

Multicast-oriented key provision in hybrid DV/CV multi-domain quantum networks

Xinyu Chen(陈欣宇), Yuan Cao(曹原), Yuxiang Lu(陆宇翔), Yue Chen(陈越), Kunpeng Zheng(郑昆朋), Xiaosong Yu(郁小松), Yongli Zhao(赵永利), Jie Zhang(张杰), and Qin Wang(王琴)

Citation: Chin. Phys. B, 2025, 34 (**9**): 090301. DOI: 10.1088/1674-1056/adecf8
http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

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

Witnessing the distribution of sources in quantum networks via hierarchical nonlocality

Shu-Yuan Yang(杨舒媛), Jin-Chuan Hou(侯晋川), and Kan He(贺衍)
Chin. Phys. B, 2025, 34 (**6**): 060303. DOI: 10.1088/1674-1056/add507

Measurement-based entanglement purification for hybrid entangled state

Cheng-Chen Luo(罗程晨), Shi-Pu Gu(顾世浦), Xing-Fu Wang(王兴福), Lan Zhou(周澜), and Yu-Bo Sheng(盛宇波)
Chin. Phys. B, 2025, 34 (**3**): 030307. DOI: 10.1088/1674-1056/adb267

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)
Chin. Phys. B, 2025, 34 (**1**): 010310. DOI: 10.1088/1674-1056/ad9018

Security analysis of satellite-to-ground reference-frame-independent quantum key distribution with beam wandering

Chun Zhou(周淳), Yan-Mei Zhao(赵燕美), Xiao-Liang Yang(杨晓亮), Yi-Fei Lu(陆宜飞), Yu Zhou(周雨), Xiao-Lei Jiang(姜晓磊), Hai-Tao Wang(汪海涛), Yang Wang(汪洋), Jia-Ji Li(李家骥), Mu-Sheng Jiang(江木生), Xiang Wang(汪翔), Hai-Long Zhang(张海龙), Hong-Wei Li(李宏伟), and Wan-Su Bao(鲍皖苏)
Chin. Phys. B, 2024, 33 (**8**): 080306. DOI: 10.1088/1674-1056/ad51f6

Verifying hierarchical network nonlocality in general quantum networks

Shu-Yuan Yang(杨舒媛), Jin-Chuan Hou(侯晋川), and Kan He(贺衍)
Chin. Phys. B, 2024, 33 (**7**): 070304. DOI: 10.1088/1674-1056/ad3dd5

SPECIAL TOPIC — Quantum communication and quantum network

Multicast-oriented key provision in hybrid DV/CV multi-domain quantum networks

Xinyu Chen(陈欣宇)[1], Yuan Cao(曹原)[1,†], Yuxiang Lu(陆宇翔)[1], Yue Chen(陈越)[1], Kunpeng Zheng(郑昆朋)[2], Xiaosong Yu(郁小松)[2], Yongli Zhao(赵永利)[2], Jie Zhang(张杰)[2], and Qin Wang(王琴)[1]

[1] *School of Communications and Information Engineering, 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 25 April 2025; revised manuscript received 16 June 2025; accepted manuscript online 8 July 2025)

As the cornerstone of future information security, quantum key distribution (QKD) is evolving towards large-scale hybrid discrete-variable/continuous-variable (DV/CV) multi-domain quantum networks. Meanwhile, multicast-oriented multi-party key negotiation is attracting increasing attention in quantum networks. However, the efficient key provision for multicast services over hybrid DV/CV multi-domain quantum networks remains challenging, due to the limited probability of service success and the inefficient utilization of key resources. Targeting these challenges, this study proposes two key-resource-aware multicast-oriented key provision strategies, namely the link distance-resource balanced key provision strategy and the maximum shared link key provision strategy. The proposed strategies are applicable to hybrid DV/CV multi-domain quantum networks, which are typically implemented by GG02-based intra-domain connections and BB84-based inter-domain connections. Furthermore, the multicast-oriented key provision model is formulated, based on which two heuristic algorithms are designed, i.e., the shared link distance-resource (SLDR) dependent and the maximum shared link distance-resource (MSLDR) dependent multicast-oriented key provision algorithms. Simulation results verify the applicability of the designed algorithms across different multi-domain quantum networks, and demonstrate their superiority over the benchmark algorithms in terms of the success probability of multicast service requests, the number of shared links, and the key resource utilization.

Keywords: quantum networks, discrete-variable (DV), continuous-variable (CV), key provision, multicast services

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

DOI: 10.1088/1674-1056/adecf8 **CSTR:** 32038.14.CPB.adecf8

1. Introduction

In real-world scenarios such as online interaction, video conferencing, and multi-site data center backup, multicasting provides an effective point-to-multipoint communication modality. However, multicast services face several challenging security issues.[1,2] Once the data transmitted to any user in a multicast service is eavesdropped, the sensitive information of all associated users may be exposed. To address these security issues, data encryption is widely employed to protect communications against eavesdropping.[3] Nevertheless, the emergence of powerful quantum computers and quantum algorithms renders conventional key distribution approaches insecure.

Quantum communication encompasses the main branches of quantum key distribution (QKD),[4] quantum teleportation,[5,6] and quantum secure direct communication.[7,8] Among these, QKD has already achieved initial practical applications, ranging from metropolitan networks[9–14] to wide-area networks.[15,16] It enables the generation of information-theoretically secure keys without relying on computational complexity assumptions, thereby effectively defending against potential threats from quantum computers.

Over the past decades, various advanced QKD protocols have been developed since the original BB84 protocol proposed by Bennett and Brassard in 1984.[17] These protocols are generally categorized into discrete-variable (DV) and continuous-variable (CV) approaches, each with unique advantages stemming from their intrinsic mechanisms. For example, the GG02 protocol[18] is highly compatible with existing telecom infrastructures and can achieve higher secret key rates (SKRs) over relatively short distances. In contrast, the BB84 protocol typically supports longer transmission distances. To date, a variety of QKD protocols have been successfully deployed in real-world quantum networks, including BB84-based networks in Cambridge[10] and London,[11] as well as GG02-based networks in Madrid[12] and Shanghai.[13] These field experiments have demonstrated the feasibility of building practical quantum networks with different QKD protocols. In practice, however, achieving higher performance requires more sophisticated systems and incurs greater costs.

[†]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.

Therefore, it is preferable for quantum networks to adopt protocols suited to their specific requirements rather than relying on a single QKD protocol.

In recent years, the continuous evolution of QKD protocols and the growing demand from multiple users have spurred increasing research interest in large-scale multi-protocol quantum networks. In Ref. [19], a network architecture for software-defined heterogeneous QKD chaining was proposed, considering the characteristics of different protocols. Flexible switching between BB84 and measurement-device-independent (MDI) protocols in a non-standalone network was demonstrated in Ref. [20], while a multi-protocol CV-QKD system was experimentally realized in Ref. [21]. To support the transition from single-protocol to large-scale multi-protocol quantum networks, a multi-protocol translation framework was introduced.[22] Furthermore, recent studies have investigated multi-protocol upgrading[23] and updating[24] in quantum metro networks, as well as multi-protocol relay chaining[25] in large-scale quantum networks.

In particular, integrating DV and CV protocols within a single quantum network has been recognized as an effective means of leveraging their respective strengths while mitigating their limitations. The feasibility of integrating CV and DV protocols in a real-world quantum metro network was demonstrated in Madrid, Spain.[26] Moreover, a scalable quantum network model based on hybrid CV and DV protocols was presented,[27] confirming the applicability of CV-QKD for intra-domain links and DV-QKD for inter-domain links. As such, the hybrid DV/CV multi-domain quantum network has emerged as a practical scenario for large-scale quantum network deployment. In this context, due to the different characteristics of inter- and intra- domain QKD links as well as the diverse locations of multiple users, multi-party key negotiation becomes a critical challenge requiring further study. In recent years, alongside the development of point-to-multipoint QKD protocols and systems,[28] multicast technologies for multi-party key negotiation have also been explored. In fiber-based quantum networks, a tree-topology-based quantum-key-relay strategy was proposed for secure multicast services,[29] where a multi-relay node structure was designed to enable point-to-multipoint key relaying. Dong *et al.*[30] proposed a secure multicast scheme for quantum data center networks, while He *et al.*[31] developed a routing and secret key assignment algorithm for multicast services in quantum satellite networks. However, multicast technologies in hybrid DV/CV quantum networks remain largely unexplored, particularly regarding the challenge of dynamically adapting to practical DV/CV QKD environments.

In this work, to achieve efficient multi-party key negotiation for securing multicast services, we focus on the problem of multicast-oriented key provision in hybrid DV/CV multi-domain quantum networks. For multicast services in quantum networks,[29] traditional methods may lead to inefficient utilization of key resources and a relatively high probability of key provision failure, since they often overlook the real characteristics (e.g., distance and SKR) of DV/CV-based QKD links. By developing key-resource-aware multicast-oriented key provision strategies, we aim to overcome the limitations of traditional methods that lack dynamic adaptability to hybrid DV/CV key resources. The main contributions of this work are summarized as follows.

(i) We propose a link distance-resource balanced key provision strategy and a maximum shared link key provision strategy, in which the link weight factor is jointly determined by the link distance and SKR slices, thereby overcoming the limitation of relying solely on the link distance factor.

(ii) We formulate the multicast-oriented key provision model, where the SKR model for the QKD path is derived from the typical SKR models of the BB84 and GG02 protocols. Moreover, we define the global, inter-domain, and intra-domain key resource utilization to characterize the efficiency and distribution of key resource consumption across the multi-domain quantum network.

(iii) We design two heuristic algorithms to implement the proposed key provision strategies, namely the shared link distance-resource (SLDR) dependent and the maximum shared link distance-resource (MSLDR) dependent multicast-oriented key provision algorithms.

(iv) We evaluate the proposed algorithms on two hybrid DV/CV multi-domain quantum network topologies, where their applicability and effectiveness are validated and compared against benchmark algorithms.

The remainder of this paper is organized as follows. Section 2 describes the key-resource-aware multicast-oriented key provision strategies. Section 3 formulates the multicast-oriented key provision model. Section 4 presents the heuristic algorithms. Section 5 provides simulation results and a detailed performance analysis. Finally, Section 6 concludes the paper.

2. Key-resource-aware multicast-oriented key provision strategy

This section introduces the key-resource-aware multicast-oriented key provision strategies for hybrid DV/CV multi-domain quantum networks. This includes a description of the hybrid DV/CV multi-domain network scenario, a discussion of traditional methods, and the introduction of two novel key provision strategies.

2.1. Hybrid DV/CV multi-domain quantum networks

In a hybrid DV/CV multi-domain quantum network, multiple quantum metro networks are interconnected via inter-

domain links. Each domain may adopt a specific QKD protocol depending on its physical constraints and user requirements. In this work, two representative protocols are considered: the BB84 protocol for DV-QKD and the GG02 protocol for CV-QKD. As shown in Fig. 1, we focus on a common hybrid architecture in which the GG02 protocol is used for intra-domain links owing to its high SKRs, while the BB84 protocol is applied to inter-domain links to support longer transmission distances. This configuration offers a practical framework for the construction of hybrid DV/CV quantum networks.

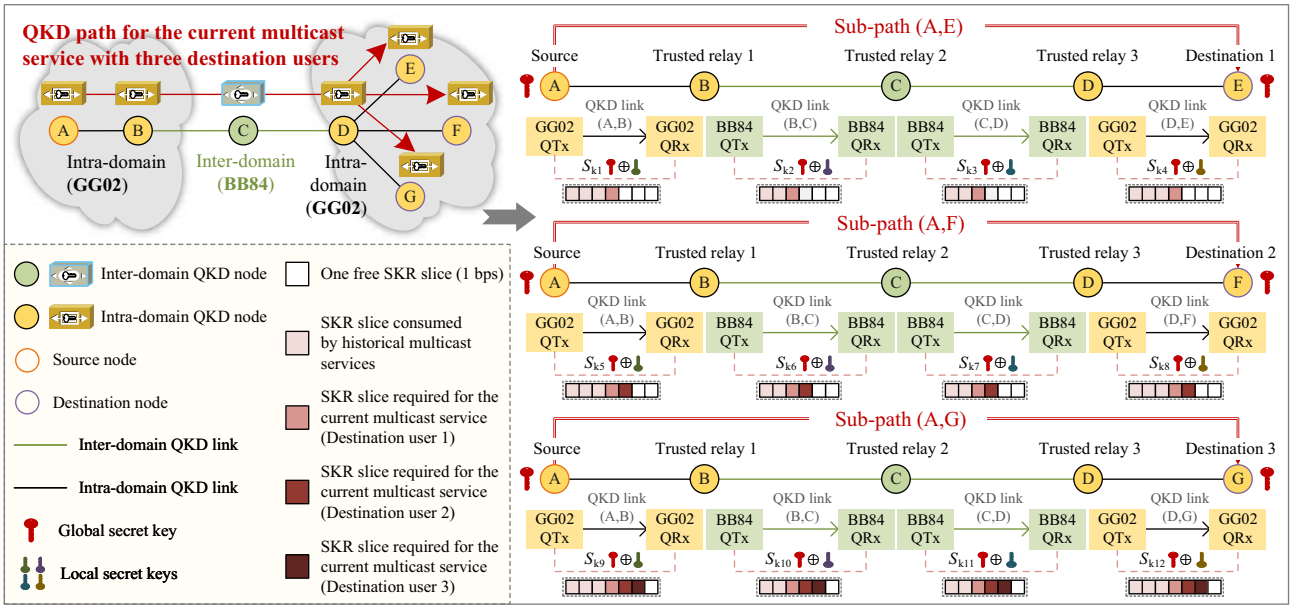


Fig. 1. Illustration of the multicast-oriented key provision in hybrid DV/CV multi-domain quantum networks.

A quantum network commonly comprises multiple QKD nodes interconnected by QKD links.[4] The QKD link consists of the quantum channel and the classical channel. The quantum channel is responsible for transmitting quantum signals, whereas the classical channel performs classical communication tasks for key negotiation. Each QKD node is equipped with several QKD devices, including QKD transmitters (QTxs) and QKD receivers (QRxs). In a multi-domain quantum network, QKD nodes are divided into inter-domain and intra-domain QKD nodes based on their connections and locations. The inter-domain QKD nodes are equipped with QKD devices for realizing the inter-domain protocol. Some intra-domain QKD nodes have devices supporting only the intra-domain protocol, while some bordering intra-domain QKD nodes connected to the inter-domain QKD nodes require QKD devices that support both intra- and inter-domain protocols. This allows different QKD protocols to interoperate seamlessly.

In the multi-domain quantum network, a multicast service involves a source node and multiple destination nodes, with the source and destination nodes located in different quantum metro networks. Figure 1 exemplifies the establishment of a hybrid DV/CV QKD path between the source and destination nodes of a multicast service, which is composed of several sub-paths corresponding to different destination nodes. The path from the source node to each destination node of a multicast service is referred to as a subpath. Hence, a QKD path consists of all the QKD links and QKD nodes involved in its sub-paths. As exemplified in Fig. 1, the source of the multicast service is QKD node A, and the associated destination nodes are E, F, and G. According to the routing algorithm, the sub-paths from the source node to three destination nodes are determined as "A–B–C–D–E", "A–B–C–D–F", and "A–B–C–D–G", respectively. The QKD links generate local secret keys S_{k1} to S_{k12}, which are stored in their respective key managers. The trusted relays are employed to forward the global secret key from the source node to the destination node in a hop-by-hop manner. An example of the trusted relay chain relying on the sub-path (A, E) is as follows.

(i) **Source QKD Node** encrypts the global secret key S_k using S_{k1} and sends the ciphertext $S_{k1} \oplus S_k$ to trusted relay 1;

(ii) **Trusted relay 1** decrypts S_k based on $S_{k1} \oplus (S_{k1} \oplus S_k) = S_k$, then encrypts S_k using S_{k2} and sends the ciphertext $S_{k2} \oplus S_k$ to trusted relay 2;

(iii) **Trusted relay 2** decrypts S_k based on $S_{k2} \oplus (S_{k2} \oplus S_k) = S_k$, then encrypts S_k using S_{k3} and sends the ciphertext $S_{k3} \oplus S_k$ to trusted relay 3;

(iv) **Trusted relay 3** decrypts S_k based on $S_{k3} \oplus (S_{k3} \oplus S_k) = S_k$, then encrypts S_k using S_{k4} and sends the ciphertext $S_{k4} \oplus S_k$ to destination QKD node;

(v) **Destination QKD node** decrypts S_k based on $S_{k4} \oplus (S_{k4} \oplus S_k) = S_k$. Finally, the global secret key S_k is shared between the source and destination nodes.

In order to improve the usage of precious key resources,

here we introduce the SKR slicing approach. In practice, the SKRs on different QKD links in the quantum network may be different, which can be segmented into a string of small SKR slices to accommodate multiple services. In this work, the size of an SKR slice is uniformly set to 1 bps. Based on Fig. 1, we illustrate this slicing approach using the QKD link (A, B) as an example. The total SKR slices on this QKD link are 7 bps, in which 3 bps have already been consumed by historical multicast services, leaving 4 bps of free SKR slices. The current multicast service requires 1 bps per sub-path, and since all three sub-paths pass through this QKD link, the multicast service occupies a total of 3 bps on QKD link (A, B). In practice, by allocating SKR slices on demand, more multicast services can be supported with limited physical QKD devices.

2.2. Traditional methods for multicast-oriented key provision

Figure 2 depicts two traditional methods for multicast-oriented key provision. Figure 2(a) illustrates a multi-domain quantum network topology, where the GG02 protocol is used for intra-domain links and the BB84 protocol is used for inter-domain links, with routing performed using the link weight factor characterized by the link distance. The SKR requirement of a multicast service is 1 bps (i.e., one SKR slice) with source node A and destination nodes E, F, and G. The QKD path from the source node to the destination nodes is the shortest path selected relying on the link weight factor, yielding the following sub-paths: "A–B–C–D–E", "A–B–C–D–F", and "A–J–I–H–G".

For the traditional method 1, as exemplified in Fig. 2(b), the QKD link (A, B) consumes 2 bps of SKR slices to encrypt the same global secret key S_k, which is wasteful, as only one SKR slice is sufficient. This method ignores the fact that the global secret key is identical for all destination nodes of a multicast service. As a result, the same global secret key may be redundantly encrypted with different local secret keys on the same QKD link, leading to inefficient use of key resources.

As shown in Fig. 2(c), the traditional method 2 provides a more efficient way to conserve key resources by exploiting the uniqueness of the global secret key required by the multicast service and aggregating the sub-paths onto shared links, thereby reducing overall key consumption. As an example, when the source node A distributes the global secret key S_k to destination nodes E, F, and G, only one SKR slice is consumed on link (A, B), whereas two SKR slices are required in traditional method 1. Hence, the total consumption of SKR slices is reduced from 12 bps to 9 bps.

It is important to note that the use of shared links does not compromise the security of multi-party key negotiation. Considering that a multicast service requires the sharing of global secret keys between a source node and multiple destination nodes, the use of shared links can serve as a routing optimization mechanism to conserve key resources for multicast-oriented key provision, instead of reusing local secret keys.

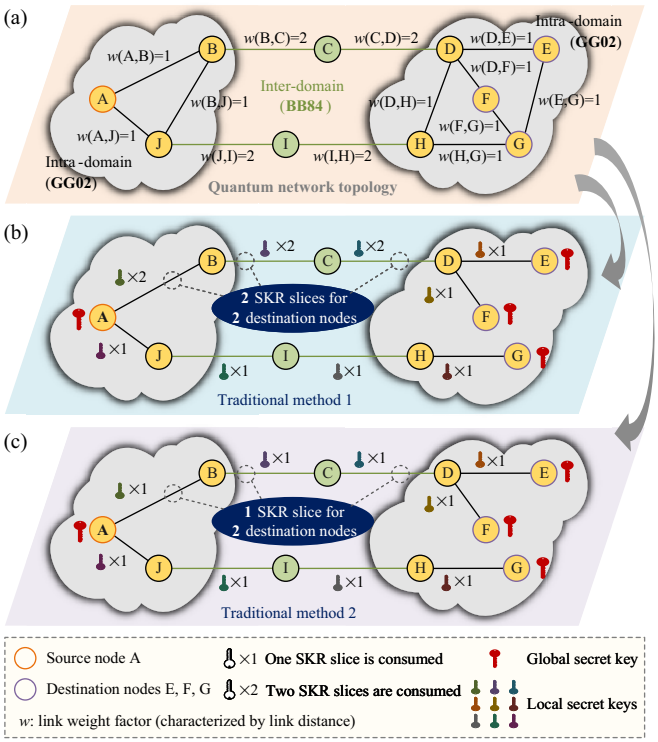


Fig. 2. Illustration of the traditional methods for multicast-oriented key provision: (a) quantum network topology, (b) traditional method 1, and (c) traditional method 2.

2.3. Link distance-resource balanced key provision strategy

The traditional method 2 illustrated in Fig. 2 provides an efficient solution for multicast-oriented key provision. However, the link weight factor characterized only by the link distance may not consider the availability of key resources on the QKD link. Therefore, we introduce a new link weight factor in this subsection, characterized by both the link distance and real-time free SKR slices.

To account for the different values in the link weight factor, we normalize the link distance and real-time free SKR slices. For the physical distance z (m, n) in kilometers (km) of the QKD link (m, n), we normalize it as

$$\tilde{z}(m,n) = \frac{z(m,n)}{z_{\max}}, \tag{1}$$

where $z_{\max}$ is the maximum physical distance among all QKD links in the multi-domain quantum network. The higher value of $\tilde{z}(m,n)$ indicates a longer QKD link.

Furthermore, for the real-time free SKR slices $y(m,n)$ in units of bps on the QKD link (m, n), we normalize it as

$$\tilde{y}(m,n) = \frac{y(m,n)}{y_{\max}}, \tag{2}$$

where $y_{\max}$ represents the maximum real-time free SKR slices among all QKD links in the multi-domain quantum network.

The higher value of $\tilde{y}(m,n)$ indicates more available key resources.

Accordingly, the link weight factor can be expressed as

$$w(m,n) = \frac{\tilde{z}(m,n)}{\tilde{y}(m,n)+\varepsilon}, \tag{3}$$

where ε is a very small constant introduced to avoid division by zero. The value of ε does not need to be dynamically adjusted. Hence, including such a small positive constant introduces neither computational nor logical complexity to the model. Compared to other optional models such as the additive model, Eq. (3) naturally emphasizes QKD links that are both short and resource-rich, without requiring the introduction of weighting parameters. Moreover, this model for the link weight factor scales well with diverse link characteristics and resource conditions. This factor balances the tradeoff between link distance and key resource availability. A smaller link weight factor indicates a more favorable link for routing.

Figure 3(a) illustrates the difference between the distance-only link weight factor and the new distance-resource link weight factor. As an example, the QKD links (I, H) and (C, D) have the same physical distance, hence their link weight factors are equal under the distance-only routing, i.e., $w(\mathrm{I},\mathrm{H}) = 2$ and $w(\mathrm{C},\mathrm{D}) = 2$. However, their real-time free SKR slices are different, that is, 1 bps on QKD link (I,H) and 4 bps on QKD link (C, D). By jointly considering the link distance and real-time free SKR slices, the corresponding link weight factors are adjusted to $w(\mathrm{I},\mathrm{H}) = 4$ and $w(\mathrm{C},\mathrm{D}) = 1$, thus making the QKD link (C, D) more likely to be selected.

Figure 3(b) shows the QKD path selected based on the new link weight factors. It is obvious that the sub-path from source node A to destination node G is changed to "A–B–C–D–F–G", which traverses a different inter-domain route compared to using the distance-only link weight factor. Although the total path distance increases, the selected QKD links have more abundant key resources, thereby contributing to a higher success probability of the multicast service.

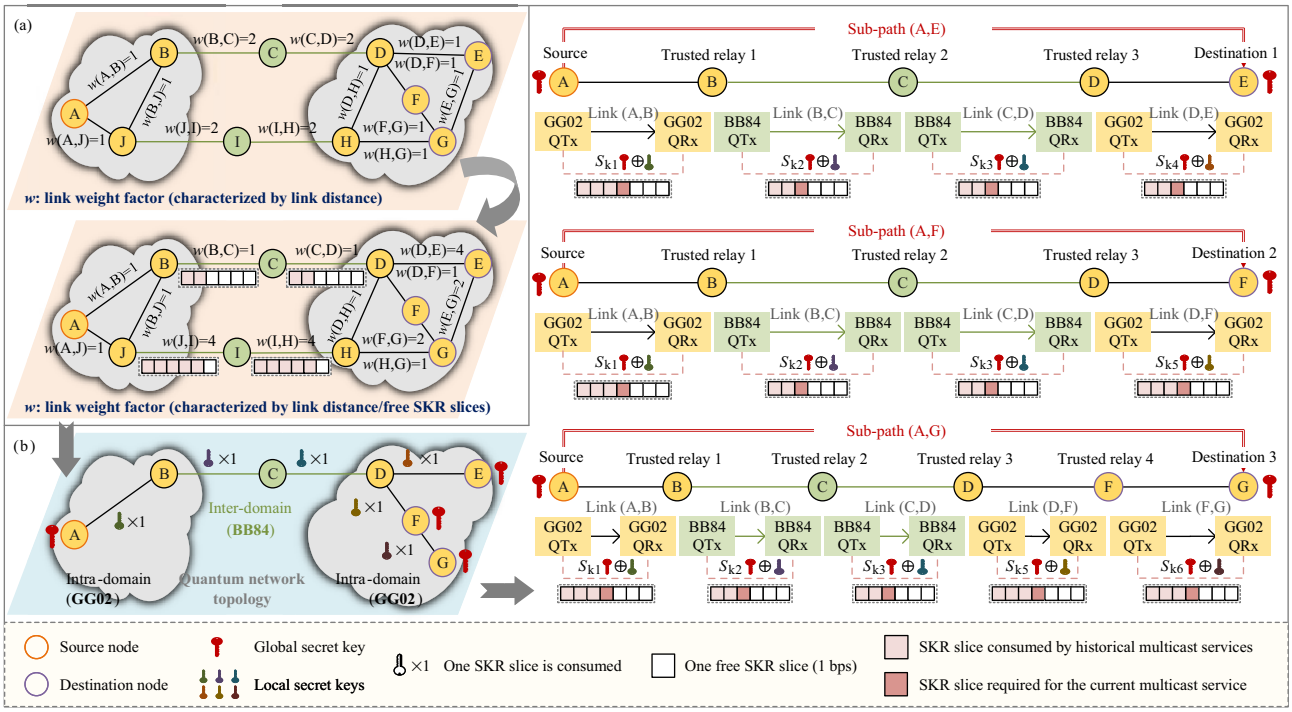


Fig. 3. Illustration of the link distance-resource balanced key provision strategy: (a) link weight factor transformation and (b) the QKD path selected based on the new link weight factor (characterized by link distance/free SKR slices).

2.4. Maximum shared link key provision strategy

In the previously discussed methods, each sub-path exhibits a high degree of independence, i.e., each sub-path from the source node to a destination node is determined independently. However, the multicast service has a unique feature: its multiple destination nodes usually share some links of the QKD path. Capitalizing on this feature can reduce key consumption and improve the overall success probability of key provision. In this regard, we propose the maximum shared link key provision strategy, as illustrated in Fig. 4. This strategy aims to maximize the usage of shared QKD links from the source node to multiple destination nodes during path construction for a multicast service. It consists of the following four steps:

(i) Initial path selection: Similar to the link distance-resource balanced key provision strategy, we first select initial sub-paths from the source node to each destination node independently, relying on both the physical distance and the real-

time free SKR slices of QKD links. As shown in Fig. 4(a), the initial sub-paths are as follows: "A–B–C–D–E", "A–B–C–D–F", and "A–B–C–D–F–G".

(ii) Destination node sorting: The destination nodes of the multicast service are sorted in ascending order based on the sum of link weight factors M of their corresponding sub-paths. In this case, the order is: F ($M = 4$), G ($M = 6$), and E ($M = 7$).

(iii) Topology updating and re-routing: The original sub-path to destination node F is retained as a reference. To facilitate link sharing, we update the topology by setting the link weight factors between the source node and all other nodes on the sub-path to F as zero. If such QKD links do not exist on the original topology, virtual links are created (e.g., AC, AD, AF), as shown in Fig. 4(b). Using this updated topology, we re-select the sub-path to G and obtain "A–F–G". Next, a similar process is performed for the sub-path to destination node E, that is, we update the topology again by adding a virtual link (AG) with a zero link weight factor, as shown in Fig. 4(c), then re-calculate the sub-path to E and obtain "A–G–E".

(iv) Path construction and topology restoration: After determining all the sub-paths, the final results are as follows: "A–B–C–D–F", "A–B–C–D–F–G", and "A–B–C–D–F–G–E", as shown in Fig. 4(d). Finally, all virtual links added during the re-routing process are removed, and the modified link weight factors are restored to their original values, yielding the final QKD path.

This strategy not only enhances the link sharing among multiple destination nodes and reduces key resource consumption, but also improves the overall transmission efficiency and success probability of multicast services, providing effective support for their establishment in hybrid DV/CV multi-domain quantum networks.

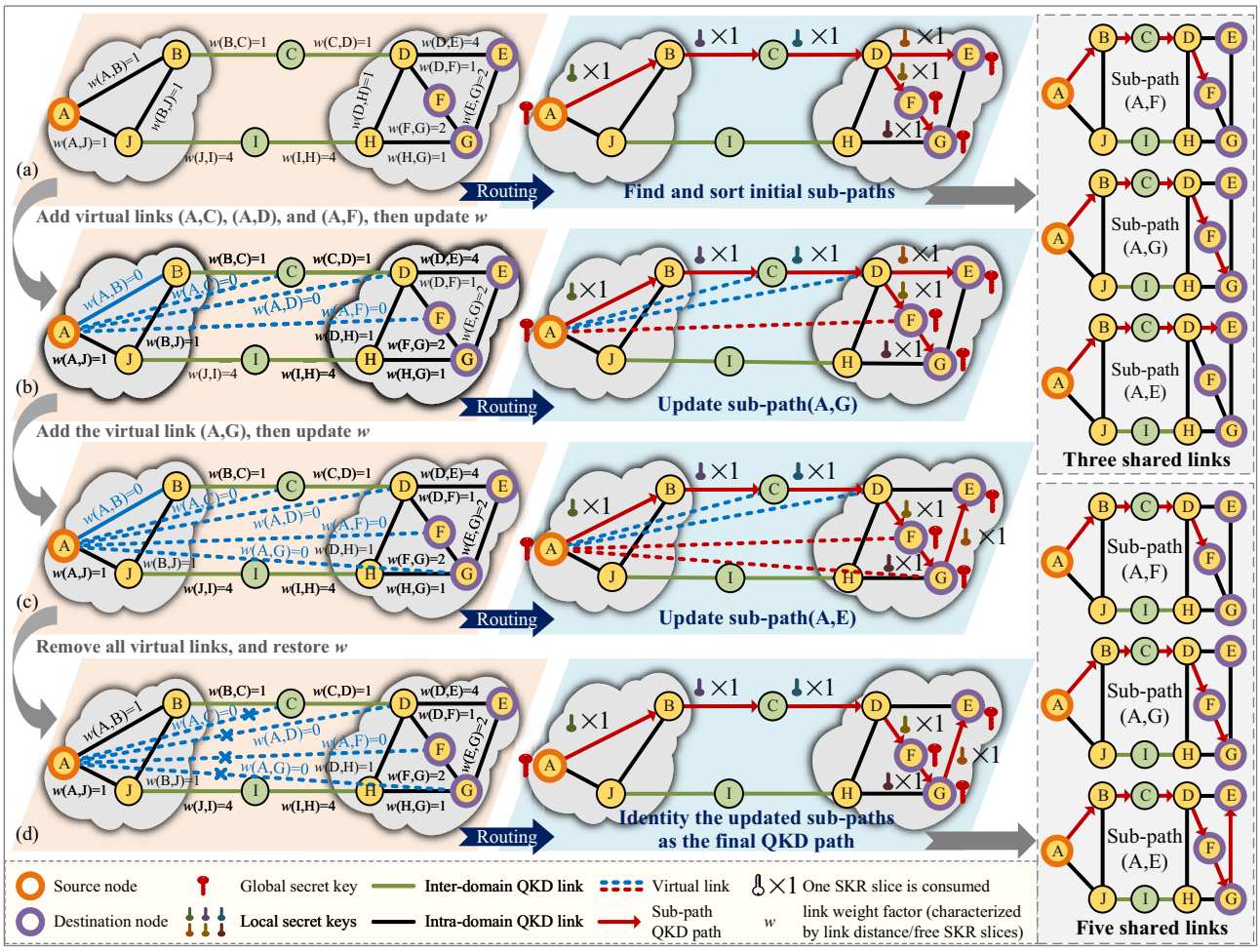


Fig. 4. Illustration of the maximum shared link key provision strategy: (a) find and sort initial sub-paths, (b) update sub-path (A, G), (c) update sub-path (A, E), and (d) identify the final QKD path.

3. Multicast-oriented key provision model

This section formulates the multicast-oriented key provision model in hybrid DV/CV multi-domain quantum networks, which primarily comprises the network model and the SKR model.

3.1. Network model

We model a multi-domain quantum network topology as $G(N, L)$, where N and L denote the sets of QKD nodes and

QKD links, respectively. The sets of inter-domain and intra-domain QKD links are denoted as L_e and L_a, respectively. Accordingly, the corresponding SKR generated on each QKD link can be obtained based on the relationship between the SKR and the transmission distance of different QKD protocols. The specific SKR models will be described in Subsection 3.2.

A multicast service request can be modeled as $r(s_r, D_r, k_r, t_r)$, where s_r denotes the source node of r, D_r ($d_r \in D_r$) is the set of destination nodes, and k_r and t_r indicate the required SKR and duration of r, respectively. Let R denote the set of all multicast service requests. The QKD path selected for the multicast service request r is denoted as $P_r(E_r, V_r, g_r)$, where E_r and V_r denote the sets of QKD links and QKD nodes on P_r, respectively. The variable g_r indicates the achievable SKR for the QKD path P_r. The sub-path for each destination node d_r is denoted as $p_{d_r} \in P_r$. In addition, we define M_{d_r} as the sum of the link weight factors of QKD links on the sub-path p_{d_r}.

The success probability of multicast service requests is an important metric for evaluating the performance of multicast-oriented key provision solutions, defined as

$$\alpha = \frac{|R_S|}{|R|}, \tag{4}$$

where R_S is the set of multicast service requests that successfully accomplish the key provision.

The number of shared links is associated with the total number of QKD links and SKR slices occupied by each multicast service request. More shared links allow more secret keys to be shared along the path for a multicast service request, thereby reducing the number of additional SKR slices consumed. The number of shared links for multicast service request r is γ_r. In the case of no shared key resources, γ_r is 0. The average number of shared links is defined as

$$\gamma = \frac{1}{|R_S|} \sum_{r \in R_S} \gamma_r. \tag{5}$$

3.2. SKR model

In this subsection, we present the typical SKR models for the BB84 and GG02 protocols. These models are then used to analyze the achievable SKRs of QKD paths employing these protocols under the proposed solutions.

The SKR of the BB84 protocol can be calculated by[32,33]

$$g_{\mathrm{BB84}} = q[-fQ_\mu H_2(E_\mu) + Q_1(1 - H_2(e_1))], \tag{6}$$

where q represents the basis reconciliation factor, f denotes the error correction efficiency, Q_μ is the overall gain of signal states, and E_μ is the quantum bit error rate. Additionally, Q_1 and e_1 are the gain and error rate of single-photon pulses, respectively. In this study, the three-intensity decoy-state method[33] is utilized with the BB84 protocol. Specifically, the binary Shannon entropy function is defined as

$$H_2(x) = -x\log_2 x - (1-x)\log_2(1-x). \tag{7}$$

Furthermore, the SKR of the GG02 protocol can be calculated by[34]

$$g_{\mathrm{GG02}} = \frac{n_f}{N_f}\left(\beta I_{AB} - \chi_{bE} - \Delta(n_f)\right), \tag{8}$$

where N_f and n_f denote the total sampling length and the block length for final key estimation, respectively. In addition, β is the reconciliation efficiency, I_{AB} represents the Shannon mutual information between Alice and Bob, χ_{bE} indicates the Holevo bound. In addition, $\Delta(n_f)$ is related to the security of the privacy amplification.

Using the SKR models for the BB84 and GG02 protocols, the SKR of each QKD link along the QKD path can be obtained. Subsequently, the total number of SKR slices for each QKD link can be derived based on the SKR of that link and its corresponding number of QKD devices. The achievable SKR for the QKD path is defined as the minimum number of SKR slices consumed across all QKD links along the path, which can be expressed as

$$g_r = \min(\{y_e | e \in E_r\}), \tag{9}$$

where y_e denotes the SKR slices consumed on each QKD link e along the path P_r.

The key resource utilization is an effective indicator to evaluate the efficiency of key provision in quantum networks. This indicator not only shows whether key resources are fully utilized, but also reflects any resource waste or redundancy in the quantum network when accommodating multicast service requests. In a multi-domain quantum network, the global, inter-domain, and intra-domain key resource utilization are defined as follows:

$$\eta_{\mathrm{global}} = \frac{\sum_{l \in L}(y_l^{\mathrm{ini}} - y_l)}{\sum_{l \in L} y_l^{\mathrm{ini}}}, \tag{10}$$

$$\eta_{\mathrm{inter}} = \frac{\sum_{l \in L_e}(y_l^{\mathrm{ini}} - y_l)}{\sum_{l \in L_e} y_l^{\mathrm{ini}}}, \tag{11}$$

$$\eta_{\mathrm{intra}} = \frac{\sum_{l \in L_a}(y_l^{\mathrm{ini}} - y_l)}{\sum_{l \in L_a} y_l^{\mathrm{ini}}}, \tag{12}$$

where y_l^{ini} and y_l represent the initial and real-time free SKR slices of each QKD link l in the multi-domain quantum network, respectively.

4. Heuristic algorithm design

This section presents two heuristic algorithms based on the proposed strategies for efficient multicast-oriented key provision in hybrid DV/CV multi-domain quantum networks. These two algorithms are referred to as the SLDR dependent algorithm and the MSLDR dependent algorithm for multicast-oriented key provision. Their detailed pseudocodes are presented in Algorithms 1 and 2. In each algorithm, line 1 initializes the elements and line 28 returns the results of QKD path establishment for successful multicast service requests. Based on these returned results, the values of α, γ, η_{global}, η_{inter}, and η_{intra} can be calculated.

In Algorithm 1, the QKD path is determined by considering both link distance and key resources, while key resource sharing is applied on QKD links with overlapping sub-paths. Line 3 updates the real-time free SKR slices of each QKD link in the multi-domain quantum network. Lines 4–6 update the link weight factors based on Eq. (3). Lines 7–9 find the sub-path for each destination node of the multicast service request according to the Dijkstra algorithm. Lines 10–19 record the QKD path information based on the sub-paths, with each link and node recorded only once. Lines 20–26 calculate the achievable SKR for the QKD path to check whether it fulfills the SKR requirement. If satisfied, the QKD path is output, and this multicast service request is inserted into the set of successful multicast service requests. Additionally, the SKR slices required for r are allocated for each QKD link along the path P_r. The multicast service request r is identified as failed if the achievable SKR for the QKD path cannot fulfill the SKR requirement. While finding the shortest path for multicast service requests, this algorithm considers the current network key resources, allowing requests to preferentially utilize QKD links with abundant resources.

Algorithm 1: SLDR algorithm.

Input: A multi-domain quantum network $G(N,L)$ and the set of multicast service requests R.
Output: The set of successful multicast service requests R_{S} and the corresponding QKD paths $P_r(E_r,V_r,g_r)$ for each $r \in R_{\text{S}}$.

1: initialize $R_{\text{S}} \leftarrow \emptyset$, $W \leftarrow \emptyset$;
2: **for** each multicast service request $r(s_r,D_r,k_r,t_r) \in R$ **do**
3: update the real-time free SKR slices of each QKD link in the multi-domain quantum network;
4: **for** each QKD link $l \in L$ **do**
5: update the link weight factor $w(m,n)$ of QKD link l based on Eq. (3) and insert it into set W;
6: **end for**
7: **for** each $d_r \in D_r$ **do**
8: perform routing from s_r to d_r using the Dijkstra algorithm according to W, and record the selected sub-path p_{d_r};
9: **end for**
10: **for** each sub-path p_{d_r} **do**
11: **for** each QKD node v on p_{d_r} **do**
12: **if** $v \notin V_r$ **then** insert v into V_r;
13: **end if**
14: **end for**
15: **for** each QKD link e on p_{d_r} **do**
16: **if** $e \notin E_r$ **then** insert e into E_r and find the real-time free SKR slices y_e;
17: **end if**
18: **end for**
19: **end for**
20: $g_r \leftarrow \min(\{y_e | e \in E_r\})$;
21: **if** $g_r \geq k_r$ **then**
22: identify $P_r(E_r,V_r,g_r)$ as the final QKD path for r;
23: allocate the required SKR slices for each QKD link on P_r;
24: **else**
25: mark the multicast service request r as failed;
26: **end if**
27: **end for**
28: **return** R_{S}, $P_r(E_r,V_r,g_r)$ for $r \in R_{\text{S}}$.

The time complexity of Algorithm 1 is analyzed below. The worst-case complexity of lines 3–6 is $O(|L|)$. The time complexity of lines 7–9 is $O((|N|-1)(|N|+|L|)\log|N|)$. The time complexity of lines 10–26 is $O((|N|-1)(|N|+|L|))$. Accordingly, the overall time complexity of the SLDR algorithm is $O(|R|(|L|+(|N|-1)(|N|+|L|)(\log|N|+1)))$.

Algorithm 2 aims to maximize the number of shared links to further reduce the key resources consumed by multicast service requests. Line 3 performs the same operations as lines 3–6 in Algorithm 1. Lines 4–7 compute the initial sub-path for each destination node according to the Dijkstra algorithm and calculate the sum of the link weight factors for each sub-path. Line 8 sorts the destination nodes in ascending order based on the sum of link weight factors of their correspond-

ing sub-paths. Lines 9–15 sequentially update the sub-paths for each destination node to maximize the number of shared links. More specifically, line 11 adds virtual links based on the sub-path of the current destination node and updates the link weight factors of the corresponding links. Line 12 reroutes the next destination node on the updated topology. After updating the sub-paths, line 16 removes all virtual links and restores the link weight factors of QKD links that were set to zero. Lines 17–24, similar to Algorithm 1, record the QKD path information, ignoring any virtual links. Line 25 verifies the key resources, and line 26 follows the same logic as lines 21–26 of Algorithm 1. Unlike Algorithm 1, which attempts to find short and key-abundant QKD links, this algorithm aims to find QKD paths with as many shared links as possible to establish a multicast service with fewer key resources, even if the sub-path distance is relatively long.

The time complexity of Algorithm 2 is analyzed as follows. The worst-case complexity of line 3 is $O((|N|-1)(|N|+|L|)\log|N|)$. The complexity of lines 8–16 is $O((|N|-1)(|N|+|L|)\log|N|+(|N|-1)\log(|N|-1))$, and the complexity of lines 17–26 is $O((|N|-1)(|N|+|L|))$. Accordingly, the overall time complexity of the MSLDR algorithm is

$$O\Big(|R|\big(2(|N|-1)(|N|+|L|)\log|N| +(|N|-1)(\log(|N|-1)+|N|+|L|)\big)\Big).$$

Algorithm 2: MSLDR algorithm.

Input: $G(N,L)$, R.
Output: R_S, $P_r(E_r,V_r,g_r)$ for $r\in R_S$.
1: initialize $R_S\leftarrow\emptyset$, $W\leftarrow\emptyset$;
2: **for** each multicast service request $r(s_r,D_r,k_r,t_r)\in R$ **do**
3: execute lines 3–6 of Algorithm 1;
4: **for** each $d_r\in D_r$ **do**
5: compute routing from s_r to d_r based on the Dijkstra algorithm according to W, and record p_{d_r};
6: compute the sum of link weight factors M_{d_r} on p_{d_r};
7: **end for**
8: sort d_r in ascending order according to M_{d_r}, and rename each d_r as d_r^i based on order $i\in[1,|D_r|]$;
9: $j\leftarrow 1$;
10: **while** $|D_r|>1$ **do**
11: add virtual links based on $p_{d_r^j}$, and update W;
12: recompute routing from s_r to d_r^{j+1} according to updated W, and update $p_{d_r^{j+1}}$;
13: remove d_r^j from D_r;
14: $j\leftarrow j+1$;
15: **end while**
16: remove all virtual links and restore W based on step 3;
17: **for** each sub-path $p_{d_r^i}$ **do**
18: **for** each QKD node v on $p_{d_r^i}$ **do**
19: execute lines 12–13 of Algorithm 1;
18: **end for**
21: **for** each QKD link e (ignoring virtual links) on $p_{d_r^i}$ **do**
22: execute lines 16–17 of Algorithm 1;
23: **end for**
24: **end for**
25: $g_r\leftarrow\min(\{y_e\,|\,e\in E_r\})$;
26: execute lines 21–26 of Algorithm 1;
27: **end for**
28: **return** R_S, $P_r(E_r,V_r,g_r)$ for $r\in R_S$.

5. Performance evaluation and discussion

This section evaluates and discusses the applicability and effectiveness of the two designed multicast-oriented key provision algorithms through numerical simulations. The two traditional methods for multicast-oriented key provision introduced in Subsection 2.2 are utilized as the benchmark algorithms (i.e., Benchmark1 and Benchmark2) for comparison. In the simulations, we employ two hybrid DV/CV multi-domain quantum network topologies, as illustrated in Fig. 5. Figure 5(a) shows a two-domain quantum network topology, where the left quantum metro network features a 15-node topology, while the right quantum metro network is based on the real-world Shanghai quantum metro network.[16] These two GG02-based domains are connected by BB84-based inter-domain links, with one or two relays deployed between them. Figure 5(b) depicts a four-domain quantum network topology, which comprises four GG02-based domains with eight to ten QKD nodes each. These domains are interconnected by BB84-based inter-domain links, with one to three relays in between. The variations in the number of QKD nodes and inter-domain

connections across the multi-domain quantum network topologies enable a comprehensive assessment of the adaptability of the designed algorithms.

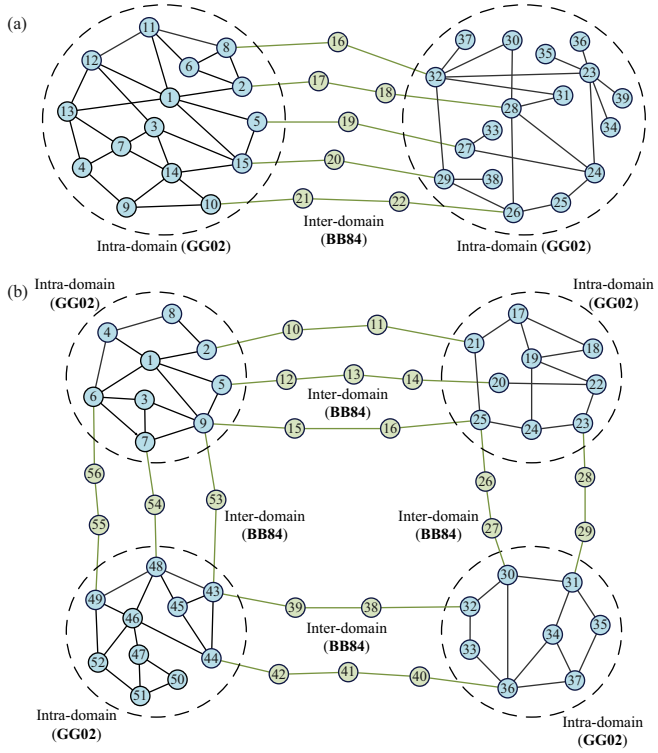


Fig. 5. Hybrid DV/CV multi-domain quantum network topologies used for simulations: (a) two-domain quantum network topology and (b) four-domain quantum network topology.

Table 1. Simulation parameters for BB84 and GG02 protocols.

	BB84[35]	GG02[36]
Misalignment error probability	0.7%	–
Overall dark count rate	3×10^{-7}	–
Detection efficiency	11%	56%
Error correction efficiency	1.5	–
Total pulse number	6.25×10^{8}	–
Fiber loss coefficient (dB/km)	0.2	0.2
Repetition frequency (MHz)	625	100
Total sampling length	–	10^{8}
Block length	–	5×10^{7}
Modulation variance	–	3.246
Excess noise	–	0.022
Electronic noise	–	0.042
Reconciliation efficiency	–	95%

Furthermore, we assume that each QKD link has an ample supply of fiber channels. For both topologies, the physical distances of intra- and inter-domain QKD links are randomly distributed within 10–30 km and 40–80 km, respectively. The simulation analysis considers several variables, including the number of intra- and inter-domain QKD devices, as well as the number and distribution of destination users. Additionally, multicast service requests are randomly generated, with SKR requirements uniformly distributed within 20–80 kbps. The simulation includes a total of 100000 multicast service requests, which arrive dynamically according to a Poisson distribution. Notably, Table 1 lists the simulation parameters used to obtain the SKRs of BB84[35] and GG02[36] protocols.

5.1. Performance evaluation under different numbers of intra- and inter-domain QKD devices

The number of QKD devices (including QTxs and QRxs) within a QKD node can affect the available key resources, hence we conduct the performance evaluation under different numbers of intra- and inter-domain QKD devices. We adopt a node degree-based configuration approach to ensure that the device deployment matches the node's connectivity level, where the number of QKD devices in a QKD node is proportional to the number of QKD links directly connected to that node. Simulations are conducted under a relatively high traffic load of 260 Erlangs. The number of QKD device pairs (i.e., QTxQRx pairs) deployed on an intra-domain QKD link and an inter-domain QKD link are selected from [1, 5] and [1, 7], respectively. The distribution of destination nodes is uniform, i.e., the multicast destination nodes are randomly chosen from all QKD nodes in domains outside the domain where the source node is located.

Figures 6 and 7 depict the success probability of multicast service requests under different device configurations on the two-domain and four-domain quantum network topologies, respectively. In all subplots, clear color variations indicate that the success probability is significantly influenced by the number of QKD devices. Comparison results show that, for the same number of QKD devices, both designed algorithms consistently outperform the benchmark algorithms, validating the effectiveness of our solutions for multicast-oriented key provision.

Moreover, from Figs. 6 and 7 we observe minimal color change from left to right but significant variation from bottom to top, indicating that the success probability is more sensitive to the number of inter-domain QKD devices than to the number of intra-domain QKD devices. This observation aligns well with the characteristics of the selected QKD protocols. Intra-domain communication adopts the GG02 protocol, which offers higher SKRs and typically involves more QKD links within a domain, resulting in relatively abundant key resources. In contrast, inter-domain communication relies on the BB84 protocol, which involves fewer available QKD links and lower SKRs for relatively long inter-domain connections, leading to more constrained key resources. Consequently, increasing the number of inter-domain QKD devices has a more pronounced impact on improving the overall success probability.

Considering overall performance and resource efficiency, we deploy 1 pair of intra-domain QKD devices and 5 pairs of inter-domain QKD devices on each corresponding intra- and

inter-domain QKD link for the two-domain topology, and 1 pair of intra-domain QKD devices and 7 pairs of inter-domain QKD devices for the four-domain topology. In both cases, the designed algorithms achieve a success probability exceeding 95% under a traffic load of 260 Erlangs, while demonstrating good scalability to support higher traffic loads.

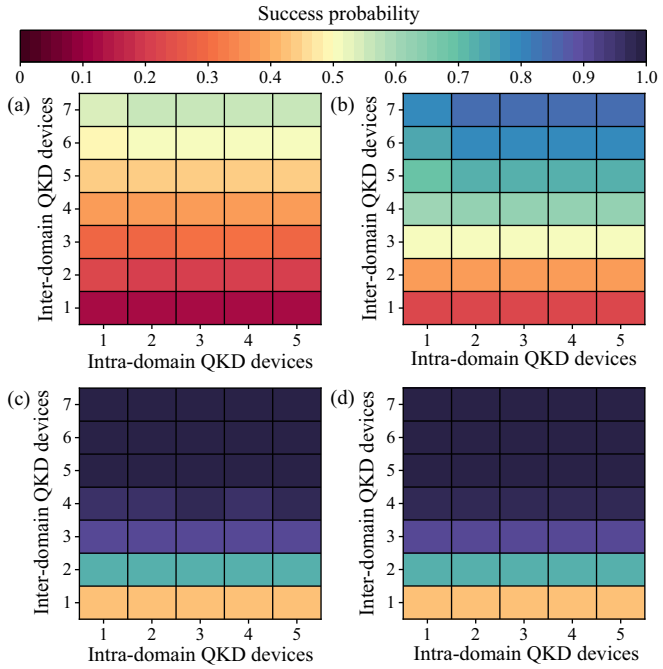


Fig. 6. Success probability of multicast service requests versus the numbers of intra-domain and inter-domain QKD devices for different algorithms on the two-domain quantum network topology: (a) Benchmark1, (b) Benchmark2, (c) SLDR, and (d) MSLDR.

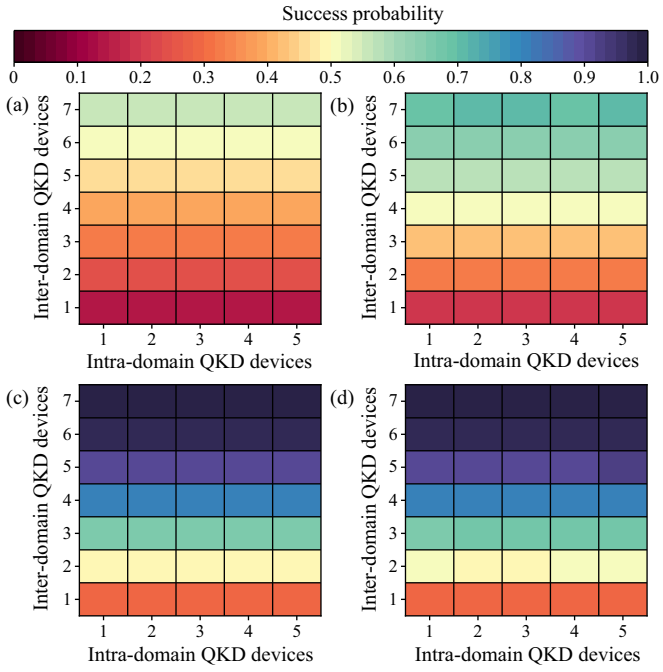


Fig. 7. Success probability of multicast service requests versus the numbers of intra-domain and inter-domain QKD devices for different algorithms on the four-domain quantum network topology: (a) Benchmark1, (b) Benchmark2, (c) SLDR, and (d) MSLDR.

5.2. Performance evaluation under different number of destination nodes

This subsection analyzes the impact of the number of multicast destination nodes ($|D_r|$) on the success probability, the average number of shared links, and key resource utilization. Three intervals for $|D_r|$ are considered: [2, 3], [2, 4], and [2, 5], with destination nodes uniformly selected from all QKD nodes across the multi-domain quantum network (excluding the source domain).

Figure 8 illustrates the success probability of multicast service requests for different algorithms on both the two-domain and four-domain topologies. Overall, within the same interval for $|D_r|$, the MSLDR algorithm consistently achieves the highest success probability, followed by SLDR. For instance, for $|D_r| \in [2,3]$ under 280 Erlangs, the MSLDR algorithm improves the success probability by over 40% compared to the benchmarks, while SLDR also achieves a similar improvement. As the number of destination nodes increases, the success probability of all algorithms decreases due to higher key resource consumption per multicast service request. Benchmark1 is most sensitive, since each additional destination consumes keys along an independent subpath, whereas Benchmark2 benefits from key sharing, reducing resource consumption. The MSLDR and SLDR algorithms show the smallest decline, as they tend to select subpaths with more abundant key resources, demonstrating better adaptability to a growing number of destination users.

Figure 9 illustrates the average number of shared links for different algorithms on the two-domain and four-domain quantum network topologies. Overall, within the same interval of destination nodes, the MSLDR and SLDR algorithms achieve more shared links compared to the benchmark algorithms. Specifically, for $|D_r| \in [2,5]$ under 280 Erlangs, on the two-domain topology, MSLDR and SLDR outperform Benchmark2 by 34.9% and 29.0%, respectively, whereas on the four-domain topology, the corresponding improvements are 47.0% and 33.5%. The MSLDR algorithm achieves the largest number of shared links, consistent with its design goal of maximizing link sharing. SLDR ranks second, reflecting its preference for QKD links with abundant key resources, which naturally induces some sub-path aggregation, particularly in inter-domain segments. In contrast, Benchmark2 exhibits fewer shared links due to its distance-based routing, which selects independent sub-paths with limited coordination, leading to low resource overlap, while Benchmark1 consistently yields zero shared links as it does not support key resource sharing.

As the traffic load increases, the growth of shared links varies across algorithms. The increase is most pronounced for SLDR, moderate for MSLDR, and negligible for Benchmark2. This trend arises because higher traffic loads result in more QKD links being traversed by multicast service re-

quests, thus increasing the demand for key resources. SLDR and MSLDR tend to select QKD links with concentrated key resources, causing multiple sub-paths to converge on a few links. Conversely, Benchmark2's path selection is primarily based on the shortest distance, keeping sub-paths relatively dispersed and reducing aggregation.

Figures 10 and 11 illustrate the key resource utilization versus traffic load for different algorithms under varying numbers of destination nodes on the two-domain and four-domain quantum network topologies, respectively. Overall, the inter-domain key resource utilization is higher than the global utilization, which in turn exceeds the intra-domain utilization. As discussed in Subsection 5.1, BB84-based inter-domain QKD links offer lower SKRs and limited availability, leading to more constrained key resources.

Within the same interval of destination nodes, both SLDR and MSLDR achieve higher global, inter-domain, and intra-domain key resource utilization compared to the benchmark algorithms. Notably, SLDR consistently exhibits slightly higher utilization than MSLDR. This is because, while both algorithms achieve similar success probabilities, SLDR consumes more key resources per service on average, resulting in increased overall utilization. As traffic load rises, SLDR and MSLDR further increase key resource utilization due to shortages on shorter QKD paths, necessitating the use of longer paths with more QKD links and higher key consumption. In contrast, the benchmark algorithms, which always select the shortest paths regardless of key availability, show nearly constant key resource consumption, and thus their overall utilization remains largely unchanged.

These results highlight that increasing the number of multicast destination nodes intensifies pressure on key resource consumption, emphasizing the importance of efficient resource utilization. The MSLDR and SLDR algorithms clearly outperform the benchmarks by maintaining higher success probabilities, achieving more shared links, and dynamically adjusting routing based on real-time key availability. Such capabilities are essential in multi-domain quantum networks to sustain multicast service performance under high traffic loads and a growing number of destination users.

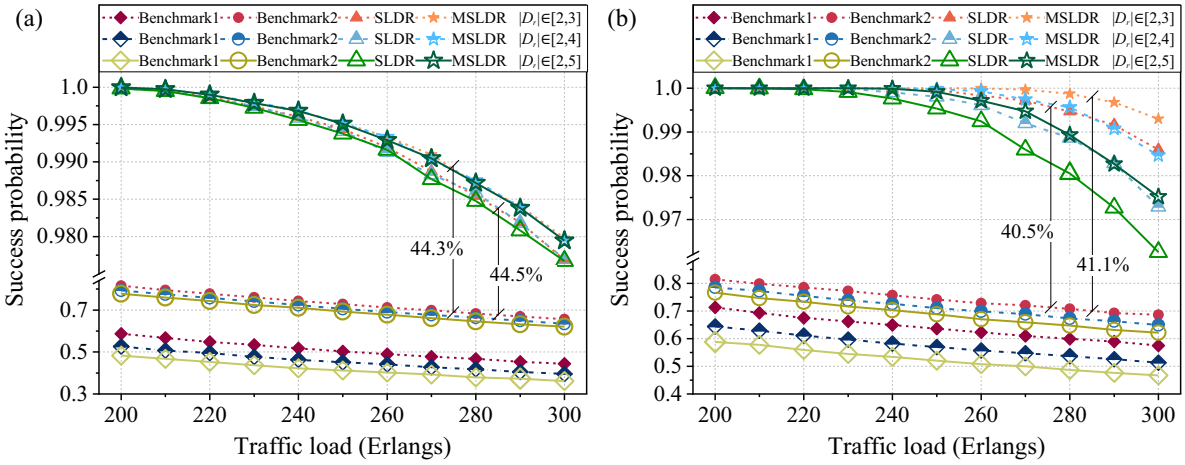


Fig. 8. Success probability of multicast service requests versus traffic load for different algorithms: (a) two-domain quantum network topology and (b) four-domain quantum network topology.

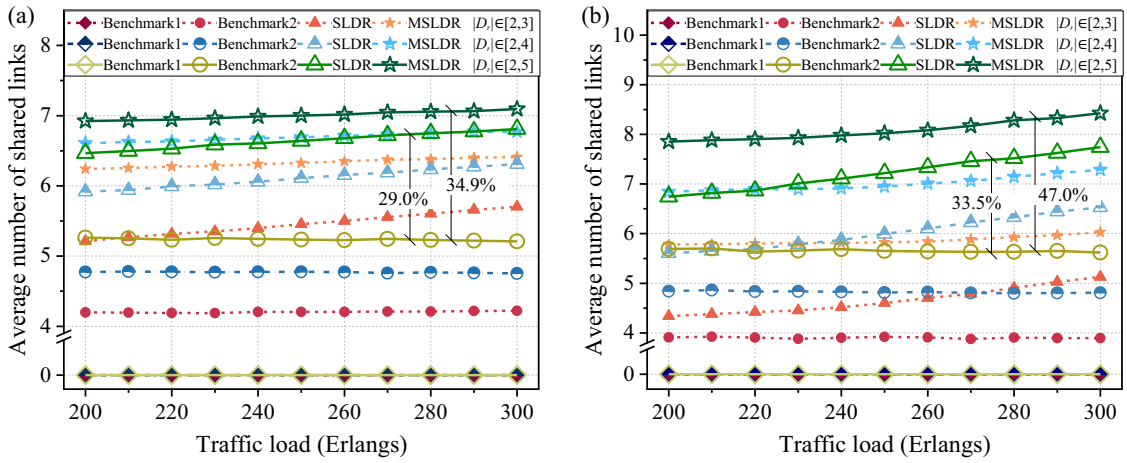


Fig. 9. Average number of shared links versus traffic load for different algorithms: (a) two-domain quantum network topology and (b) four-domain quantum network topology.

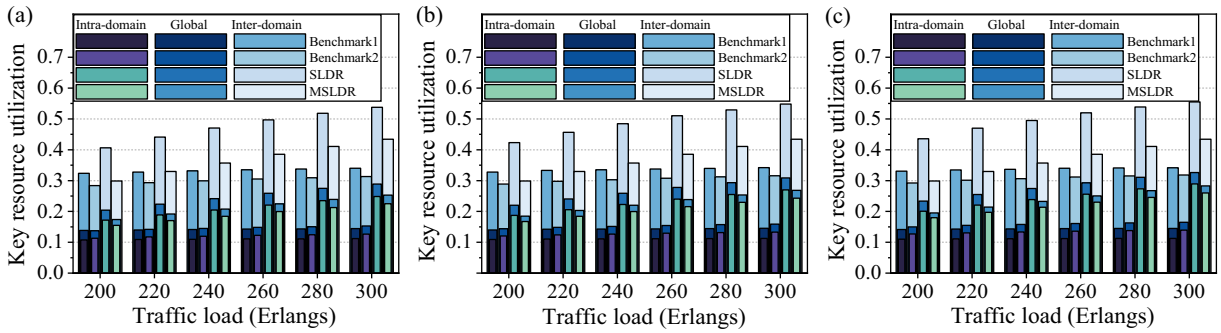


Fig. 10. Key resource utilization versus traffic load for different algorithms on the two-domain quantum network topology: (a) $|D_r| \in [2,3]$, (b) $|D_r| \in [2,4]$, and (c) $|D_r| \in [2,5]$.

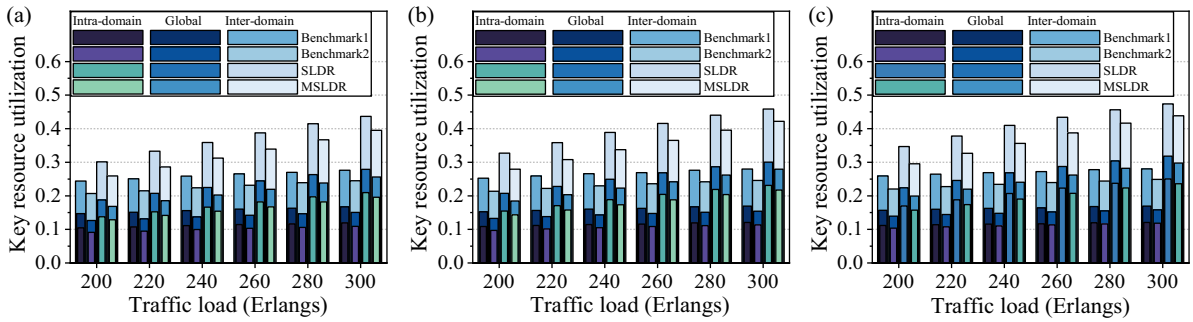


Fig. 11. Key resource utilization versus traffic load for different algorithms on the four-domain quantum network topology: (a) $|D_r| \in [2,3]$, (b) $|D_r| \in [2,4]$, and (c)$|D_r| \in [2,5]$.

5.3. Performance evaluation under different destination node distributions

In addition to the number of destination nodes, their spatial distribution can significantly affect multicast-oriented key provision performance. In this subsection, we consider three spatial distribution scenarios (i.e., centralized, uniform, and dispersive) on the four-domain quantum network topology, with the number of destination nodes chosen from [2, 4]. In the centralized scenario, all destination nodes reside within the same domain. The uniform scenario represents a random distribution of destination nodes across the multi-domain network (excluding the source domain). In the dispersive scenario, destination nodes are deliberately placed in different domains; specifically, for two destination nodes, each is located in a separate domain, while for three or more nodes, each domain (excluding the source domain) contains at least one destination node.

Figure 12 illustrates the success probability of multicast service requests versus traffic load for different algorithms under these distribution scenarios. Across all distributions, the performance ranking of the algorithms remains consistent with Subsection 5.2: MSLDR achieves the highest success probability, followed by SLDR, with both benchmark algorithms performing worse.

Further analysis indicates that a centralized distribution yields better performance than a uniform distribution, which in turn outperforms a dispersive distribution. This is because centralized placement maximizes sub-path aggregation, reducing the total number of QKD links involved and minimizing key consumption, thereby reserving more key resources for subsequent multicast services. Dispersive placement, however, requires more inter-domain QKD links and consumes additional key resources, while the uniform distribution achieves intermediate performance. Notably, due to the limited inter-domain links in the four-domain topology, the SLDR algorithm can effectively aggregate paths, resulting in success probabilities close to MSLDR across all three distributions and demonstrating strong adaptability in resource-aware routing.

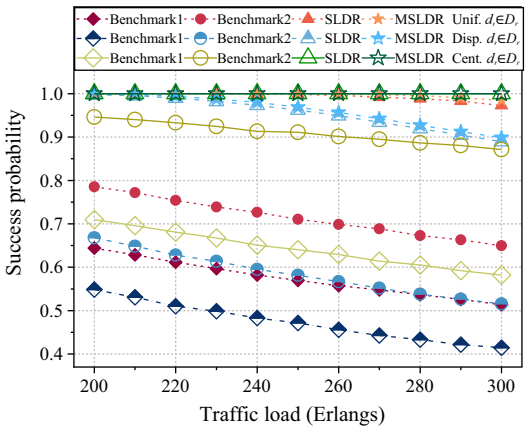


Fig. 12. Success probability of multicast service requests versus traffic load for different algorithms and destination node distributions on the four-domain quantum network topology.

Figure 13 illustrates the average number of shared links for multicast service requests as a function of traffic load across different algorithms and destination node distributions.

Consistent with the analysis in Subsection 5.2, the MSLDR algorithm achieves the highest number of shared links, followed by SLDR, Benchmark2, and Benchmark1, which exhibits zero shared links. For instance, in the dispersive distribution scenario at 280 Erlangs, the MSLDR and SLDR algorithms increase the number of shared links by 67.1% and 47.9%, respectively, compared to Benchmark2. The number of shared links in Benchmark2 remains nearly constant as traffic load increases, since it ignores the key resource distribution, resulting in dispersed sub-paths and limited aggregation. Notably, in both uniform and dispersive distributions, the shared links for MSLDR and SLDR gradually increase with traffic load, whereas in the centralized scenario, they remain almost unchanged. This is because all destination nodes reside within a single domain, and few inter-domain QKD links exist, leading to highly overlapping paths regardless of traffic load.

Figure 14 shows the key resource utilization versus traffic load for the same algorithms and destination node distributions. Consistent with the observations in Subsection 5.2, inter-domain key resource utilization is higher than global utilization, which is in turn higher than intra-domain utilization for all algorithms. Within the same distribution scenario, the SLDR algorithm consistently achieves higher utilization across global, inter-domain, and intra-domain resources compared to MSLDR. Comparing across distribution scenarios, in the uniform and dispersive cases, the utilization follows the order: SLDR, MSLDR, Benchmark1, and Benchmark2. However, in the centralized scenario, Benchmark1 exhibits the highest utilization, which deviates from the trend observed in other scenarios. This occurs because Benchmark1 does not employ key sharing, resulting in high key resource utilization while serving relatively few multicast services. This effect is amplified in the four-domain topology with centralized destination nodes, where the limited number of inter-domain QKD links and highly overlapping paths lead to constrained inter-domain communication and intensive key consumption.

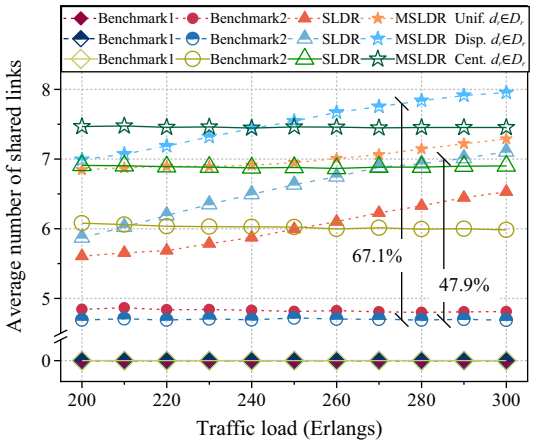


Fig. 13. Average number of shared links versus traffic load for different algorithms and destination node distributions on the four-domain quantum network topology.

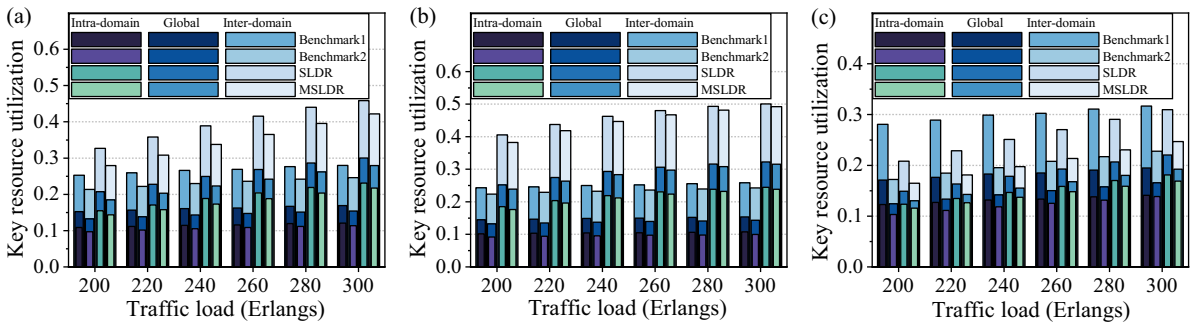


Fig. 14. Key resource utilization versus traffic load for different algorithms and destination node distributions on the four-domain quantum network topology: (a) uniform, (b) dispersive, and (c) centralized.

6. Conclusion

In this paper, we have proposed two key-resource-aware, multicast-oriented key provision strategies for hybrid DV/CV multi-domain quantum networks, employing the BB84 and GG02 protocols for inter- and intra-domain connections, respectively. We formulated a multicast-oriented key provision model and designed the SLDR and MSLDR algorithms to efficiently support multicast service key provisioning. Simulation results demonstrate that both algorithms consistently outperform benchmark methods across different multi-domain network topologies, highlighting their superior adaptability.

Due to the more restrictive key resource constraints on inter-domain links, the success probability of multicast service requests is particularly sensitive to the number of inter-domain QKD devices, underscoring the importance of their proper deployment. Compared with benchmark algorithms, both SLDR and MSLDR effectively accommodate varying numbers of destination nodes, achieving higher success probabilities while improving key resource utilization. Furthermore, the spatial distribution of destination nodes significantly affects network performance: a centralized layout enhances QKD link aggregation and key resource efficiency, whereas a dispersive layout increases inter-domain key resource consumption.

Overall, the MSLDR algorithm attains the highest success probability and the largest number of shared links, whereas

the SLDR algorithm achieves comparable performance with slightly higher key resource consumption. Both designed algorithms can adaptively manage key resources to support efficient multicast service establishment. Future work will investigate multi-domain quantum networks employing diverse QKD protocols, explore different types of cross-domain services, and develop strategies to balance network reliability with resource efficiency.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (Grant Nos. 62201276, 62350001, U22B2026, and 62425105), the Innovation Program for Quantum Science and Technology (Grant No. 2021ZD0300701), and the Key R&D Program (Industry Foresight and Key Core Technologies) of Jiangsu Province (Grant No. BE2022071).

References

[1] Cohen A, Cohen A, Médard M and Gurewitz O 2019 *IEEE Trans. Commun.* **67** 708
[2] Park C S 2020 *IEEE Internet Things J.* **7** 3441
[3] Skorin-Kapov N, Furdek M, Zsigmond S and Wosinska L 2016 *IEEE Commun. Mag.* **54** 110
[4] Cao Y, Zhao Y, Wang Q, Zhang J, Ng S X and Hanzo L 2022 *IEEE Commun. Surv. Tutor.* **24** 839
[5] Li Z, Xue K, Li J, Chen L, Li R, Wang Z, Yu N, Wei D S, Sun Q and Lu J 2023 *IEEE Commun. Surv. Tutor.* **25** 2133
[6] Li J, Wang M, Xue K, Li R, Yu N, Sun Q and Lu J 2022 *IEEE Trans. Commun.* **70** 6748
[7] Pan D, Long G L, Yin L, Sheng Y B, Ruan D, Ng S X, Lu J and Hanzo L 2024 *IEEE Commun. Surv. Tutor.* **26** 1898
[8] Pan D, Liu Y C, Niu P, Zhang H, Zhang F, Wang M, Song X T, Chen X, Zheng C and Long G L 2025 *Sci. Adv.* **11** eadt4627
[9] Chen T Y, Jiang X, Tang S B, Zhou L, Yuan X, Zhou H, Wang J, Liu Y, Chen L K, Liu W Y, Zhang Q, Chen Z B, Pan J W and Zhang J 2021 *npj Quantum Inf.* **7** 134
[10] Dynes J, Wonfor A, Tam W S, Sharpe A, Takahashi R, Lucamarini M, Plews A, Yuan Z, Dixon A, Lavieville J, Radig C, Kindness S, Penty R and Shields A 2019 *npj Quantum Inf.* **5** 101
[11] Lord A, Woodward R, Murai S, Sato H, Dynes J, Wright P, White C, Davey R, Wilkinson M, Penty R and Shields A 2023 *Proc. Opt. Fiber Commun. Conf.* (San Diego) pp. W4K.4
[12] Aguado A, Lopez V, Lopez D, Peev M, Poppe A, Pastor A, Folgueira J and Martin V 2019 *IEEE Commun. Mag.* **57** 20
[13] Huang D, Huang P, Li H, Wang T, Zhou Y and Zeng G 2016 *Opt. Lett.* **41** 3511
[14] 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 S, Jiang X, Wang J, Zhang T Y, Wang X B, Ma X F, Li H W, Zhang Q, Chen T Y and Pan J W 2016 *Phys. Rev. X* **6** 011024
[15] Wang S, Chen W, Yin Z Q, Li H W, He D Y, Li Y H, Zhou Z, Song X T, Li F Y, Wang D, Chen X F, Han Y G, Huang J Z, Guo J F, Hao P L, Li M, Zhang C M, Liu D, Liang W Y, Miao C H, Wu P, Guo G C and Han Z F 2014 *Opt. Express* **22** 21739
[16] Chen Y A, Zhang Q, Chen T Y, Cai W Q, Liao S K, Zhang J, Chen K, Yin J, Ren J G, Chen Z, Han S L, Yu Q, Liang K, Zhou F, Yuan X, Zhao M S, Wang T Y, Jiang X, Zhang L, Liu W Y, Li L, Liu N L, Xu B, Wang X B, Peng C Z and Pan J W 2021 *Nature* **589** 214
[17] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. Comput. Syst. Signal Process.* (Bangalore) p175
[18] Grosshans F and Grangier P 2002 *Phys. Rev. Lett.* **88** 057902
[19] Cao Y, Zhao Y, Zhang J and Wang Q 2022 *IEEE Commun. Mag.* **60** 38
[20] 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
[21] Wang T, Xu Y, Zhao H, Li L, Huang P and Zeng G 2023 *Opt. Lett.* **48** 719
[22] Cao Y, Zhao Y, Zhang J, Wang Q, Niyato D and Hanzo L 2022 *IEEE Netw.* **36** 14
[23] Guo M, Cao Y, Zhu J, Zhou X, Zhang C, Yu X, Zhao Y, Zhang J and Wang Q 2023 *J. Opt. Commun. Netw.* **15** 700
[24] Zhu J, Cao Y, Guo M, Zhou X, Zhang C, Li J, Yu X, Zhao Y, Zhang J and Wang Q 2024 *J. Opt. Commun. Netw.* **16** 735
[25] Cao Y, Yu X, Zhao Y, Zhang C, Zhou X, Zhang J and Wang Q 2025 *Chin. Phys. B* **34** 010310
[26] Martin V, Brito J P, Ortíz L, Méndez R, Buruaga J, Vicente R J, Sebastián-Lombraña A, Rincón D, Pérez F, Sánchez C, Martín J, Martín J C, Martín J M, Martín J L and Martín J A 2024 *npj Quantum Inf.* **10** 80
[27] Ren S, Wang Y and Su X 2022 *Sci. China Inf. Sci.* **65** 200502
[28] Zhang Y, Bian Y, Li Z, Yu S and Guo H 2024 *Appl. Phys. Rev.* **11** 011318
[29] Dong K, Zhao Y, Yang T, Li Y, Nag A, Yu X and Zhang J 2020 *J. Opt. Commun. Netw.* **12** 120
[30] Dong K, Zhao Y, Nag A, Yu X and Zhang J 2020 *Opt. Eng.* **59** 065102
[31] He X, Li L, Han D, Zhao Y, Nag A, Wang W, Wang H, Cao Y and Zhang J 2022 *J. Opt. Commun. Netw.* **14** 190
[32] Gottesman D, Lo H K, Lütkenhaus N and Preskill J 2004 *Quantum Inf. Comput.* **4** 325
[33] Ma X, Qi B, Zhao Y and Lo H K 2005 *Phys. Rev. A* **72** 012326
[34] Leverrier A, Grosshans F and Grangier P 2010 *Phys. Rev. A* **81** 062343
[35] 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
[36] Wang H, Pi Y, Huang W, Li Y, Shao Y, Yang J, Liu J, Zhang C, Zhang Y and Xu B 2020 *Opt. Express* **28** 32882