKD nodes.

The total distance between the source and destination QKD nodes of a multi-protocol relay chain request r is formulated as

$$D_r = \sum_{e \in E} x^r_e d_e. \tag{9}$$

Based on Eq. (9), the minimum and maximum numbers of relays deployed for a multi-protocol relay chain request r in a transparent manner are formulated as

$$\alpha^r_{\min} = \lceil D_r/d_{\max} - 1 \rceil, \tag{10}$$

$$\alpha^r_{\max} = \lceil D_r/d_{\min} - 1 \rceil. \tag{11}$$

Let α_r represent the number of relays deployed for the multi-protocol relay chain request r in a transparent manner. α_r belongs to an interval $[\alpha^r_{\min}, \alpha^r_{\max}]$. The untrusted relay first policy is enforced on the path of the multi-protocol relay chain. Then, the number of trusted relays deployed for a multi-protocol relay chain request r is formulated as

$$N^r_{\mathrm{TR}} = \lfloor \alpha_r/2 \rfloor. \tag{12}$$

For an opaque manner, the minimum and maximum numbers of relays deployed on physical link e are formulated as

$$\alpha^e_{\min} = \lceil d_e/d_{\max} - 1 \rceil, \tag{13}$$

$$\alpha^e_{\max} = \lceil d_e/d_{\min} - 1 \rceil. \tag{14}$$

Let α_e denote the number of relays deployed on physical link e in an opaque manner. α_e belongs to an interval $[\alpha^e_{\min}, \alpha^e_{\max}]$. The untrusted relay first policy is performed on each physical link along the path of the multi-protocol relay chain. Then, the number of trusted relays deployed for a multi-protocol relay chain request r is formulated as

$$N^r_{\mathrm{TR}} = \sum_{e \in E} x^r_e \lfloor \alpha_e/2 \rfloor. \tag{15}$$

5. Heuristic algorithm design

Based on the above formulated network model and defined policies, we present three heuristics in this section to facilitate the deployment of multi-protocol relay chains for large-scale QKD networks. These three heuristics are named as existing network upgrade (ENU), transparent intermediate node (TIN), and opaque intermediate node (OIN) based multi-protocol relay chaining (MPRC) algorithms, whose detailed pseudocodes are shown in Algorithms 1, 2, and 3, respectively. More concretely, Algorithm 1 is designed for upgrading the existing QKD backbone network, while Algorithms 2 and 3 are designed for constructing a new QKD backbone network over the existing optical fiber backbone network based on the above-mentioned transparent and opaque manners for passing the intermediate QKD nodes, respectively. Lines 1 and 3 in the three algorithms are for the initialization, while lines 25, 23, and 28 in Algorithms 1, 2, and 3 return the results of multi-protocol relay chain deployment, respectively. Based on the returned results, the values of Z and S_F can be calculated.

In Algorithm 1, the for-loop covering lines 2 to 24 carries out the ENU-MPRC by processing all multi-protocol relay chain requests to be deployed, aiming for upgrading the existing QKD backbone network. Each multi-protocol relay chain request $r \in R$ is handled in lines 3 to 23. Given that the path for each multi-protocol relay chain request in the existing QKD backbone network is known in advance, line 4 finds the path between the source and destination QKD nodes of r, and line 5 finds all physical links on this path. The inner for-loop covering lines 6 to 16 calculates the minimum number of trusted relays deployed for each request that is successfully assigned with the required wavelength channels.

In Algorithms 2 and 3, the for-loops covering lines 2–22 and 2–27 accomplish the TIN-MPRC and OIN-MPRC by handling all multi-protocol relay chain requests to be deployed over the existing optical fiber backbone network, respectively. Each multi-protocol relay chain request $r \in R$ is processed in lines 3–21 and 3–26 of Algorithms 2 and 3, respectively. For r in both algorithms, the shortest path between its source and destination QKD nodes is computed and selected using Dijkstra's algorithm (line 4 in Algorithms 2 and 3), with the intention of facilitating the minimization of the number of relays deployed. Lines 5 to 8 in Algorithm 2 calculate the total distance between the source and destination QKD nodes of r.

Algorithm 1: ENU-MPRC algorithm

Input: $G(V, E), N, L, W, P, R, N_e$.

Output: F, N^r_{TR} for $r \in F$, result of multi-protocol relay chain deployment over the existing QKD backbone network, updated network status.

```
1:  initialize F ← ∅;
2:  for each multi-protocol relay chain request r ∈ R do
3:      initialize N^r_TR ← 0;
4:      find the path p_r between s_r and d_r;
5:      find all physical links on p_r and insert them into set E(p_r);
6:      for each physical link e ∈ E(p_r) do
7:          find available wavelength channels in W on e and insert them into set W_e;
8:          if |W_e| ≥ w_r then
9:              select w_r wavelength channels from W_e with first-fit algorithm for r;
10:             mark Λ as SUCCESS;
11:             N^r_TR ← N^r_TR + ⌊N_e/2⌋;
12:         else
13:             mark Λ as FAILURE;
14:             break;
15:         end
16:     end
17:     if Λ is marked as SUCCESS then
18:         insert r into F;
19:         record N^r_TR for r;
20:     else
21:         release the selected wavelength channels for r;
22:     end
23:     update network status;
24: end
25: return F, N^r_TR for r ∈ F, result of multi-protocol relay chain deployment over the existing QKD backbone network, updated network status.
```

Algorithm 2: TIN-MPRC algorithm

Input: $G(V, E)$, d_e, W, P, R, $d_{\min}$, $d_{\max}$.

Output: F, N_{TR}^r for $r \in F$, result of multi-protocol relay chain deployment over the existing optical fiber backbone network, updated network status.

1: initialize $F \leftarrow \emptyset$;
2: **for** *each multi-protocol relay chain request* $r \in R$ **do**
3: initialize $N_{\mathrm{TR}}^r \leftarrow 0$, $D_r \leftarrow 0$;
4: compute and select the shortest path p_r between s_r and d_r with *Dijkstra's* algorithm;
5: find all physical links on p_r and insert them into set $E(p_r)$;
6: **for** *each physical link* $e \in E(p_r)$ **do**
7: $D_r \leftarrow D_r + d_e$;
8: **end**
9: find available wavelength channels in W on p_r and insert them into set $W(p_r)$;
10: **if** $|W(p_r)| \geq w_r$ **then**
11: select w_r wavelength channels from $W(p_r)$ with *first-fit* algorithm for r;
12: $\alpha_{\min}^r \leftarrow \lceil D_r/d_{\max} - 1 \rceil$;
13: $\alpha_{\max}^r \leftarrow \lceil D_r/d_{\min} - 1 \rceil$;
14: identify α_r randomly from $[\alpha_{\min}^r, \alpha_{\max}^r]$;
15: $N_{\mathrm{TR}}^r \leftarrow \lfloor \alpha_r/2 \rfloor$;
16: **else**
17: **continue**;
18: **end**
19: insert r into F;
20: record N_{TR}^r for r;
21: update network status;
22: **end**
23: **return** F, N_{TR}^r for $r \in F$, result of multi-protocol relay chain deployment over the existing optical fiber backbone network, updated network status.

Algorithm 3: OIN-MPRC algorithm

Input: $G(V, E)$, d_e, W, P, R, $d_{\min}$, $d_{\max}$.

Output: F, N_{TR}^r for $r \in F$, result of multi-protocol relay chain deployment over the existing optical fiber backbone network, updated network status.

1: initialize $F \leftarrow \emptyset$;
2: **for** *each multi-protocol relay chain request* $r \in R$ **do**
3: initialize $N_{\mathrm{TR}}^r \leftarrow 0$;
4: compute and select the shortest path p_r between s_r and d_r with *Dijkstra's* algorithm;
5: find all physical links on p_r and insert them into set $E(p_r)$;
6: **for** *each physical link* $e \in E(p_r)$ **do**
7: find available wavelength channels in W on e and insert them into set W_e;
8: **if** $|W_e| \geq w_r$ **then**
9: select w_r wavelength channels from W_e with *first-fit* algorithm for r;
10: mark Λ as SUCCESS;
11: $\alpha_{\min}^e \leftarrow \lceil d_e/d_{\max} - 1 \rceil$;
12: $\alpha_{\max}^e \leftarrow \lceil d_e/d_{\min} - 1 \rceil$;
13: identify α_e randomly from $[\alpha_{\min}^e, \alpha_{\max}^e]$;
14: $N_{\mathrm{TR}}^r \leftarrow N_{\mathrm{TR}}^r + \lfloor \alpha_e/2 \rfloor$;
15: **else**
16: mark Λ as FAILURE;
17: **break**;
18: **end**
19: **end**
20: **if** Λ *is marked as* SUCCESS **then**
21: insert r into F;
22: record N_{TR}^r for r;
23: **else**
24: release the selected wavelength channels for r;
25: **end**
26: update network status;
27: **end**
28: **return** F, N_{TR}^r for $r \in F$, result of multi-protocol relay chain deployment over the existing optical fiber backbone network, updated network status.

The main difference between Algorithms 2 and 3 is the manner for passing the intermediate QKD nodes between the source and destination QKD nodes of r, where the transparent and opaque intermediate QKD nodes are involved, respectively. In this context, lines 9–18 and 5–19 in Algorithms 2 and 3 calculate the minimum number of trusted relays deployed for each request that is successfully assigned with the required wavelength channels, respectively. In the case of a flexible distance between two adjacent relays, the number of relays deployed for r is identified randomly from the potential relay quantity

interval.

Furthermore, a simple and efficient *first-fit* algorithm is utilized for allocating the available wavelength channels to each successfully deployed multi-protocol relay chain request. Such an algorithm has been widely employed for resource allocation,[27,28,39,40] where all available resource units are numbered and an available resource unit with a lower serial number is given a higher priority to be selected. Each successfully deployed r is accommodated in F and the number of trusted relays deployed for r is recorded, both of which are implemented by lines 18–19, 19–20, and 21–22 in Algorithms 1, 2, and 3, respectively.

The complexities of the designed three heuristics for MPRC are discussed below. In the worst case, the time complexities are $O(|V||W|)$, $O(|E|+|V|\log|V|+|W|)$, and $O[|E|+|V|\ (\log|V|+|W|)]$ for processing one multi-protocol relay chain request in Algorithms 1, 2, and 3, respectively.

6. Performance evaluation and discussion

In this section, we conduct numerical simulations to analyze the proposed three MPRC heuristic algorithms. To evaluate them against the commonly used single-protocol trusted relay chaining methods for practical QKD backbone networks,[15,17,27] we introduce three benchmark algorithms (named ENU-BM, TIN-BM, and OIN-BM) corresponding to the three MPRC heuristics. In fact, the TIN-BM algorithm is essentially the same as the cost-efficient QKD networking (CEQN) algorithm presented in Ref. [27], while the other two benchmark algorithms are redesigned according to the associated network paradigms and MPRC heuristics. Each benchmark algorithm relies on the number of all relays to characterize the security level, where each relay is set as the trusted relay based on a single SP2P-QKD protocol. Hence, the benchmark algorithms can only accommodate SP2P-QKD-based single-protocol relay chain requests. The available protocols for multi-protocol relay chain requests cover diverse protocols belonging to SP2P-QKD, MDI-QKD, and EB-QKD. Further, we carry out a comparative evaluation of the MPRC heuristics and their benchmarks in terms of deployment success probability, trusted relay quantity, and average security level.

As depicted in Fig. 5, two backbone network topologies are employed in simulations. Based on the scope of the designed heuristics described in Section 5, an existing QKD backbone network comprising four backbone nodes (i.e., QKD nodes) and 28 trusted relays in Fig. 5(a) is adopted for evaluating the ENU-MPRC algorithm. It involves a bus network topology belonging to the Beijing–Shanghai QKD backbone network (called BSQNET).[17] As shown in Fig. 5(b), an existing large optical fiber backbone network (commonly known as USNET) with 24 backbone nodes[27,28] is used for evaluating the TIN-MPRC and OIN-MPRC algorithms. The location of each trusted relay is fixed with pre-knowledge on the BSQNET topology, while the distance (in units of km) of each physical link is indicated on the USNET topology.

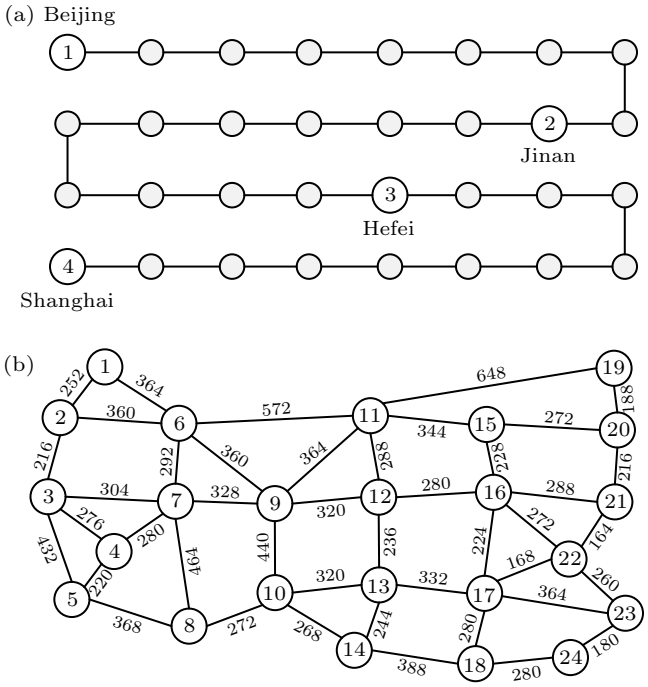


Fig. 5. Backbone network topologies employed in simulations: (a) BSQNET topology;[17] (b) USNET topology.[27,28]

Given that each single/multi-protocol relay chain request can normally fulfill the known secret key demands between its source and destination QKD nodes, each QKD (backbone) node pair may trigger one or more relay chain requests to satisfy current or future secret key demands. Based on the assumption given in Section 4, the specific secret key rate of each relay chain request is not involved in simulations. We set the number of relay chain requests within [3, 27] and [20, 180] on the BSQNET and USNET topologies, respectively, aiming to discuss the upgrading or construction of QKD backbone networks. The value of m is assumed to be 10%. Specifically, each relay chain request is randomly generated between any two backbone nodes. The results are averaged from 1000 independent simulations for maintaining sufficient statistical accuracy.

6.1. Different wavelength resources and requirements

We consider different wavelength resources/requirements to compare different heuristics. The following three cases are defined in the performance comparison: case-1, $|W|=40$, $w_r=2$; case-2, $|W|=20$, $w_r=2$; case-3, $|W|=40$, $w_r\in[2,4]$. More concretely, the number of wavelength channels reserved for QKD (i.e., wavelength resource) on each physical link is set to 40 or 20, while the number of wavelength channels required (i.e., wavelength requirement) for each relay chain request is set to 2 or within [2, 4]. Each relay chain request can

optionally use two or more wavelength channels, since a wavelength channel for exchanging quantum signals and a wavelength channel for synchronization are typically essential, but other classical functions such as key distillation and key management for QKD can be implemented relying on individual wavelength channels or classical data channels.[27,28,44] A span of 50–100 km between two adjacent relays is employed, which is derived from a realistic QKD backbone network.[17]

The deployment success probability versus the number of relay chain requests is shown in Fig. 6, where the BSQNET and USNET topologies are adopted in the heuristics associated with ENU and TIN/OIN, respectively. It can be observed that the deployment success probability for each algorithm maintains at 1 when the number of relay chain requests is relatively small, and then it declines as the number of relay chain requests rises. This is because the increased wavelength requirements of relay chain requests cannot be fulfilled by the limited wavelength resources. In addition, when the number of relay chain requests is relatively large, e.g., more than 12 and 40 in Figs. 6(a) and 6(b)/6(c), respectively, the deployment success probability reduces with $|W|$ decreasing, which stems from the decrease in the total available wavelength resources. The deployment success probability also decreases as the range of w_r expands, because the total wavelength requirements for establishing relay chains increase. In particular, the deployment success probability of the MPRC-oriented algorithm is the same as that of its benchmark algorithm in each case. This reflects that the deployment success probability is not influenced by the QKD protocols. Further, from Figs. 6(b) and 6(c) we can see that the deployment success probability of the OIN-based algorithm is a little higher than that of the TIN-based algorithm in the context of a large number of relay chain requests. The reason is that the TIN-based heuristics are subject to the wavelength continuity constraint in the wavelength allocation stage.

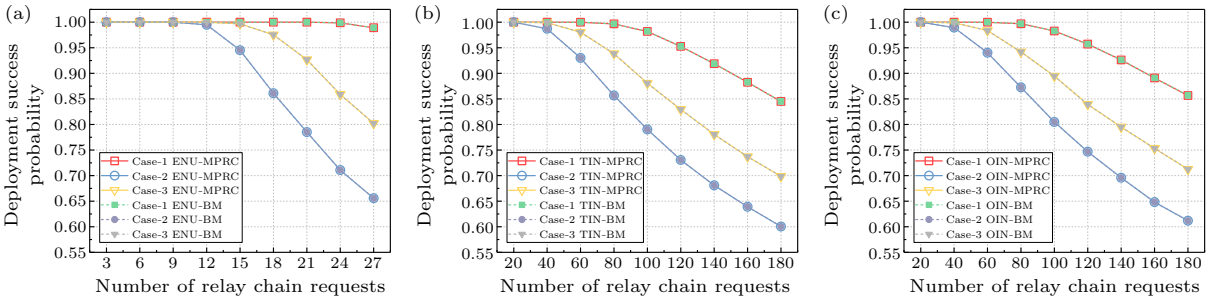


Fig. 6. Deployment success probability versus number of relay chain requests: (a) ENU-MPRC on the BSQNET topology; (b) TIN-MPRC on the USNET topology; (c) OIN-MPRC on the USNET topology.

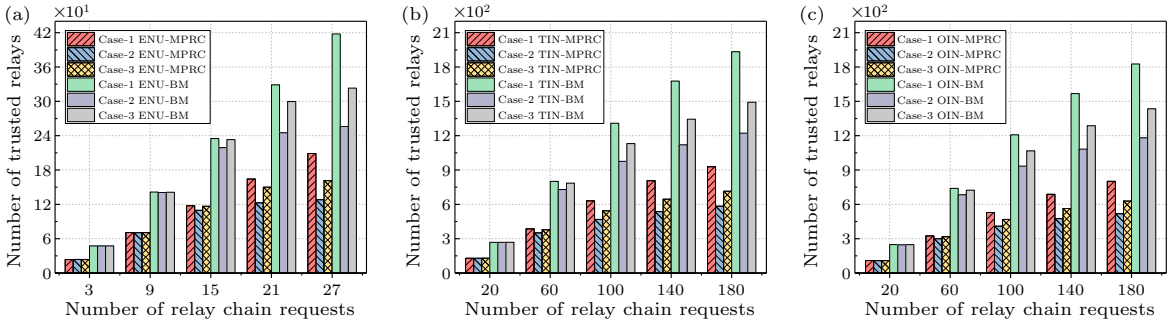


Fig. 7. Number of trusted relays versus number of relay chain requests: (a) ENU-MPRC on the BSQNET topology; (b) TIN-MPRC on the USNET topology; (c) OIN-MPRC on the USNET topology.

The number of trusted relays versus the number of relay chain requests is plotted in Fig. 7. Similar to Fig. 6, these results are obtained based on the heuristics associated with ENU and TIN/OIN for BSQNET and USNET topologies, respectively. The number of trusted relays grows as the number of relay chain requests rises. Hence the trusted relay quantity is directly related to the number of relay chain requests. It should be noted that the number of trusted relays shown in Fig. 7 does not reflect the number of relay locations, since many relays belonging to different relay chains may be placed at the same physical location. Besides, the number of trusted relays may partially reveal the QTx/QRx usage and the deployment cost, but we do not cover such analysis in this work. It can be seen that the number of trusted relays diminishes with the decrease of $|W|$ or the expanding range of w_r. This can be explainable by analyzing Fig. 6, where the number of successfully deployed relay chain requests decreases. However, in each case, the number of trusted relays for the OIN-based algorithm displayed in Fig. 7(c) is reduced compared to that for the TIN-based algorithm displayed in Fig. 7(b). This is due to the fact that the opaque manner can fully capitalize on the intermediate QKD nodes equipped with trusted relays. Notably, the num-

ber of trusted relays for the MPRC-oriented algorithm is much lower than that for its corresponding benchmark, because the usage of untrusted relays based on MDI-QKD or EB-QKD is maximized, replacing many of the trusted relays relying on SP2P-QKD used in the benchmark algorithm. As a result, the number of trusted relays can be considerably reduced by employing the proposed MPRC heuristics.

Figure 8 shows the average security level versus the number of relay chain requests on two backbone network topologies according to the three MPRC heuristics and their benchmarks. From Fig. 8 we can find that the average security level first keeps stable with a small number of relay chain requests, and then it rises as the number of relay chain requests increases. This indicates that the variation of the deployment success probability can result in an unstable average security level. Specifically, when the number of relay chain requests becomes relatively large, the average security level corresponding to a lower deployment success probability (e.g., in the context of a lower $|W|$ or an expanding range of w_r) is higher than that corresponding to a larger one. In each case, the average security level for the OIN-based algorithm shown in Fig. 8(c) is higher than that for the TIN-based algorithm shown in Fig. 8(b) due to the fact that the opaque manner utilized in the OIN-based algorithm facilitates a reduction in the number of trusted relays deployed. Nonetheless, this does not mean that the transparent manner always exhibits the worse performance, since these two manners are not equivalent in the QKD node cost, space, and scalability. Further, the MPRC-oriented algorithm significantly outperforms its benchmark algorithm in terms of the average security level. This phenomenon can be explainable based on the above analysis of the reduced number of trusted relays shown in Figs. 7(b) and 7(c).

Based on Fig. 8, the average security level enhancements of the proposed three MPRC heuristics versus their benchmarks in different cases are listed in Table 1. In each case, the average security level enhancement essentially declines as the number of relay chain requests rises, which stems from the decrease in the deployment success probability. When the ENU-MPRC algorithm is adopted, the average security level enhancement ranges from 114% to 130%, where the number of relays on each physical link of the BSQNET topology is a fixed even number. In particular, the combination of the untrusted relay first policy and the interleaving scheme can reduce the total number of trusted relays by at least half compared to the commonly adopted single-protocol trusted relay chaining approaches. The average security level enhancements of the TIN-MPRC and OIN-MPRC algorithms relative to their benchmarks can reach approximately 86%–108% and 88%–108% on the USNET topology, respectively. Such an average security level enhancement may be different for diverse network topologies, but the proposed heuristic algorithms are applicable to MPRC on various backbone network topologies with upgrading or construction purposes.

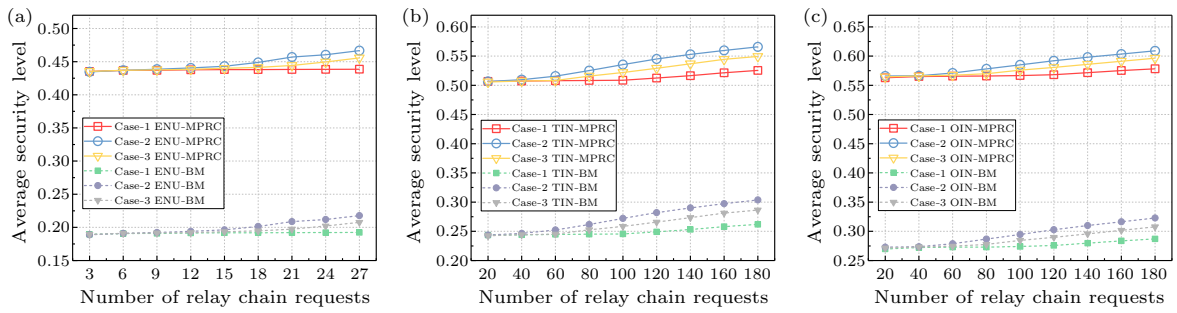


Fig. 8. Average security level versus number of relay chain requests: (a) ENU-MPRC on the BSQNET topology; (b) TIN-MPRC on the USNET topology; (c) OIN-MPRC on the USNET topology.

Table 1. Average security level enhancements of MPRC heuristics versus their benchmarks in different cases.

BSQNET topology				USNET topology						
	ENU-MPRC vs. ENU-BM (%)				TIN-MPRC vs. TIN-BM (%)			OIN-MPRC vs. OIN-BM (%)		
$\|R\|$	Case-1	Case-2	Case-3	$\|R\|$	Case-1	Case-2	Case-3	Case-1	Case-2	Case-3
3	129.8	130.1	129.8	20	108.1	108.0	108.6	108.7	107.5	107.9
6	129.0	128.8	128.8	40	107.9	106.8	107.8	107.6	107.0	107.2
9	128.9	128.0	128.5	60	107.5	104.3	107.3	107.3	104.8	106.7
12	128.4	127.1	128.1	80	107.4	100.7	104.3	107.3	101.6	105.3
15	128.3	125.7	127.3	100	107.2	96.8	101.9	106.9	98.6	102.5
18	128.3	122.8	126.6	120	105.7	93.3	99.2	106.0	95.5	100.4
21	128.2	118.9	125.1	140	104.0	90.6	96.3	104.4	93.0	98.2
24	128.1	117.3	122.5	160	102.1	88.2	93.6	102.9	90.8	96.0
27	128.0	114.3	119.5	180	100.6	86.3	91.9	101.5	88.7	93.8

6.2. Fixed and flexible distances between adjacent relays

The fixed and flexible distances between two adjacent relays are considered in the performance comparison for different algorithms. In order to achieve a secret key rate of kbps level, a fixed distance of 80 km or a flexible distance of 80–100 km is utilized. In the former case, each relay is placed at the same physical location as an erbium-doped fiber amplifier (EDFA) in the optical fiber backbone network to facilitate EDFA bypass;[27,28,51] while in the latter one, the distance parameter is derived from a typical span of the optical fiber backbone network.[52] Given the fact that the relay locations are fixed on the BSQNET topology, here we only conduct performance evaluation on the USNET topology. Also, we assume that the wavelength channels reserved for QKD on each physical link have no limit, such that all relay chain requests can be successfully deployed over the existing optical fiber backbone network.

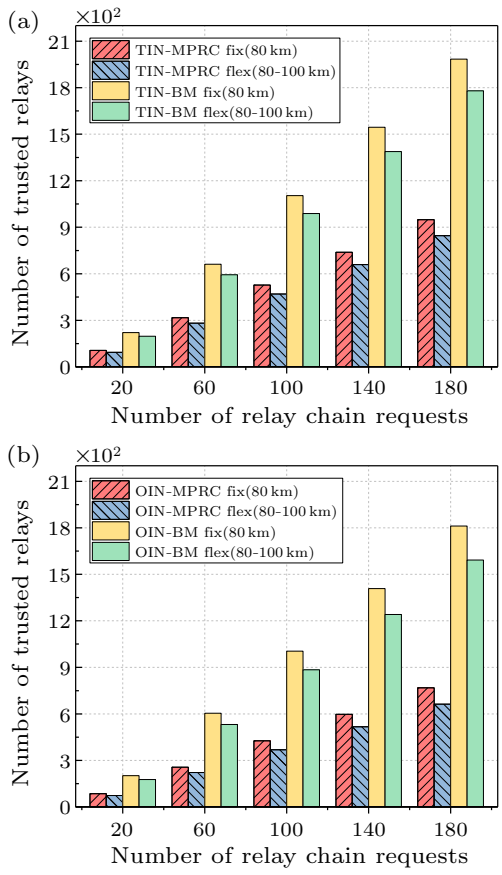


Fig. 9. Number of trusted relays versus number of relay chain requests under fixed/flexible distances between two adjacent relays on the USNET topology: (a) TIN-MPRC; (b) OIN-MPRC.

The number of trusted relays versus the number of relay chain requests on the USNET topology is illustrated in Fig. 9, where the TIN-MPRC/BM and OIN-MPRC/BM algorithms are employed. Similar to Fig. 7, we can observe that the number of trusted relays increases with the growing number of relay chain requests, and it shows larger values for the TIN-based algorithm compared to the OIN-based algorithm. These phenomena have already been discussed in the previous subsection. However, the number of trusted relays displays an approximately linear increasing tendency with the number of relay chain requests in Fig. 9. This is because all the randomly generated relay chain requests are successfully accommodated on the USNET topology. From Fig. 9 we can also see that each algorithm under 80–100 km yields fewer trusted relays than that under 80 km, which results from the decrease in the average number of relays deployed per relay chain. In reality, the secret key rate of a relay chain in the case of 80–100 km may be reduced compared to that under 80 km, but the specific secret key rate is not our focus in this work. Furthermore, the number of trusted relays for the MPRC-oriented algorithm is considerably fewer than its benchmark under both fixed and flexible distances, demonstrating the applicability of the designed MPRC heuristic algorithms in the context of diverse parameters for the distance between two adjacent relays.

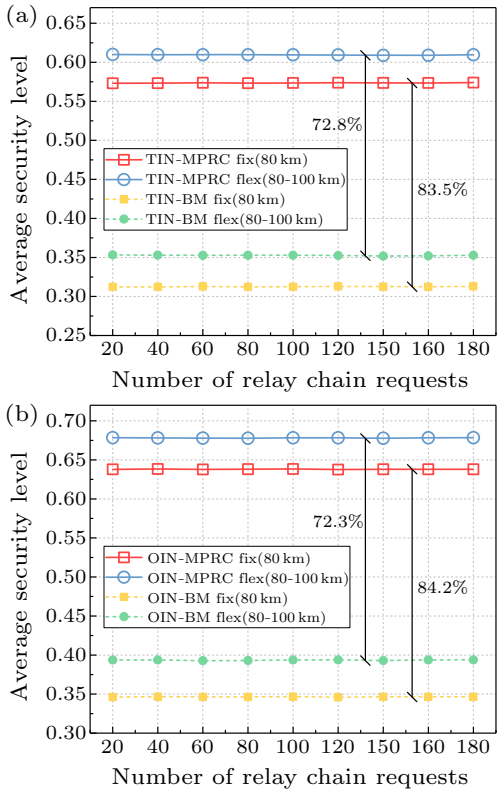


Fig. 10. Average security level versus number of relay chain requests under fixed/flexible distances between two adjacent relays on the USNET topology: (a) TIN-MPRC; (b) OIN-MPRC.

Figure 10 demonstrates the average security level versus the number of relay chain requests for the two MPRC heuristics and their benchmarks on the USNET topology. The average security level for each algorithm remains essentially stable with the variation of the number of relay chain requests under both fixed and flexible distances between two adjacent relays. This can be explicable according to the linear increasing tendency discussed in Fig. 9. More concretely, the average security level enhancements of the TIN-MPRC and

OIN-MPRC algorithms relative to their benchmarks are up to 83.5% and 84.2% under the fixed distance of 80 km, respectively; while they are up to 72.8% and 72.3% under the flexible distance of 80–100 km, respectively. Hence, the average security level enhancement of the MPRC-oriented algorithm versus its benchmark is closely associated with the distance between two adjacent relays, while it is weakly related to the manner of passing the intermediate QKD nodes. Notably, both TIN-MPRC and OIN-MPRC algorithms relying on hybrid SP2P and MDI/EB QKD significantly outperform the commonly used single-protocol trusted relay chaining methods based on SP2P-QKD, while the OIN-MPRC algorithm achieves a similar average security level improvement as the TIN-MPRC algorithm.

7. Conclusion

In this paper, we delved into the multi-protocol relay chain deployment for QKD backbone networking. Based on the independent/hybrid SP2P-QKD, MDI-QKD, and EB-QKD, we described the structures of diverse multi-protocol relay chains. Next, we formulated the network model according to the upgrading and construction purposes over the existing QKD backbone network and the existing optical fiber backbone network, respectively. We also provided the definitions as well as elaborated the objective and policies. Further, we proposed three MPRC heuristic algorithms for minimizing the number of trusted relays deployed to achieve the maximum end-to-end security level. Simulation results demonstrated the applicability of the three MPRC heuristics in the context of diverse network environments and fixed/flexible distances between two adjacent relays. Thanks to the intermediate QKD nodes equipped with trusted relays, the OIN-MPRC algorithm achieved a higher average security level than the TIN-MPRC algorithm. In particular, the ENU-MPRC algorithm can achieve up to 130% average security level enhancement versus existing SP2P-QKD-based trusted relay chains on the BSQNET topology. In the case of 80 km between two adjacent relays on the USNET topology, the average security level can be enhanced by up to 84.2% with the OIN-MPRC algorithm relative to the commonly used single-protocol trusted relay chaining methods. Hence, MPRC holds the promise of facilitating the practical evolution of large-scale QKD networks on the road to the Qinternet. In future work, we will further balance the trade-off between deployment cost and security level for MPRC as well as explore the new benefits of MPRC.

Acknowledgements

This work was supported in part by the National Natural Science Foundation of China (Grant Nos. 62201276, 62350001, U22B2026, and 62471248), Innovation Program for Quantum Science and Technology (Grant No. 2021ZD0300701), the Key R&D Program (Industry Foresight and Key Core Technologies) of Jiangsu Province (Grant No. BE2022071), and Natural Science Research of Jiangsu Higher Education Institutions of China (Grant No. 22KJB510007).

References

[1] Arute F, Arya K, Babbush R, *et al.* 2019 *Nature* **574** 505
[2] Zhong H S, Wang H, Deng Y H, *et al.* 2020 *Science* **370** 1460
[3] Diamanti E, Lo H K, Qi B and Yuan Z 2016 *npj Quantum Inf.* **2** 16025
[4] Xu F, Ma X, Zhang Q, Lo H K and Pan J W 2020 *Rev. Mod. Phys.* **92** 025002
[5] Diffie W and Hellman M 1976 *IEEE Trans. Inf. Theory* **22** 644
[6] Cao Y, Zhao Y, Wang Q, Zhang J, Ng S X and Hanzo L 2022 *IEEE Commun. Surv. Tutorials* **24** 839
[7] Tang Y L, Yin H L, Zhao Q, Liu H, Sun X X, Huang M Q, Zhang W J, Chen S J, Zhang L, You L X, Wang Z, Liu Y, Lu C Y, Jiang X, Ma X, Zhang Q, Chen T Y and Pan J W 2016 *Phys. Rev. X* **6** 011024
[8] Huang D, Huang P, Li H, Wang T, Zhou Y and Zeng G 2016 *Opt. Lett.* **41** 3511
[9] Aguado A, López V, López D, Peev M, Poppe A, Pastor A, Folgueira J and Martín V 2019 *IEEE Commun. Mag.* **57** 20
[10] Tessinari R S, Bravalheri A, Hugues-Salas E, Collins R, Aktas D, Guimaraes R S, Alia O, Rarity J, Kanellos G T, Nejabati R and Simeonidou D 2019 *45th European Conference on Optical Communication* (ECOC 2019)
[11] Dynes J F, Wonfor A, Tam W W S, Sharpe A W, Takahashi R, Lucamarini M, Plews A, Yuan Z L, Dixon A R, Cho J, Tanizawa Y, Elbers J P, Greiæer H, White I H, Penty R V and Shields A J 2019 *npj Quantum Inf.* **5** 101
[12] Joshi S K, Aktas D, Wengerowsky S, Lončarić M, Neumann S P, Liu B, Scheidl T, Lorenzo G C, Samec Ž, Kling L, Qiu A, Razavi M, Stipčević M, Rarity J G and Ursin R 2020 *Sci. Adv.* **6** eaba0959
[13] Chen T Y, Jiang X, Tang S B, *et al.* 2021 *npj Quantum Inf.* **7** 134
[14] Wang S, Chen W, Yin Z Q, *et al.* 2014 *Opt. Express* **22** 21739
[15] Wonfor A, White C, Bahrami A, Pearse J, Duan G, Straw A, Edwards T, Spiller T, Penty R and Lord A 2019 *45th European Conference on Optical Communication* (ECOC 2019)
[16] Zhang Q, Xu F, Li L, Liu N L and Pan J W 2019 *Quantum Sci. Technol.* **4** 040503
[17] Chen Y A, Zhang Q, Chen T Y, *et al.* 2021 *Nature* **589** 214
[18] Li Z D, Zhang R, Yin X F, Liu L Z, Hu Y, Fang Y Q, Fei Y Y, Jiang X, Zhang J, Li L, Liu N L, Xu F, Chen Y A and Pan J W 2019 *Nat. Photon.* **13** 644
[19] Liu X, Hu J, Li Z F, Li X, Li P Y, Liang P J, Zhou Z Q, Li C F and Guo G C 2021 *Nature* **594** 41
[20] Lo H K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[21] Lucamarini M, Yuan Z L, Dynes J F and Shields A J 2018 *Nature* **557** 400
[22] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[23] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557
[24] Wang S, Yin Z Q, He D Y, Chen W, Wang R Q, Ye P, Zhou Y, Fan-Yuan G J, Wang F X, Chen W, Zhu Y G, Morozov P V, Divochiy A V, Zhou Z, Guo G C and Han Z F 2022 *Nat. Photon.* **16** 154
[25] Liu Y, Zhang W J, Jiang C, Chen J P, Zhang C, Pan W X, Ma D, Dong H, Xiong J M, Zhang C J, Li H, Wang R C, Wu J, Chen T Y, You L, Wang X B, Zhang Q and Pan J W 2023 *Phys. Rev. Lett.* **130** 210801
[26] Wehner S, Elkouss D and Hanson R 2018 *Science* **362** eaam9288
[27] Cao Y, Zhao Y, Wang J, Yu X, Ma Z and Zhang J 2019 *J. Opt. Commun. Netw.* **11** 285
[28] Cao Y, Zhao Y, Li J, Lin R, Zhang J and Chen J 2021 *IEEE J. Sel. Areas Commun.* **39** 2701
[29] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. Comput. Syst. Signal Process.* p. 175
[30] Grosshans F and Grangier P 2002 *Phys. Rev. Lett.* **88** 057902
[31] Stucki D, Brunner N, Gisin N, Scarani V and Zbinden H 2005 *Appl. Phys. Lett.* **87** 194108
[32] Pan D, Long G L, Yin L, Sheng Y B, Ruan D, Ng S X, Lu J and Hanzo L 2024 *IEEE Commun. Surv. Tutorials* **26** 1898

[33] Pan D, Lin Z, Wu J, Zhang H, Sun Z, Ruan D, Yin L and Long G L 2020 *Photon. Research* **8** 1522
[34] Fan-Yuan G J, Lu F Y, Wang S, Yin Z Q, He D Y, Zhou Z, Teng J, Chen W, Guo G C and Han Z F 2021 *Photon. Res.* **9** 1881
[35] Guccione G, Darras T, Jeannic H L, Verma V B, Nam S W, Cavaillès A and Laurat J 2020 *Sci. Adv.* **6** eaba4508
[36] Chen J P, Zhang C, Liu Y, Jiang C, Zhang W J, Han Z Y, Ma S Z, Hu X L, Li Y H, Liu H, Zhou F, Jiang H F, Chen T Y, Li H, You L X, Wang Z, Wang X B, Zhang Q and Pan J W 2021 *Nat. Photon.* **8** 570
[37] Liao S K, Cai W Q, Handsteiner J, *et al.* 2018 *Phys. Rev. Lett.* **120** 030501
[38] Yin J, Li Y H, Liao S K, *et al.* 2020 *Nature* **582** 501
[39] Zhao Y, Cao Y, Wang W, Wang H, Yu X, Zhang J, Tornatore M, Wu Y and Mukherjee B 2018 *IEEE Commun. Mag.* **56** 130
[40] Cao Y, Zhao Y, Wang J, Yu X, Ma Z and Zhang J 2019 *IEEE Commun. Mag.* **57** 152
[41] Wang R, Tessinari R S, Hugues-Salas E, Bravalheri A, Uniyal N, Muqaddas A S, Guimaraes R S, Diallo T, Moazzeni S, Wang Q, Kanellos G T, Nejabati R and Simeonidou D 2020 *J. Lightwave Technol.* **38** 139
[42] Niu J, Sun Y, Jia X and Ji Y 2021 *J. Lightwave Technol.* **39** 2661
[43] Moghaddam E E, Beyranvand H and Salehi J A 2021 *IEEE J. Sel. Areas Commun.* **39** 2688
[44] 2019 *Overview on Networks Supporting Quantum Key Distribution* ITU-T Y.3800
[45] Wang W, Xu F and Lo H K 2019 *Phys. Rev. X* **9** 041012
[46] Zhou X Y, Zhang C H, Zhang C M and Wang Q 2019 *Phys. Rev. A* **99** 062316
[47] Wang X B 2013 *Phys. Rev. A* **87** 012320
[48] Wang Q and Wang X B 2013 *Phys. Rev. A* **88** 052332
[49] Shannon C E 1949 *Bell Labs Tech. J.* **28** 656
[50] 2020 *Quantum Key Distribution Networks - Key Management* ITU-T Y.3803
[51] Aleksic S, Hipp F, Winkler D, Poppe A, Schrenk B and Franzl G 2015 *Opt. Express* **23** 10359
[52] Mao Y, Wang B X, Zhao C, Wang G, Wang R, Wang H, Zhou F, Nie J, Chen Q, Zhao Y, Zhang Q, Zhang J, Chen T Y and Pan J W 2018 *Opt. Express* **26** 6010