



A cluster-based networking approach for large-scale and wide-area quantum key agreement

Zhonghui Li, Kaiping Xue, Qidong Jia, Jian Li, David S. L. Wei, Jianqing Liu, et al. *[full author details at the end of the article]*

Received: 26 June 2021 / Accepted: 26 April 2022 / Published online: 30 May 2022

© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022

Abstract

Quantum key distribution (QKD), a cryptographic technology developed to generate random secure keys, can realize unconditional secure remote classical communication in theory. However, QKD technology is currently confronted with two core problems: the extension of key distribution distance and the implementation of concurrent key agreements between multiple pairs of QKD nodes. To overcome these problems, in this paper, we present an innovative design—a cluster-based QKD network structure—which is composed of QKD nodes grouped into clusters interconnected by a backbone. A cluster serves as an access network in a master-slave structure to enable effective intra-cluster key agreements. To expand the key distribution over a longer distance and support concurrent key agreements, quantum repeaters are interconnected to form a mesh network as the QKD backbone. In our design, long-range QKD could be achieved by entanglement swapping performed in the backbone network, and the master-slave structure of the clusters is beneficial to the performance of the cluster-based QKD network. The simulation results show that the distance between two neighboring quantum repeaters, the size of quantum memory, quantum memory life-time, the success probability of entanglement distribution, and the success probability of entanglement swapping are essential factors affecting the key generation rate.

Keywords Quantum key distribution (QKD) · Cluster-based QKD network · Master–slave structure

1 Introduction

With the protection of cryptography, the security of classical communication is guaranteed based on computational complexity assumptions such as the difficulty of the decomposition of large prime numbers [28]. However, such assumptions are not able

✉ Kaiping Xue
kpxue@ustc.edu.cn

to hold for a quantum computer [17, 19]. As such, quantum key distribution (QKD)—a quantum-based key generation protocol—is adopted as new technology to realize secure classical communication [23]. Due to the properties of quantum mechanics [29, 38], QKD enables classical communication to be unconditionally secure in theory [21]. However, there have some doubts about if QKD is secure because of the imperfections of optical devices. As QKD gradually becomes mature and physical devices are improved, QKD technology will undoubtedly provide an unconditional security service for classical communication [32]. Currently, the study of QKD has been well beyond the experimental phase as some QKD systems, such as [14, 25, 31], have been in operation.

As the number of QKD nodes and communication distance between QKD nodes increase, a wide-area QKD network infrastructure needs to be developed [37]. What a QKD network needs to support are remote key agreements and efficient concurrent key agreements between multiple pairs of QKD nodes [4, 8]. However, the degradation of quantum states is generally ineluctable during the transmission in the realistic noisy quantum channel, e.g., optical fiber and free space. Most notably, quantum states cannot be cloned since the no-cloning theorem. Hence, photon loss and decoherence significantly hinder the implementation of remote QKD [27]. Moreover, how to efficiently realize concurrent key agreements between multiple pairs of QKD nodes is also a vital issue. Hence, these two critical issues need to be addressed to develop a large-scale and wide-area QKD network.

To overcome the limitation of remote key agreements, the quantum repeater is introduced [3]. There are two types of repeaters: trusted repeater and entanglement-based repeater [10, 13]. However, the implementation of a trusted repeater requires strong security assumptions that the repeater must be wholly trusted as it needs to perform classical encryption operations on keys, such as XOR operation [30, 35]. Fortunately, owing to the unique properties of entanglement [15], the entanglement-based repeater can facilitate the unconditional secure key agreement between remote QKD nodes. That is, two far-apart QKD nodes can establish remote entanglements to realize key agreements using local operation and classical communication (LOCC).

To realize concurrent key agreements between multiple pairs of QKD nodes, there is a need to connect the QKD nodes through quantum repeaters to form a network. However, the most concerning point in current research is how to improve the performance of the QKD system with only three QKD nodes, i.e., the basic unit of entanglement swapping (Fig. 1a). As two QKD nodes separate further, more entanglement-based repeaters need to be deployed between them to form a quantum repeater chain (Fig. 1b). Then remote key distribution can be realized by performing entanglement swapping on the repeater chain. However, a single linear repeater chain can not be used to realize efficient concurrent key agreements between multiple pairs of QKD nodes. Fortunately, thanks to the development of the storage-and-retrieval technology of quantum states, quantum memory will be instrumental in the implementation of secure long-distance communications [1, 34]. With the help of quantum memory, Einstein-Podolsky-Rosen (EPR) pairs, also known as entangled pairs, can be stored in QKD nodes and be used for concurrent key agreements. Connecting numerous entanglement-based repeaters to form a network for concurrent key agreements thus becomes feasible in the near future (Fig. 1c).

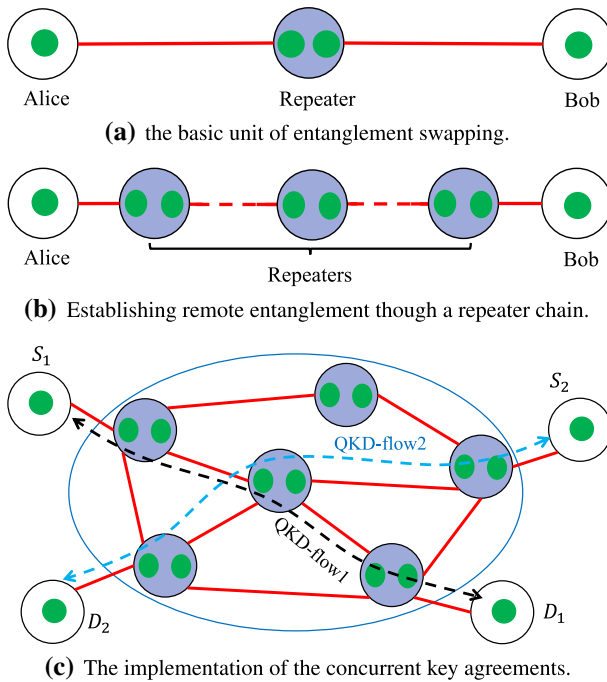


Fig. 1 The development stage of the key agreement. (a) Alice and Bob establish entanglement by measuring EPR pairs (green) at an intermediate repeater. (b) Bell state measurements are performed by intermediate repeaters to establish long-distance entanglement. (c) A number of repeaters are interconnected to form a mesh network, and the concurrent key agreements between multiple pairs of QKD nodes can be realized through different repeater chains

What lies forward is the challenge to connect numerous QKD nodes to realize efficient remote and concurrent key agreements. Although there have been some metropolitan-area testbed networks in Boston, Vienna, Geneva, Tokyo [14, 25, 31], and China [5], these testbed networks only consist of a couple of QKD nodes. It is expected that a wide-area QKD network with numerous QKD nodes could be implemented to serve as an ideal platform for secure classical communication. It is thus a meaningful work to design a QKD network structure in this regard. The main innovation of this paper is to present a cluster-based structure design of QKD networks with the help of entanglement-based repeaters and quantum memory. In our design, the QKD network comprises a backbone and some access networks. We adopt a master-slave structure in the access network: QKD nodes are divided into different entangled clusters consisting of a master node and some slave nodes. A master node is primarily responsible for distributing EPR pairs to any two slave nodes in the same cluster, and classic hosts are connected to slave nodes to obtain random keys. Meanwhile, entanglement-based repeaters with routing functions are connected to form a wide area network that serves as the QKD network's backbone. With the help of repeaters and quantum memory, the key agreement between two QKD nodes can be extended to any distance. Moreover, we perform simulations to explore what factors would affect

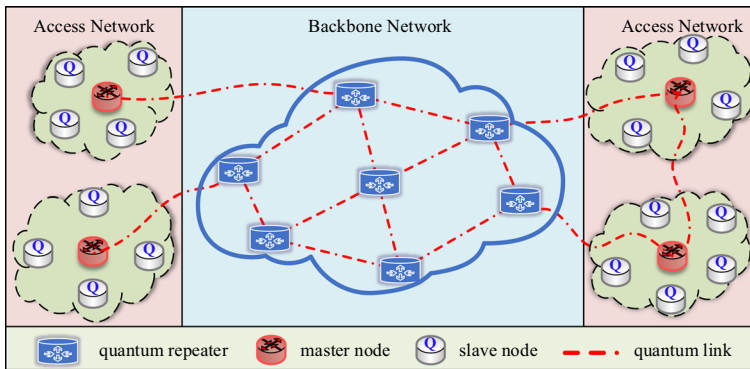


Fig. 2 The cluster-based QKD network structure. One master node and some slave nodes form a cluster, i.e., access network. Entanglement-based repeaters are interconnected to form the backbone network. Any two remote slave nodes belonging to different clusters can establish entanglements through the backbone network by performing entanglement swapping

the performance of the QKD network. The simulation results show that the rate of entanglement distribution and the size of quantum memory significantly impact the performance of the QKD network. Besides, the success rate of entanglement swapping also affects the performance of key agreements.

The rest of the work is organized as follows: Sect. 2 presents the design of the cluster-based QKD network. Section 3 describes how intra-cluster and inter-cluster QKD nodes perform key agreements. Section 4 gives a comprehensive performance evaluation. Finally, a summary is concluded in Sect. 5.

2 The cluster-based QKD network design

We propose a cluster-based QKD network structure, which consists of numerous master-slave access networks and a mesh-like backbone network composed of entanglement-based repeaters (Fig. 2). In this design, secure keys are generated by performing QKD protocols in the same or between different access networks. The main task of the backbone network is to expand the distance of key agreements by performing entanglement swapping on the selected repeater chains. In general, quantum bits (qubits) and entangled states can be directly measured or stored in a quantum memory. Here, quantum memory stores two kinds of photons with different functions to implement different key generation functions. In an access network, qubits or entangled states are stored in quantum memory for generating random secret keys. In the backbone network, quantum memory stores EPR pairs used to establish remote entanglements.

2.1 The access network

Generally, each EPR pair generated from the same entanglement source is sent to two neighboring nodes, and all neighboring nodes can be treated as an entangled cluster.

In our design, some slave nodes and a master node are generally grouped into an entangled cluster. Each master node is configured with an EPR source and is mainly responsible for distributing EPR pairs. Consequently, any two slave nodes in the same cluster can be entangled by sharing EPR pairs. Furthermore, each slave node and the master node can generate, store, and measure qubits.

Two different types of QKD protocols, known as single-photon and entanglement-based, can be performed between two slave nodes in the same cluster. Here, we take the measurement-device-independent QKD (known as MDI-QKD) [22] and Ekert91 [12] protocol as examples. Since the master node acts as the third party between a pair of slave nodes in the same cluster, MDI-QKD and Ekert91 protocol can be implemented simultaneously to improve the key generation rate between a pair of slave nodes. For the MDI-QKD protocol, any two slave nodes send qubits to the master node when a key agreement attempt is requested, and then the results of the joint measurement are feedback to the two slave nodes. For the Ekert91 protocol, the master node distributes EPR pairs to any two slave nodes. Then two slave nodes measure the shared EPR pairs to obtain secure keys. Consequently, the total key generation rate between two slave nodes in the same cluster is the sum of the key generation rate of these two QKD protocols. Besides, MDI-QKD does not need to make any security assumptions about the third party [39], i.e., MDI-QKD performs well in the security of the QKD system [20]. Moreover, the security of the Ekert91 protocol can be guaranteed by the entanglement characteristics. Hence, the master-slave design in access networks also benefits QKD networks' security.

2.2 The backbone network

The backbone network is responsible for expanding the distance of key agreements. In our design, entanglement-based repeaters are interconnected to form a backbone network. We can select a repeater chain to connect two slave nodes in different access networks to establish entanglement. The distance can be effectively extended by performing the swapping operation along the repeater chain. Establishing a long-distance entanglement between two slave nodes in different access networks is implemented with three steps as follows:

- (1) *Path selection* A routing algorithm is executed to select a path (or repeater chain) connecting two slave nodes.
- (2) *Entanglement distribution* Each entanglement-based repeater on the selected repeater chain attempts to share EPR pairs with its neighboring repeaters.
- (3) *Entanglement swapping* The LOCC operation is performed iteratively on the repeater chain to establish a remote slave-to-slave entanglement.

Step 1. Path selection aims to select a 'good' entanglement-based repeater chain to establish long-distance entanglement. Most notably, many quantum operations are imperfect, i.e., they are usually characterized by a success probability. Furthermore, entanglement swapping consumes EPR pairs, and the entangled states cannot be reused after measurement. Therefore, entanglement resource is essential to QKD networks' performance. To achieve efficient key agreements, designing an efficient routing algorithm is meaningful work to study. However, since the realization of QKD depends on

the properties of quantum mechanics, the routing algorithm design in the cluster-based QKD network is fundamentally different from that in a classical network. Hence, when developing a new routing algorithm for QKD networks, we need to consider the properties of quantum mechanics. Some routing algorithms have been proposed for the entanglement-based repeater backbone network [24, 33]. However, the properties of quantum mechanics were not fully considered. It is hard to define a ‘good’ path in the cluster-based QKD network, and we briefly discuss what factors influence the path selection in the following.

A quantum channel is inherently loss, i.e., the success probability of each attempt to create an entanglement decreases exponentially with the increase of the physical distance of a point-to-point quantum channel [9]. The entanglement distribution rate is significant to the key agreement’s performance. Hence, distance is an inviolable factor in routing algorithm design. Moreover, the success probability of entanglement swapping is also a vital factor since it affects the remote entanglement establishment rate. Besides, the size and lifetime of quantum memory also affect the routing performance. A larger quantum memory size means more entanglement resources can be used to establish entanglement between QKD nodes. The lifetime of memory indicates that the de-coherence does not affect the information represented by quantum states within the lifetime. Generally, imperfect quantum memory results in entanglement fidelity attenuation since the environment noise. Entanglement fidelity, defined as the degree of coincidence between the output state and the input state of quantum memory [18], is essential for the perfection of the entanglement-based quantum operations. Although purification operation can improve entanglement fidelity, the cost is a reduction of entanglement resources. Summarily, these factors should be considered when developing a routing algorithm. However, the trade-off between them needs to be well studied. In this work, we only study their influence on the performance of the key agreement, and we will look into how they affect the routing algorithm design in our future work.

Step 2. Entanglement distribution [11, 16] is the basis for the backbone network to realize the function of expanding secure communication to a greater distance. Generally, EPR pairs can be used directly or stored in quantum memory. Most notably, the success probability of each entanglement distribution attempt decreases exponentially with the physical length of a quantum channel, i.e., it is hard to establish entanglement between adjacent repeaters. In other words, successfully establishing entanglement between adjacent repeaters requires multiple entanglement distribution attempts. Hence, the successful entanglement distribution will result in non-negligible QKD latency, which significantly affects the key generation rate. To improve the performance of the cluster-based QKD network, each repeater configures a quantum memory to store entangled states that are used for entanglement swapping. In our design, any two neighboring repeaters are entangled in the backbone network. After path selection, each quantum repeater on the selected path assigns point-to-point entanglements for each key agreement request. Here, we adopt an event-based trigger model to replenish point-to-point entanglements after entanglement swapping. Specifically, free quantum memory units trigger entanglement distribution to fill quantum memory. With the help of quantum memory, entangled states can be measured directly without requiring an entanglement distribution first when entanglement swapping is required.

Step 3. Entanglement swapping is a magic operation that enables two distant non-entangled QKD nodes to share EPR pairs. For example, there are two EPR pairs:

$$|\psi\rangle_{ab} = \frac{1}{\sqrt{2}}(|0\rangle_a|1\rangle_b + |1\rangle_a|0\rangle_b), \tag{1}$$

$$|\psi\rangle_{cd} = \frac{1}{\sqrt{2}}(|0\rangle_c|1\rangle_d + |1\rangle_c|0\rangle_d). \tag{2}$$

They constitute a composite system: $|\psi\rangle = |\psi\rangle_{ab} \otimes |\psi\rangle_{cd}$. In the composite system, a joint measurement is performed on entangled photons b and c , and eventually photons a and d form an entangled system:

$$|\psi\rangle_{ad} = \frac{1}{\sqrt{2}}(|1\rangle_a|0\rangle_d + |0\rangle_a|1\rangle_d). \tag{3}$$

Assume that the distance between two EPR pairs is $dist_{(a,b)}$ and $dist_{(c,d)}$, respectively. After the swap operation, the distance of the entanglement between photons a and d is $dist_{(a,d)} = dist_{(a,b)} + dist_{(c,d)}$. Hence, entanglement swapping can be adopted for establishing entanglement between any two distant slave nodes.

Theorem 1 *Long-range QKD can be achieved by the entanglement swapping performed in backbone network.*

Proof We assume a path from the source slave node to the destination slave node is selected after path selection, and the repeaters along this path form a repeater chain. Specially, the nodes on the path are labeled as $0, 1, 2, \dots, S$ and the edge set is $\{(0, 1), (1, 2), \dots, (S - 1, S)\}$. The distance of each edge $(i, i + 1)$ is $dist_{(i,i+1)}$. After entanglement distribution between neighboring nodes, EPR pairs are shared by each pair of adjacent nodes. Then entanglement swapping can be iteratively performed on the repeater chain. In this way, short-distance entanglement can be extended hop-by-hop. Finally, two distant slave nodes in different clusters are entangled, i.e., the distance of the remote slave-to-slave entanglement is the sum of all edges' distance:

$$dist_{total} = \sum_{i=0}^{S-1} dist_{(i,i+1)}. \tag{4}$$

Note that two communication parties sharing EPR pairs can generate random secure keys based on the Ekert91 protocol. Hence, any pair of distant slave nodes can share EPR pairs by performing entanglement swapping in the backbone network, thus achieving long-range QKD. □

3 The implementation of key agreement

Some preliminaries need to be expounded before describing the implementation of the key agreement in the cluster-based QKD network. First, qubits are unknown to

QKD nodes before being measured. Hence, an identification label is required for each EPR pair to be distinguished from others stored in the quantum memory. When entanglement swapping or teleportation is required, we need to use the label to select entangled states stored in the quantum memory to measure. Besides, the identification label of the two photons needs to be updated when two non-entangled photons establish an entanglement after entanglement swapping. Generally, the key generation rate is lower than the consumption rate, especially during the encryption of multimedia files. To improve the performance of classical secure communication, we introduce a key pool to store keys in each slave node. Finally, both QKD nodes and entanglement-based quantum repeaters can manipulate quantum states.

The implementation of QKD-based secure communication consists of key management and key agreement. Key management is responsible for key storage and derivation. Before secure communications, two slave nodes perform QKD protocol to generate random keys, and the keys are stored in a key pool. When the classical host requests secret keys from the slave node which it is connected, the requested keys are retrieved from the key pool and provided to the classical host in a secure way. Notably, semi-quantum key distribution (SQKD) technology [2, 41] can also be adopted as one of the candidates to realize this function since SQKD only requires one of the communicating parties to possess quantum resources. Considering that the secret keys are generated by performing SQKD protocol after the key request occurs rather than retrieving directly from the key pool, SQKD is only suitable for applications that are not latency-sensitive and have low key requirements. To discuss general application scenarios for secret keys, we only use the design of key management to realize key distribution in this paper. To meet the requirement of key consumption, a method of key derivation needs to be adopted to derive more keys from fewer keys. No matter what derivation method we adopt, we must ensure that the keys generated by performing QKD protocols are not reused. Key management is achieved by classical methods [36, 40], and we pay more attention to the process of the key agreement between any two slave nodes in the cluster-based QKD network. In our design, the key agreement can be classified into two scenarios, i.e., the key agreement between two slave nodes in the same cluster and in different clusters. We conclude the process of key agreement between a pair of slave nodes (referred to as Alice and Bob) in the cluster-based QKD network as follows:

- (1) Alice initiates a request to perform QKD with Bob.
- (2) Bob receives the request and judges the geographic relationship with Alice. If Alice and Bob belong to the same access network, step (3) is performed; otherwise, step (4) is executed.
- (3) Alice and Bob perform QKD protocol directly to obtain secure keys.
- (4) Alice and Bob first attempt to establish an entanglement through the backbone network, and then QKD protocol is performed to generate secure keys.

For key agreement between any two slave nodes in the same cluster, Ekert91 and MDI-QKD protocol can be implemented simultaneously. Two slave nodes can send qubits to the master node, and the master node measures the qubits according to the MDI-QKD protocol. Accordingly, the measurement results are published to slave nodes. Two slave nodes perform related operations based on the results to obtain secret

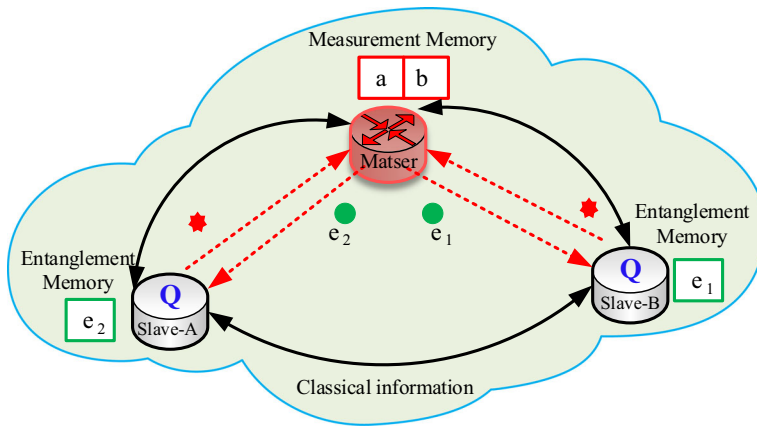


Fig. 3 Key agreement between two slave nodes in the same cluster. Slave-A and Slave-B send qubits a and b (red star) to the master node, respectively, and the qubits are stored in measurement memory. The master node follows MDI-QKD protocol to measure the qubits and publishes measurement results to these two slave nodes through classical channels. The master node can distribute an EPR pair (e_1, e_2) (green dot) to Slave-A and Slave-B, and e_1 and e_2 are stored in measurement memory, respectively. Then, Slave-A and Slave-B generate shared secret keys by means of LOCC under the rules of the Ekert91 protocol

keys. For Ekert91 protocol, the master node distributes EPR pairs to any two slave nodes, and Bell measurement is performed in these two slave nodes. Accordingly, two slave nodes publish their measurement basis on the classical authentication channel, keeping the parts measured by the same base as secret keys. As the measurement operations are performed in the master node and slave nodes, respectively, we can perform MDI-QKD and Ekert91 in each cluster simultaneously (Fig. 3).

Theorem 2 *The master-slave structure of the access network facilitates the security and efficiency of QKD between slave nodes in the same cluster.*

Proof The number of slave nodes in a cluster is denoted as $|V|$. Assume that the memory size of each slave node and the master node is N_s and N_m , respectively. And quantum memory will be filled during each key agreement attempt. Besides, the key generation ratio of MDI-QKD and Ekert91 protocol is R_{mdi} and R_{ekr} , respectively. Most notably, joint measurement is performed on the master node for the MDI-QKD protocol. Hence, there is only a pair of slave nodes can perform MDI-QKD protocol to generate secure keys at each key agreement. However, the measurement operation of the Ekert91 protocol is performed in each slave node. So, there are multiple pairs of slave nodes that can perform the Ekert91 protocol simultaneously to generate secure keys at each key agreement attempt. We can get the number of pairs of slave nodes executing Ekert91 protocol in each key agreement attempt is

$$M = \begin{cases} V/2 & \text{if } |V| \text{ is even,} \\ (V - 1)/2 & \text{if } |V| \text{ is odd.} \end{cases} \quad (5)$$

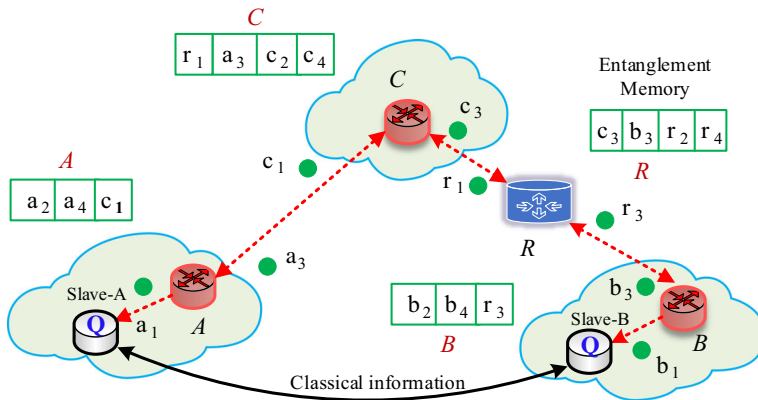


Fig. 4 Key agreement between two slave nodes in different clusters. Initially, the master node and quantum repeaters distribute EPR pairs to neighboring nodes, and entangled states are stored in quantum memory. When an entanglement path is determined according to a routing algorithm, long-distance entanglement can be established by performing entanglement swappings along the selected path. Finally, Slave-A and Slave-B perform the Ekert91 protocol to generate secret keys

After each key agreement attempt, we can get the total amount of secure keys that are shared between slave nodes in a cluster is

$$\begin{aligned}
 Key_{total} &= R_{mdi} \cdot N_m + R_{ekr} \cdot N_s \cdot M \\
 &= \begin{cases} R_{mdi} \cdot N_m + R_{ekr} \cdot N_s \cdot |V|/2 & \text{if } V \text{ is even,} \\ R_{mdi} \cdot N_m + R_{ekr} \cdot N_s \cdot (|V| - 1)/2 & \text{if } V \text{ is odd.} \end{cases} \quad (6)
 \end{aligned}$$

Generally, the number of slave nodes in a cluster is greater than or equal to two. i.e., M is greater than zero in Eq. 5. Hence, the mixed implementation of MDI-QKD and the Ekert91 facilitates the performance of the key agreement in access networks as shown in Eq. 6. Besides, neither MDI-QKD nor Ekert91 requires the security assumption about a third party. Hence, the master-slave structure is beneficial to the performance of QKD between slave nodes in the same cluster in terms of efficiency and security. \square

For key agreement between any two slave nodes in different clusters, the Ekert91 protocol is performed to generate random secret keys. Before the key agreement, entanglement between two slave nodes in different clusters should be established. Different clusters are connected by the backbone network made up of quantum repeaters. Therefore, routing and entanglement swapping is indispensable in establishing long-distance slave-to-slave entanglement. Initially, entanglement distribution is executed multiple times between two neighboring repeaters, and entangled states are stored in quantum memory. First, a path from the source slave node to the destination is determined according to the routing algorithm, quantum repeaters on the path form a chain. Then, entanglement swappings are iteratively performed along the quantum repeater chain until the two slave nodes establish an entanglement. Finally, the Ekert91 QKD pro-

ocol is performed to obtain random secret keys. The detailed process is shown in Fig. 4.

Theorem 3 *The distance between two neighboring nodes, the edge capacity, the number of hops in a repeater chain, the success rate of entanglement distribution between two neighboring quantum repeaters, and the success probability of entanglement swapping affect the slave-to-slave entanglement distribution rate, thus affecting the key generation rate between a pair of distant slave nodes in the different access networks.*

Proof For any two neighboring nodes u and v that are $dist_{(u,v)}$ kilometers apart, the success probability of an entanglement distribution attempt in a solid-state platform is (as shown in [6]):

$$p \approx 10^{-\alpha \cdot dist_{(u,v)}/10}, \tag{7}$$

where α is the loss rate of signal [27] caused from quantum channel noise and $\alpha \approx 0.4\text{dB/km}$ in an Nitrogen-Vacancy platform [6]. Generally, the duration of an entanglement distribution attempt between nodes u and v is $dist_{(u,v)}/s$, where s is the speed at which a photon is transmitted in a quantum channel. Hence, according to Eq. 7, the time spent for successfully establishing an entanglement between u and v is denoted as

$$t_{(u,v)} = \frac{dist_{(u,v)} \cdot 10^{\alpha \cdot dist_{(u,v)}/10}}{s}. \tag{8}$$

Assume that the quantum memory size of each entanglement-based repeater is limited, and m quantum memory units are configured on each edge, i.e., a pair of adjacent repeaters can establish m entanglements. Besides, the success probability of entanglement swapping is denoted by q . For a homogeneous repeater chain with k hops, the long-distance entanglement distribution ratio between two distant slave nodes is (as shown in [7]):

$$\lambda = \begin{cases} \frac{m \cdot k \cdot p \cdot q^{n+1}}{2 \cdot (k-2^n) + q \cdot (2^{n+1} - k)} & \text{if } k \text{ is even,} \\ \frac{m \cdot (k-1) \cdot p \cdot q^{n+1}}{2 \cdot (k-2^n) + q \cdot (2^{n+1} - k - 1)} & \text{if } k \text{ is odd,} \end{cases} \tag{9}$$

where $n = \lceil \log_2(k) \rceil - 1$. Assume that entanglement distribution and entanglement swapping are performed hop-by-hop on the selected repeater chain. Besides, the delay time of joint measurement and label-based photon retrieval cannot be ignored, and they are denoted as t_{mea} and t_{ret} , respectively. According to Eqs. 8 and 9, we can get the latency of establishing a slave-to-slave entanglement on a repeater chain with k hops is:

$$\begin{aligned}
 T_{total} &= \frac{\sum_{i=0}^k t_{(i,i+1)}}{\lambda} + k \cdot (t_{mea} + t_{ret}) \\
 &= \begin{cases} \sum_{i=0}^k \frac{dist_{(i,i+1)} \cdot 10^{\alpha \cdot dist_{(i,i+1)}/10}}{s} \cdot \frac{2 \cdot (k-2^n) + q \cdot (2^{n+1} - k)}{m \cdot k \cdot p \cdot q^{n+1}} + k \cdot (t_{mea} + t_{ret}) & \text{if } k \text{ is even,} \\ \sum_{i=0}^k \frac{dist_{(i,i+1)} \cdot 10^{\alpha \cdot dist_{(i,i+1)}/10}}{s} \cdot \frac{2 \cdot (k-2^n) + q \cdot (2^{n+1} - k - 1)}{m \cdot (k-1) \cdot p \cdot q^{n+1}} + k \cdot (t_{mea} + t_{ret}) & \text{if } k \text{ is odd,} \end{cases}
 \end{aligned}
 \tag{10}$$

where $t_{(i,i+1)}$ is the duration of the successful entanglement distribution between adjacent nodes i and j . As shown in Eq. 10, the distance between two neighboring nodes, the number of hops in a repeater chain, the success rate of entanglement distribution between two neighboring quantum repeaters, and the success probability of entanglement swapping are essential to the slave-to-slave entanglement distribution rate in the cluster-based QKD network. Due to the key agreement between two slave nodes in the different clusters being achieved by employing EPR pairs, so the different factors mentioned above significantly affect the key agreement between a pair of slave nodes by influencing the slave-to-slave entanglement distribution rate. □

4 Performance evaluation

To better evaluate the impact of different factors on the performance of the proposed QKD network structure, we perform some related simulations. In our simulation, we assume that the capability and robustness of classical information transmission are significantly better than that of quantum information transmission, and the delay brought by classical communication is negligible in key agreement. Besides, a path can be found in classical networks to realize classical communications between any two QKD nodes. In general, the bottleneck of the key generation rate mainly lies in the entanglement distribution rate and the size of quantum memory. Here, we explore the performance of the key agreement in the cluster-based QKD network under different scenarios. We assume that the success probability of entanglement swapping of each quantum repeater is the same. Furthermore, Bell state measurement takes about $100\mu s$ in a Nitrogen-Vacancy platform, and the time for retrieving a qubit is about $1040\mu s$. The time for an attempt to generate an EPR pair using a point-to-point channel is about $145\mu s$ [26].

For two slave nodes in two different access networks far apart, we can deploy some quantum repeaters between them to maintain a high key rate. Here, we assume that an EPR pair can be used to generate one secret key, so the slave-to-slave entanglement distribution rate can be regarded as an evaluate indicator of the key rate. When the distance between two neighboring repeaters is constant, the total distance of secure communication increases with the number of quantum repeaters N . Besides, the key generation rate can be improved by reducing the distance between two neighboring repeaters as N increases (Fig. 5). There is no doubt that the cluster-based QKD networks can expand

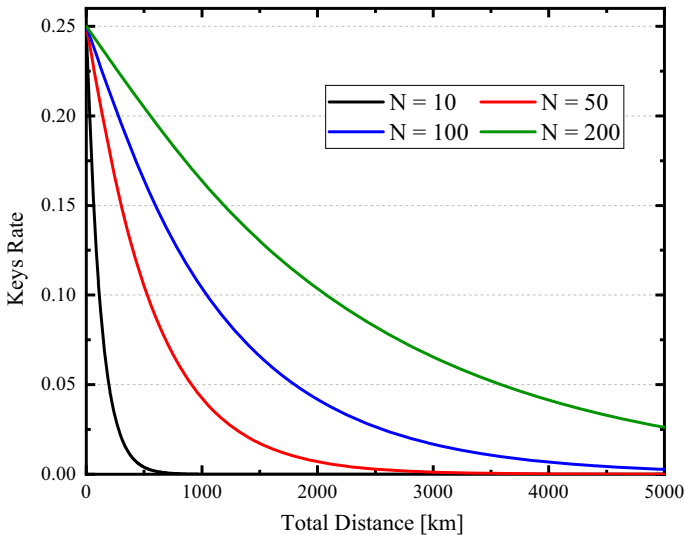


Fig. 5 Quantum repeater is conducive to the expansion of secure communication. We set $\alpha = 0.4\text{dB/km}$, $q = 1.0$, and the distance between two neighboring quantum repeaters is set from 0 to 20 km. When N is small, the key rate drops rapidly as the distance increases (black and red line). On the contrary, when N is a large value, the key rate decreases more slowly (blue and green line), and the total distance of secure communication reaches a good value

the range of secure communication with the help of entanglement-based quantum repeaters.

There are two performance metrics for quantum memory: lifetime and size. These two metrics influence the efficiency of key agreements, and the success rate of entanglement swapping also affects QKD network performance. When the distance *Distance* between two adjacent repeaters is fixed, the time to generate a specific account of keys decreases gradually with the increased memory size. Besides, the decline rate of time spent increases with the distance. The efficiency of key agreement can be improved by increasing memory size when *Distance* is a large value (Fig. 6a). As shown in Fig. 6b, for two slave nodes in the same cluster, the lifetime of qubits in a quantum memory affects the key generation rate. In a time slot, if the total time taken to finish the measurement of all qubits stored in a quantum memory is less than the lifetime of qubits, the number of keys generated in a time slot has a linear relationship with lifetime (red and black line). Besides, a higher rate of entanglement distribution means that more qubits can be stored in quantum memory, though some qubits may not be measured during the lifetime. In general, when the two slave nodes are in the same cluster, i.e., entanglement swapping is not needed, the quantum memory size and lifetime determine the number of qubits that can be measured, which affects the key generation rate. However, when the slave nodes to be entangled are in different clusters, q has a significant impact on the entanglement distribution rate (Fig. 6c).

When the total distance between two slave nodes to be entangled is fixed, λ is determined by the number of quantum channels $k \cdot m$ and q . Although p increases with the number of quantum repeaters, there is a trade-off between q and N on the key

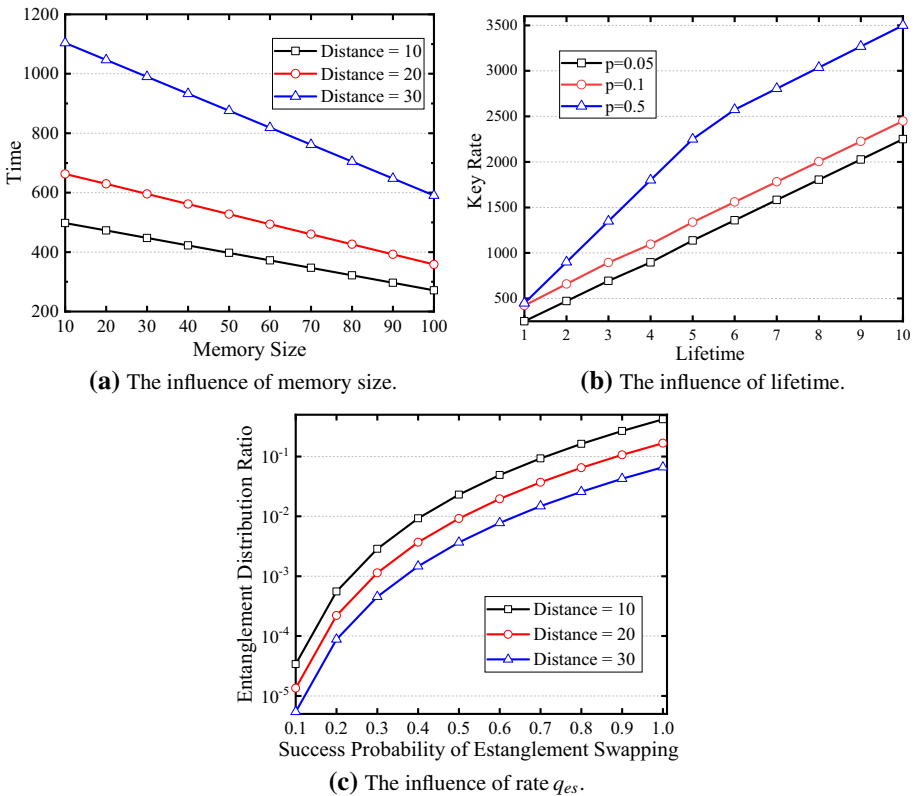


Fig. 6 The influence of different factors on cluster-based QKD networks. **(a)** The size of quantum memory determines the rate at which entanglement is established between two QKD nodes. **(b)** The number of keys generated in a time slot first increases with lifetime, and then the rate of increase will decrease after a certain point of lifetime. **(c)** We set $k = 21$ and $\alpha = 0.4$ dB/km. When the number of quantum repeaters and $l_{(i,i+1)}$ are fixed, the entanglement distribution rate between two distant slave nodes in different access network increases with the increase of q

generation rate. When the number of quantum repeaters is not a very large value, p increases with the number of repeaters, which is conducive to improving the key rate. However, q is the main factor affecting the key rate when the number of repeaters is larger than a value (Fig. 7a). In addition to expanding the distance of secure communication, our proposed cluster-based QKD network can also realize efficient concurrent key agreement for multiple pairs of slave nodes. When N and q are fixed, the influence of the point-to-point distance and memory size S on the concurrent key agreements is similar to that of a single key agreement. Concurrent key agreements require effective scheduling of resources and processes because the disadvantage of small memory size can be compensated by effective scheduling. Therefore, the distance between two neighboring QKD nodes has a great influence on the performance of multiple independent key agreements (Fig. 7b), and the cluster-based QKD network can improve the performance of concurrent key agreements.

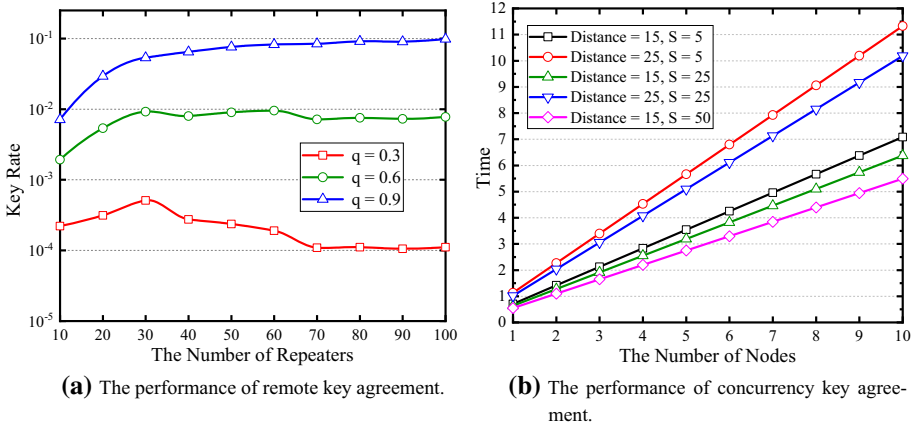


Fig. 7 The performance of cluster-based QKD networks in remote and concurrency key agreement. **(a)** The total distance between two slave node is 200 km. For $q = 0.9$, the key rate increases with the number of repeaters (blue line). For $q = 0.6$, when $N \leq 30$, the key rate increases. However, when $N > 30$, there is no significant change in the key rate due to the fact that the influence of the improvement of p offsets the increase in the number of entanglement swappings (green line). For $q = 0.3$, the variation trend is the same as that of $q = 0.6$ when $N \leq 30$. However, with the increase of the number of repeaters, the key rate tends to decrease when $N > 30$ since multiple entanglement swapping operations are performed. **(b)** $q = 0.6$ and N is 5. Multiple senders, composed of some slave nodes in the same cluster, perform concurrent key agreements with a receiver in another cluster. When the distance is fixed, it takes more time to complete key agreement as the number of slave nodes increases, but the difference in time is small (black, green and purple line). On the contrary, in the case of the same memory size, the time difference of key agreement at different distances is larger (red and black line)

5 Conclusion

In this paper, we presented a design of the cluster-based QKD network to realize efficient large-scale and wide-area key agreements. The cluster-based QKD network structure composes access networks and a backbone network. QKD nodes are grouped into different clusters, and each cluster is configured in such a way that a node serves as the master, and the remaining nodes serve as slave nodes. The secret keys can be obtained between two slave nodes in the same cluster by performing Ekert91 and MDI-QKD. The slave nodes in different clusters can establish remote entanglement by entanglement swapping in the backbone network, and Ekert91 QKD protocol is performed to generate random keys. The cluster-based QKD network can guarantee security and improve the efficiency of key agreements. Our simulation results show that the distance between two adjacent QKD nodes, quantum memory size, the lifetime of quantum memory, and the success probability of entanglement swapping all have a certain impact on the key generation rate. In the design of the cluster-based QKD network, we notice that some open problems, such as entanglement routing, need to be further studied.

Acknowledgements We acknowledge the financial support by Anhui Initiative in Quantum Information Technologies under grant No. AHY150300 and Youth Innovation Promotion Association Chinese Academy

of Sciences (CAS) under Grant No. Y202093. The datasets generated and analysed during the current study are available from the corresponding author on reasonable request.


References

1. Biham, E., Huttner, B., Mor, T.: Quantum cryptographic network based on quantum memories. *Phys. Rev. A* **54**(4), 2651 (1996)
2. Boyer, M., Kenigsberg, D., Mor, T.: Quantum key distribution with classical bob. *Phys. Rev. Lett.* **99**, 140501 (2007)
3. Briegel, H.J., Dür, W., Cirac, J.I., Zoller, P.: Quantum repeaters: the role of imperfect local operations in quantum communication. *Phys. Rev. Lett.* **81**(26), 5932 (1998)
4. Castelvecchi, D.: The quantum internet has arrived (and it hasn't). *Nature* **554**, 7692 (2018)
5. Chen, T.Y., Liang, H., Liu, Y., Cai, W.Q., Ju, L., Liu, W.Y., Wang, J., Yin, H., Chen, K., Chen, Z.B., et al.: Field test of a practical secure communication network with decoy-state quantum cryptography. *Opt. Express* **17**(8), 6540–6549 (2009)
6. Dahlberg, A., Skrzypczyk, M., Coopmans, T., Wubben, L., Rozpędek, F., Pompili, M., Stolk, A., Pawelczak, P., Knegjens, R., de Oliveira Filho, J., et al.: A link layer protocol for quantum networks. In: *Proceedings of the ACM Special Interest Group on Data Communication*, pp. 159–173 (2019)
7. Dai, W., Peng, T., Win, M.Z.: Optimal remote entanglement distribution. *IEEE J. Sel. Areas Commun.* **38**(3), 540–556 (2020)
8. Diamanti, E., Lo, H.K., Qi, B., Yuan, Z.: Practical challenges in quantum key distribution. *npj Quantum Inf* **2**(1), 1–12 (2016)
9. Duan, L.M., Lukin, M.D., Cirac, J.I., Zoller, P.: Long-distance quantum communication with atomic ensembles and linear optics. *Nature* **414**(6862), 413–418 (2001)
10. Dür, W., Briegel, H.J., Cirac, J.I., Zoller, P.: Quantum repeaters based on entanglement purification. *Phys. Rev. A* **59**(1), 169 (1999)
11. Dynes, J.F., Takesue, H., Yuan, Z.L., Sharpe, A.W., Harada, K., Honjo, T., Kamada, H., Tadanaga, O., Nishida, Y., Asobe, M., et al.: Efficient entanglement distribution over 200 kilometers. *Opt. Express* **17**(14), 11440–11449 (2009)
12. Ekert, A.K.: Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.* **67**(6), 661 (1991)
13. Elliott, C.: Building the quantum network. *New J. Phys.* **4**(1), 46 (2002)
14. Elliott, C., Colvin, A., Pearson, D., Pikalo, O., Schlafer, J., Yeh, H.: Current status of the darpa quantum network. In: *Quantum Information and Computation III*, vol. 5815, pp. 138–149. International Society for Optics and Photonics (2005)
15. Horodecki, R., Horodecki, P., Horodecki, M., Horodecki, K.: Quantum entanglement. *Rev. Mod. Phys.* **81**(2), 865 (2009)
16. Inagaki, T., Matsuda, N., Tadanaga, O., Asobe, M., Takesue, H.: Entanglement distribution over 300 km of fiber. *Opt. Express* **21**(20), 23241–23249 (2013)
17. Kaplan, M., Leurent, G., Leverrier, A., Naya-Plasencia, M.: Breaking symmetric cryptosystems using quantum period finding. In: *Annual international cryptology conference*, pp. 207–237. Springer (2016)
18. Kurz, C., Schug, M., Eich, P., Huwer, J., Müller, P., Eschner, J.: Experimental protocol for high-fidelity heralded photon-to-atom quantum state transfer. *Nat. Commun.* **5**(1), 1–5 (2014)
19. Ladd, T.D., Jelezko, F., Laflamme, R., Nakamura, Y., Monroe, C., O'Brien, J.L.: Quantum computers. *Nature* **464**(7285), 45–53 (2010)
20. Lin, J., Lütkenhaus, N.: Simple security analysis of phase-matching measurement-device-independent quantum key distribution. *Phys. Rev. A* **98**, 042332 (2018)
21. Lo, H.K., Chau, H.F.: Unconditional security of quantum key distribution over arbitrarily long distances. *Science* **283**(5410), 2050–2056 (1999)
22. Lo, H.K., Curty, M., Qi, B.: Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108**(13), 130503 (2012)
23. Lo, H.K., Curty, M., Tamaki, K.: Secure quantum key distribution. *Nat. Photonics* **8**(8), 595–604 (2014)
24. Pant, M., Krovvi, H., Towsley, D., Tassioulas, L., Jiang, L., Basu, P., Englund, D., Guha, S.: Routing entanglement in the quantum internet. *npj Quantum Inf.* **5**(1), 1–9 (2019)

25. Peev, M., Pacher, C., Alléaume, R., Barreiro, C., Bouda, J., Boxleitner, W., Debuisschert, T., Diamanti, E., Dianati, M., Dynes, J., et al.: The secoqc quantum key distribution network in Vienna. *New J. Phys.* **11**(7), 075001 (2009)
26. Pfaff, W., Hensen, B.J., Bernien, H., van Dam, S.B., Blok, M.S., Taminiau, T.H., Tiggelman, M.J., Schouten, R.N., Markham, M., Twitchen, D.J., et al.: Unconditional quantum teleportation between distant solid-state quantum bits. *Science* **345**(6196), 532–535 (2014)
27. Pirandola, S., Laurenza, R., Ottaviani, C., Banchi, L.: Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **8**(1), 1–15 (2017)
28. Rivest, R.L., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **21**(2), 120–126 (1978)
29. Robertson, H.P.: The uncertainty principle. *Phys. Rev.* **34**(1), 163 (1929)
30. Salvail, L., Peev, M., Diamanti, E., Alléaume, R., Lütkenhaus, N., Länger, T.: Security of trusted repeater quantum key distribution networks. *J. Comput. Secur.* **18**(1), 61–87 (2010)
31. Sasaki, M., Fujiwara, M., Ishizuka, H., Klaus, W., Wakui, K., Takeoka, M., Miki, S., Yamashita, T., Wang, Z., Tanaka, A., et al.: Field test of quantum key distribution in the tokyo qkd network. *Opt. Express* **19**(11), 10387–10409 (2011)
32. Scarani, V., Bechmann-Pasquinucci, H., Cerf, N.J., Dušek, M., Lütkenhaus, N., Peev, M.: The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**(3), 1301 (2009)
33. Shi, S., Qian, C.: Concurrent entanglement routing for quantum networks: Model and designs. In: Proceedings of the Annual conference of the ACM Special Interest Group on Data Communication on the applications, technologies, architectures, and protocols for computer communication, pp. 62–75 (2020)
34. Simon, C., Afzelius, M., Appel, J., de La Giroday, A.B., Dewhurst, S., Gisin, N., Hu, C., Jelezko, F., Kröll, S., Müller, J., et al.: Quantum memories. *The Eur. Phys. J. D* **58**(1), 1–22 (2010)
35. Stacey, W., Annabestani, R., Ma, X., Lütkenhaus, N.: Security of quantum key distribution using a simplified trusted relay. *Phys. Rev. A* **91**(1), 012338 (2015)
36. Wang, H., Zhao, Y., Li, Y., Yu, X., Zhang, J., Liu, C., Shao, Q.: A flexible key-updating method for software-defined optical networks secured by quantum key distribution. *Opt. Fiber Technol.* **45**, 195–200 (2018)
37. Wehner, S., Elkouss, D., Hanson, R.: Quantum internet: a vision for the road ahead. *Science*. **362**, 6412 (2018)
38. Wootters, W.K., Zurek, W.H.: A single quantum cannot be cloned. *Nature* **299**(5886), 802–803 (1982)
39. Xu, F., Curty, M., Qi, B., Lo, H.K.: Practical aspects of measurement-device-independent quantum key distribution. *New J. Phys.* **15**(11), 113007 (2013)
40. Zhao, Y., Cao, Y., Wang, W., Wang, H., Yu, X., Zhang, J., Tornatore, M., Wu, Y., Mukherjee, B.: Resource allocation in optical networks secured by quantum key distribution. *IEEE Commun. Mag.* **56**(8), 130–137 (2018)
41. Zou, X., Qiu, D., Li, L., Wu, L., Li, L.: Semiquantum-key distribution using less than four quantum states. *Phys. Rev. A* **79**(5), 052312 (2009)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Authors and Affiliations

Zhonghui Li¹ · Kaiping Xue^{1,2}  · Qidong Jia¹ · Jian Li¹ · David S. L. Wei³ · Jianqing Liu⁴ · Nenghai Yu^{1,2}

¹ School of Cyber Science and Technology, University of Science and Technology of China, Hefei 230027, China

² Department of Electronic Engineering and Information Science, University of Science and Technology of China, Hefei 230027, China

- ³ Department of Computer and Information Science, Fordham University, Bronx, NY 10458, USA
- ⁴ Department of Electrical and Computer Engineering, University of Alabama in Huntsville, Huntsville, AL 35899, USA