

A Segment-based Multipath Distribution Method in Partially-Trusted Relay Quantum Networks

Mingjun Wang, Jian Li, *Member, IEEE*, Kaiping Xue, *Senior Member, IEEE*, Ruidong Li, *Senior Member, IEEE*, Nenghai Yu, Yangyang Li, Yifeng Liu, Qibin Sun, *Fellow, IEEE*, Jun Lu

***Abstract*—As a promising application of quantum information technology, Quantum Key Distribution (QKD) can provide information-theoretically secure key exchange for adjacent communication parties. To achieve long-distance secure communication and scale expansion against inherent channel loss, trusted relays, which are assumed to be absolutely secure, are introduced into QKD networks. However, in practice, trusted relays may be compromised by attacks from ubiquitous eavesdroppers even protected by powerful hardware. Thus, how to ensure the security of end-to-end key distribution in partially-trusted relay QKD networks with the coexistence of trusted relays and untrusted relays becomes a challenging but urgent problem to be solved. To address this critical problem, in this article, we design a segment-based multipath key distribution method. The basic idea of the method is to maximize the security of the end-to-end key distribution through the segment-based multipath key distribution. Under the premise of security level requirements, we further propose a flexible key reconstruction scheme to improve the efficiency of key distribution and obtain available secret keys as many as possible. The extensive simulations are conducted and the results reveal that our method significantly outperforms the traditional multipath QKD method in terms of both security and efficiency.**

***Index Terms*—Quantum Key Distribution, Segment-based Multipath, Partially-Trusted Relay.**

I. Introduction

In the digital era, information security is always an essential and indispensable issue for various applications. Classical cryptography has been developed for decades to guarantee network communication security, and numerous cryptographic algorithms have been successfully applied. For example, Rivest-Shamir-Adleman (RSA), one of the most famous public-key encryption schemes, has been widely used in key agreement and authentication. However, since the security of most public-key ciphers is based on the difficulty of factoring integers or the discrete logarithm problem in mathematics, the upcoming quantum computers, which own exponentially increasing computational power, have posed a fatal threat to conventional cryptography by using quantum algorithms, such as Shor's algorithm [1], [2]. Therefore, it is necessary to find a powerful method to fight against the security problem caused by quantum computing.

M. Wang, J. Li, K. Xue, N. Yu, Q. Sun, J. Lu are with the School of Cyber Science and Technology, University of Science and Technology of China, Hefei, Anhui 230027, China.

R. Li is with the College of Science and Engineering, Kanazawa University, Kakuma, Kanazawa 920-1192, Japan.

Y. Li and Y. Liu are with the National Engineering Laboratory for Risk Perception and Prevention (NEL-RPP), CAEIT, Beijing 100041, China.

Corresponding Author: J. Li and K. Xue ({lijian9, kpxue}@ustc.edu.cn)

As a promising technology that provides anti-quantum computing security, Quantum Key Distribution (QKD) allows two communicating parties to share secure keys by sending and measuring quantum bits, i.e., qubits. The no-cloning theorem proves that an arbitrary unknown qubit cannot be cloned losslessly [3]. Thus, it is impossible for eavesdroppers to copy the qubits without being detected successfully, and guarantees information-theoretically secure key exchange. At present, qubits are usually achieved by photons and propagated through optical fibers or free space. There are 428 km, 509 km, 511 km, and 833 km QKD experiments in recent several years, there has been satellite to ground QKD using BB84, and BBM92 for free space QKD, and the integrated QKD network [4], [5].

Considering the inevitable photon loss and decoherence in quantum channels, trusted relay is a practical approach to extend the distance of QKD [6], [7]. Trusted relay works by using One-Time-Pad (OTP) technique to achieve end-to-end key distribution between two distant communication parties in a hop-by-hop manner. Due to its flexibility, simplicity, and scalability, trusted relay has been widely used in cutting-edge QKD networks and significantly facilitates the construction of long-haul trunk QKD [5], [8]. However, the security of key distribution process relies on the security assumption of trusted relays, i.e., eavesdroppers cannot compromise trusted relays. Unfortunately, some operations of trusted relays, including key storage, encryption, and decryption, are implemented in classical computers, which makes it possible for eavesdroppers to attack. Therefore, in the current QKD networks, the insecurity of some relay nodes must be considered, which is conducive to breaking the assumption that relays are completely trusted and further improving the security of the whole system. Hence, how to achieve end-to-end key distribution in the partially-trusted relay QKD networks becomes a critical and urgent problem to be solved.

To address the security problem caused by untrusted relays, most existing studies mainly consider Measurement-Device-Independent (MDI) QKD [9] and multipath key distribution method [10], [11]. The former can expand the distribution distance and close all detection loopholes with the aid of a measurement node that can even be untrusted. However, its requirement for the location of the measurement node makes it unable to solve the situation that two untrusted relays are adjacent and limit its application. The latter can effectively improve security by simultaneously distributing secret keys through multiple disjoint paths with the help of secret sharing. Unfortunately, some drawbacks of the existing multipath key distribution method still hinder its practical

applications: First, in practical network topologies, the number of disjoint paths required by the multipath key distribution method is limited. Second, for a partially-trusted relay QKD network, the existing multipath key distribution method can hardly utilize the location information of trusted relays for routing to further improve the security of end-to-end key distribution. Besides, considering that different fields including military, financial, and government have different security level requirements for secret keys, a dynamic secret sharing scheme is further required to achieve flexible key reconstruction.

To correspond to the above drawbacks and achieve secure and efficient key distribution in the partially-trusted relay QKD networks, in this article, we analyze the influence of different paths on the security of key distribution by using a probability model and then propose a novel segment-based multipath key distribution method that utilizes the location information of trusted relays to maximize the security of the end-to-end key distribution. After that, we further propose a flexible key reconstruction scheme, which can adjust the key reconstruction process to achieve higher distribution efficiency under the premise of meeting various security level requirements. The main contributions of our work are summarized as follows:

- To tackle the security problem in the partially-trusted relay QKD networks, we propose a segment-based multipath key distribution method, which can fully utilize the location information of trusted relays and achieve as high security as possible in the process of end-to-end key distribution. It overcomes the drawbacks of the existing schemes.
- Considering the diverse security requirements of applications, we further propose a flexible key reconstruction scheme. Based on the successfully distributed secret keys on the paths of each segment, this post-processing procedure can significantly improve the efficiency of key distribution between arbitrary communicating parties under the premise of meeting various security level requirements.
- To evaluate the performance of the proposed key distribution method, we conduct extensive simulations in different scenarios. Results show that the proposed method significantly outperforms the traditional multipath method for security and efficiency.

The rest of this article is organized as follows: Section II introduces the background, network model, and security problem considered in this article. After that, Section III describes the specific details of the segment-based multipath method. We conduct simulations and analyze the results in Section IV. Finally, we conclude this work and envision future directions in Section V.

II. Background And Problem Statement

A. Background

Currently, various QKD protocols have been proposed and demonstrated experimentally, including Bennett-Brassard-1984 (BB84), Ekert-91 (E91), and Measurement-Device-Independent QKD (MDI-QKD) [12], etc. Here, we take the prepare-and-measure protocol BB84 as an example to clarify the specific implementation procedure of QKD and further introduce the working process of long-distance key distribution and multipath key distribution.

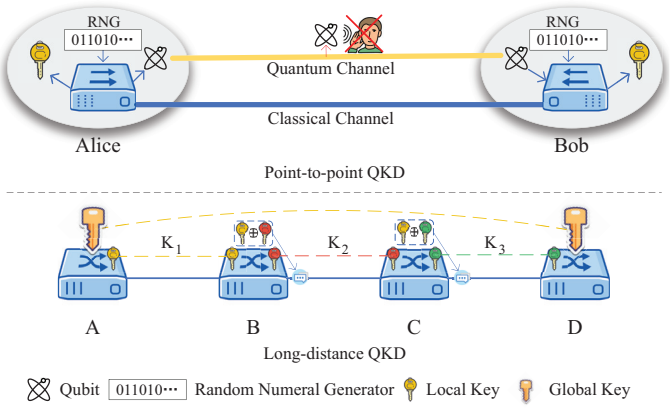

Fig. 1. The illustration of point-to-point QKD and long-distance QKD.

1) Point-to-point QKD: As shown in Fig. 1, Alice and Bob are two communicating parties who want to share secret keys, and they are connected by a quantum channel and a classical channel. Alice sends qubits to Bob, and each qubit is determined by two random classical bits, one for the encoding basis and another for the bit (0 or 1) to send. Bob receives and measures the qubits with random bases and tells Alice which qubits he received. Then, they exchange the bases they chose via a classical channel and only keep the measurement results of the same bases in the sifting. Part of the reserved bits are used for eavesdropping detection, and the remaining part will become the shared keys after error correction and privacy amplification.

2) Long-distance QKD: Long-distance QKD can be achieved in a hop-by-hop manner to break the distance limitation by deploying relays between two distant nodes [13]. As shown in Fig. 1, node A takes K_1 as the secret key; node B encrypts K_1 with K_2, i.e., $E_{K_2}(K_1)$ and sends it to node C; node C decrypts and sends it to node D in the same way. Finally, node D gets K_1. At this time, a global key K_1 is shared between node A and node D.

3) Multipath QKD: In the partially-trusted relay QKD networks, distributing global keys through one path may lead to key leakage under the attack of eavesdroppers. As shown in Fig. 2, node A and node E distribute keys through two disjoint paths and get two keys. Then they obtain a final global key through XOR reconstruction. Unless the keys on all paths are obtained by the eavesdropper, the global key is secure.

B. Network Model

In this article, as shown in Fig. 2, we consider a partially-trusted relay QKD network in which only several core relays are fully trusted as they are protected at an unrestricted cost. A centralized key management server exists in the network to obtain network information and control the key distribution. In addition to the necessary quantum devices, a quantum node needs a classical information processing unit to decrypt and encrypt classical information and a Quantum Key Pool (QKP) to manage local keys exchanged with adjacent nodes.

To highlight the security problem in the partially-trusted relay QKD networks, in the following, we give the definition of two kinds of relays in the network and introduce the adversary model considered in this article.

1) Trusted/Untrusted Relay: The relay nodes in the network are classified into trusted relays and untrusted relays. Trusted relays have extremely high-security measures to avoid attacks from eavesdroppers. They avoid illegal network access by deploying firewalls, avoid access to sensitive resources through access control mechanisms such as memory encryption, and are deployed in a protected environment. Untrusted relays have low-security insurance, which makes them possible to be eavesdropped on successfully.

2) Adversary Model: Since secret keys are transformed from ciphertext into plaintext on each relay during the end-to-end key distribution process, eavesdroppers pay more attention to compromising the relays. Each untrusted relay has a security probability to indicate that it has not been successfully attacked. The eavesdropper can arbitrarily select relay nodes to attack, but it can only obtain the key information of the successfully attacked relay. For an end-to-end key distribution, the key information will only be transmitted once on each relay node. Similarly, we adopt a probability model to evaluate the security of end-to-end key distribution. For single-path key distribution, the security probability of key is the probability that all relay nodes on the path successfully resist eavesdropping. For multipath key distribution, the security probability is the probability that at least one path is secure.

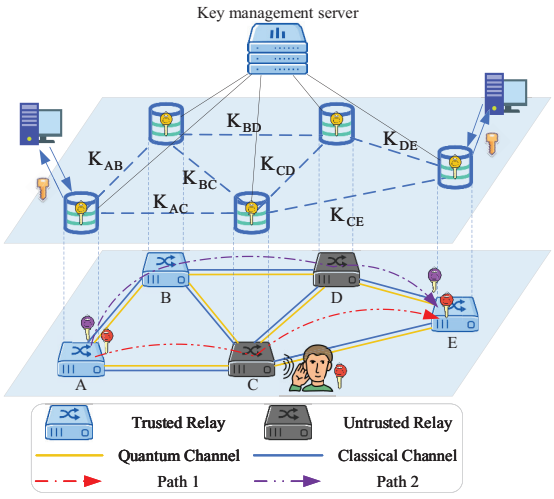

Fig. 2. A typical structure of a partially-trusted relay QKD network. In order to ensure the security of the global key, two paths are used for key distribution. The final key is reconstructed from the keys distributed by the two paths.

C. Problem Statement

Currently, many QKD networks have been deployed and used in business, and they are mainly based on the trusted relay technique. The insecurity of partial relay nodes in large-scale networks cannot be ignored. Meanwhile, the consideration of untrusted relays can break the assumption that relay nodes must be completely trusted and improve the security of the whole network. Therefore, the problem of secure key distribution must be solved in the partially-trusted relay QKD networks.

As an effective solution to protect the security of the key distribution process in the partially-trusted relay QKD networks, there are some existing studies that focus on multipath QKD in quantum networks with untrusted relays. Their security analysis of the process of key distribution can be divided into two categories: network connectivity [10] and probabilistic [11], [14]. The former usually proposes a scheme that can tolerate a certain number of compromised nodes for secure transmissions. The latter usually analyze the security of the key distribution according to the security probability of the untrusted relays and the paths for key distribution. However, these studies, on the one hand, neglect the impact of key distribution path selection but pay more attention to the number of paths. On the other hand, they ignore users' various security requirements. Hence, in the next section, to improve the security of key distribution and balance the security and efficiency of key distribution, we design a segment-based multipath key distribution method and a flexible key reconstruction scheme.

III. Segment-based Multipath Key Distribution

A. Overview

As a secret key distribution platform, QKD networks supply quantum keys for various fields, e.g., military, finance, and government. To address the potential threats of eavesdropping on immediate relays in the partially-trusted relay QKD networks, we design a novel segment-based multipath key distribution method. Different from the traditional multipath distribution scheme, the proposed method splits the end-to-end distribution process into segments, improving the security of key distribution. In addition, considering various requests in QKD networks have different security requirements for keys, we propose a flexible key reconstruction scheme to adjust the security and efficiency in the end-to-end key distribution. The overall workflow of the method is shown in Fig. 3.

B. Segment-based Key Distribution Method

In the segment-based multipath key distribution, the distribution process is divided into two stages, i.e., key distribution within segment and end-to-end distribution. The specific illustration is shown in Fig. 4. After receiving a request, the centralized server determines the routing paths and key reconstruction strategy according to the network status and security requirement, and then sends results to relays in the network. After that, the key distribution within the segment is performed, and each corresponding path is used for key distribution. The obtained keys are shared by the trusted relay nodes at both ends of the segment, and then they are reconstructed into new keys as required. Next, these physically non-adjacent but logically adjacent trusted relays share the reconstruction keys with each other and use these keys to achieve the end-to-end key distribution in a hop-by-hop manner. The security probability of the end-to-end global key is the product of the security probabilities of reconstructed keys on each segment.

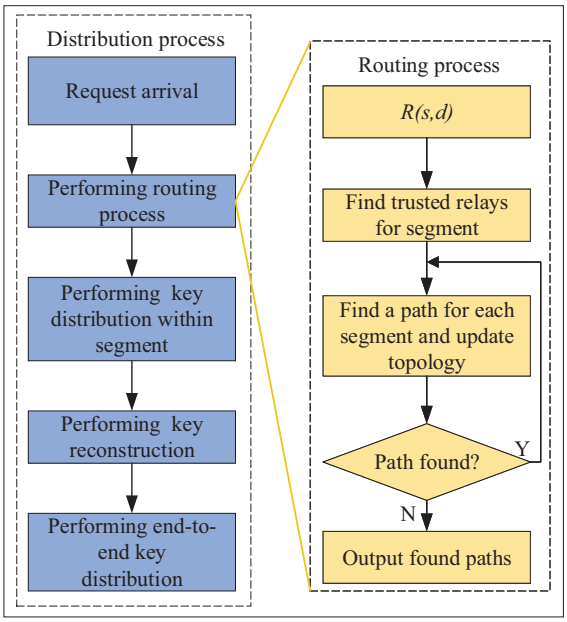

Fig. 3. The process of end-to-end distribution and segment-based multipath routing algorithm.

Under the same distribution paths, the segment-based distribution method can improve the security of the final global keys more than the non-segmented distribution method. The basic idea is that when a relay node is eavesdropped successfully, compared with the non-segmented multipath distribution, only the key on the segmented path where the relay node is located will be leaked, rather than the key on the whole path from the source node to the destination node.

Finding appropriate segmented paths is indispensable in the network. Various routing algorithms proposed for classical networks cannot be directly applied to the partially-trusted relay QKD networks because they do not consider the security of key distribution. Consumption of local keys for long-distance QKD increases with the increase of hops, which makes it necessary for routing to consider resource consumption. Besides, we can make full use of the location information of trusted relays to find more secure paths in the partially-trusted relay QKD networks.

To find more resource-saving and secure paths, we define the expected security probability E_{sp} as the routing metric to quantify a path, it equals the product of the security probability of each relay on the path. A larger value not only means that the path is safer but also usually means that the path is shorter. The classical Dijkstra algorithm can find the shortest path because the routing metric is additive, which means that the cost of the path is the sum of the costs of all edges on the path. However, our metric is multiplicative and monotonically decreasing. For the non-additive but monotonic routing metric E_{sp}, we apply it to the classical Dijkstra algorithm and call it ExDijkstra to find the path between source and destination with the maximum evaluation value.

In the previous work, the paths for multipath key distribution are usually node-disjoint (i.e., one relay can only be used in one path) to ensure an untrusted relay can only get one key. However, this strategy not only finds limited paths but also finds more scattered and long paths, which wastes more local keys and increases the risk of key leakage. Thus, we not only use the trusted relays to segment the paths but also allow multiple paths crossing on trusted relay to reduce the average length of paths.

We propose a heuristic Segment-based Multipath Routing (SMR) algorithm to find appropriate paths for maximizing the security of key distribution. The steps shown in Fig. 3 are described as follows:

1) Find trusted relays for segment: SMR finds the segment nodes between the source node s and the destination node d through an iterative process. In the beginning, the segment node set is empty. Each time, the classical Dijkstra is used to find the trusted relay node r with the minimum sum of the distances s and d, and then the ExDijkstra is used to find two non-segmented paths from s to d and two segmented paths from s to r and r to d. Judge whether the security probability of segment-based distribution is greater than that of non-segmented distribution. If yes, add r to the segment node set and set r as new s to continue the iterative process, otherwise, the iterative process will end.
2) Find segment-based multiple paths: Based on the segment node set in the previous step, each time, ExDijkstra is used to find a path for each segment, the found paths will be deleted on the topology. The algorithm stops when no more paths can be found.

C. Flexible Key Reconstruction

In the existing multipath schemes, the keys distributed on different paths are reconstructed into a global key via XOR operation. In this case, the security of the key is undoubtedly the strongest, but the security gain brought by the increase in the number of paths has a marginal utility. Besides, considering that different requests have different requirements for the security of the key, we propose a flexible key reconstruction scheme, which can offer a dynamic reconstruction process. The basic idea is adjusting the number of keys consumed by the reconstruction on the premise of meeting the requirements of the security to improve the efficiency of end-to-end key distribution.

In the partially-trusted relay QKD networks, a key request includes source node, destination node, and key security level requirement ε represented by security probability. SMR will find multiple paths that cross over trusted relays between source node and destination node. These paths are divided into multiple segments by some trusted relays, and each path of each segment performs key distribution respectively before key reconstruction.

Before actual end-to-end distribution, we need to decide how to match the reconstructed keys between segments and how to achieve the key reconstruction on each segment. The reconstructed keys on each segment have different security probabilities, in order to make as many global keys as possible meet the security level, we use a balanced matching strategy to improve the minimum security probability of global keys. The

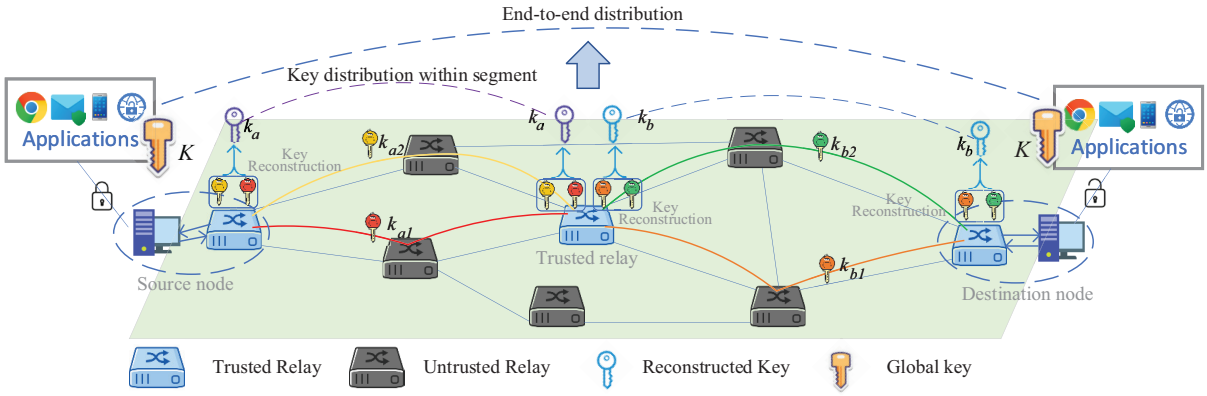

Fig. 4. The illustration of the segment-based multipath key distribution method, two segments reconstruct keys respectively and then distribute the global key in a hop-by-hop manner.

reconstructed key with the highest security probability in the previous segment will match the key with the lowest security probability in the subsequent segment; the second high will match the second low, and so on. After each match, the new security probability of the key will be calculated, which is equal to the product of the security probabilities of the two matching keys. Finally, we can get the security probability of the global key.

For the key reconstruction, we hope to increase the number of reconstructed keys of each segment to improve the distribution efficiency under the premise of meeting security. The steps of key reconstruction for the keys of each segment are as follows: 1) First, we maintain a priority queue, put all keys in the queue, and take the security probability of the key as the priority. 2) In each round, we take out the two keys with the lowest security probability, reconstruct them into a new key, and put the reconstructed key with a new security probability into the queue. The loop will not be terminated until the global key with the lowest security probability meets the security requirements and the number of reconstructed keys on different segments reaches the same.

In the reconstruction above, each key is used only once. We propose a key reuse strategy to further increase the reconstructed key through combination and combinations that do not meet security requirements will be discarded. It is worth noting that because XOR operation is additive, the reconstructed keys under the key reuse strategy will disclose each other's information. Therefore, a nonlinear function such as cryptographic hash should be used as a reconstruction function, connecting several keys as input and outputting as reconstruction key.

IV. Performance Evaluation

A. Simulation Setup

To verify the performance of the SMR algorithm, we use numerical simulation compare it with the existing Multiple Stochastic Paths (MSP) algorithm [11] in various scenarios. Considering the scale of the existing network and the simulation cost [5], we use the Waxman-Salama model to build a random topology and set the network size to 100 nodes. To make the results more reliable, we give the average value of 1000 simulations and randomly select the location of the request and trusted relays in each simulation. The amount of keys in the key pool is set to 100kb, which is also close to the amount of key generation per second in the existing network backbone. Without loss of generality, we assume that the security probability of each untrusted relay node is consistent. In the following, we evaluate and discuss the impacts of different trusted relay numbers and different untrusted relay security probabilities on the security, resource consumption, and distribution efficiency in the process of key distribution. We use end-to-end security probability to describe the average security probability of the key. The key consumption rate represents the ratio of the number of keys consumed in the distribution process to the total number of keys. The key length represents the length of the distributed end-to-end key.

B. Different Security Probability of Untrusted Relays

Simulations about the impacts of the security probability of untrusted relay nodes on the security, key consumption, and efficiency of key distribution are conducted first. As shown in Fig. 5(a), the end-to-end security probability increases with the increase of the security probability of untrusted relays, and SMR always achieves a higher value than the comparison object. At the same time, in terms of resource consumption, because our proposed routing algorithm can find more secure and shorter paths, SMR always consumes fewer keys. We set the security level requirements of key requests to 0.5, 0.7, and 0.9, respectively, and apply the proposed key reconstruction scheme to different routing algorithms. As shown in Fig. 5(b), as the security probability of untrusted relays increases, the length of key will also increase. However, SMR can always get a longer key.

C. Different Number of Trusted Relays

Then we simulate the impact of the number of different trusted relay nodes. As shown in Fig. 6(a), with the increase in the number of trusted relay nodes, the end-to-end security probability is also rising. However, SMR can still achieve considerable security advantages. In terms of resource consumption, because our proposed routing algorithm makes full

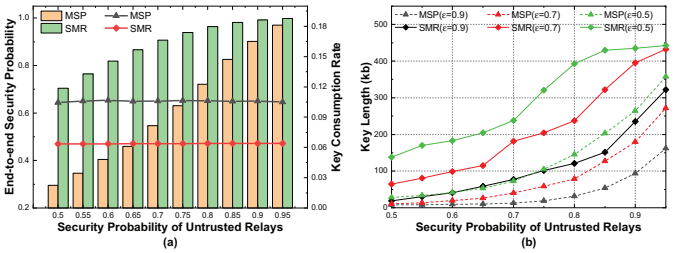

Fig. 5. The impact of different security probabilities of untrusted relay nodes: a) End-to-end security probability and key consumption rate; b) Length of the global key. The number of trusted relay nodes is set to 10.

use of trusted relay nodes, more paths can be found with the increase in the number of trusted relays, which consumes more resources and obtains a higher security rate. As shown in Fig. 6(b), with the increase in the number of trusted relay nodes, the key length under different security levels also increases. At the same time, SMR can still obtain the advantage of key length and have a more obvious improvement.

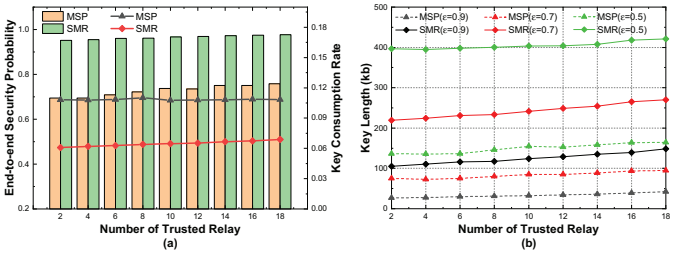

Fig. 6. The impact of different number of trusted relay nodes: a) End-to-end security probability and key consumption rate; b) Length of the global key. The security probability of untrusted relay nodes is set to 0.8.

V. Conclusions and Future Directions

In this article, we studied the potential eavesdropping attacks on immediate relays existing in the partially-trusted relay QKD networks and analyzed the impact of key distribution paths on the security of the end-to-end key distribution process. To overcome the drawbacks of the existing work and address this security problem, we designed a segment-based multipath key distribution method by utilizing the location information of trusted relays to maximize the security of the key distribution process. In addition, we further proposed a flexible key reconstruction scheme to reconstruct secret keys for numerous demands while still satisfying users' diverse security level requirements, and thus the efficiency of key distribution can be further enhanced. Extensive simulations have been conducted, and the results show that the proposed method significantly outperforms the traditional multipath key distribution method in terms of security, resource consumption, and distribution efficiency. In the future, we plan to further investigate the impact of the number and the location of trusted relays in the network and provide an optimized trusted relay deployment strategy.

With the continuous development of quantum information technology, the quantum Internet will eventually be established and support quantum computers and quantum communication [15]. As a significant application in quantum Internet, QKD provides unconditionally secure keys for classical networks. However, attacks against relay nodes emerge endlessly, which greatly affects the security of long-distance QKD. The results show that our method can effectively improve the security of key distribution, which provides assistance for building the future large-scale quantum network.

Acknowledgments

This work is supported in part by Anhui Initiative in Quantum Information Technologies under grant No. AHY150300, National Scientific and Technological Innovation 2030 Major Project of Quantum Communications and Quantum Computers under grant No. 2021ZD0301301, and Youth Innovation Promotion Association of CAS under grant No. Y202093.

References

[1] F. Arute, K. Arya, R. Babbush, D. Bacon *et al.*, "Quantum supremacy using a programmable superconducting processor," *Nature*, vol. 574, no. 7779, pp. 505–510, 2019.

[2] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *Society for Industrial and Applied Mathematics review*, vol. 41, no. 2, pp. 303–332, 1999.

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

[4] S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. Fan-Yuan, F.-X. Wang, Y.-G. Zhu *et al.*, "Twin-field quantum key distribution over 830-km fibre," *Nature Photonics*, vol. 16, no. 2, pp. 154–161, 2022.

[5] Y.-A. Chen, Q. Zhang, T.-Y. Chen, W.-Q. Cai *et al.*, "An integrated space-to-ground quantum communication network over 4,600 kilometres," *Nature*, vol. 589, no. 7841, pp. 214–219, 2021.

[6] P. Sibson, C. Erven, M. Godfrey, S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, H. Terai, M. G. Tanner, C. M. Natarajan *et al.*, "Chip-based quantum key distribution," *Nature communications*, vol. 8, no. 1, pp. 1–6, 2017.

[7] D. Ribezzo, M. Zahidy, I. Vagniluca, N. Biagi, S. Francesconi, T. Occhipinti, L. K. Oxenløwe, M. Lončarić, I. Cvitić, M. Stipčević *et al.*, "Deploying an inter-european quantum network," *Advanced Quantum Technologies*, p. 2200061, 2022.

[8] M. Mehic, M. Niemiec, S. Rass, J. Ma *et al.*, "Quantum key distribution: A networking perspective," *ACM Computing Surveys*, vol. 53, no. 5, p. 41, 2020.

[9] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Physical review letters*, vol. 108, no. 13, p. 130503, 2012.

[10] H. Zhou, K. Lv, L. Huang, and X. Ma, "Quantum network: Security assessment and key management," *IEEE/ACM Transactions on Networking*, vol. 30, no. 3, pp. 1328–1339, 2022.

[11] H. Wen, Z. Han, Y. Zhao, G. Guo *et al.*, "Multiple stochastic paths scheme on partially-trusted relay quantum key distribution network," *Science in China Series F: Information Sciences*, vol. 52, no. 1, pp. 18–22, 2009.

[12] P. Sharma, A. Agrawal, V. Bhatia, S. Prakash *et al.*, "Quantum key distribution secured optical networks: A survey," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 2049–2083, 2021.

[13] Q. Zhang, F. Xu, Y.-A. Chen, C.-Z. Peng *et al.*, "Large scale quantum key distribution: challenges and solutions," *Optics Express*, vol. 26, no. 18, pp. 24 260–24 273, 2018.

[14] T. R. Beals and B. C. Sanders, "Distributed relay protocol for probabilistic information-theoretic security in a randomly-compromised network," in *International Conference on Information Theoretic Security*. Springer, 2008, pp. 29–39.

[15] L. Gyongyosi and S. Imre, "Advances in the quantum internet," *Communications of the ACM*, vol. 65, no. 8, pp. 52–63, 2022.

MINGJUN WANG (wmj0113@mail.ustc.edu.cn) received the bachelor's degree from the Department of Information Security, University of Science and Technology of China (USTC), in 2019. He is currently a Graduate Student with the School of Cyber Science and Technology, USTC. His research interests include quantum internet architecture and quantum networking.

JIAN LI [M'20] (lijian9@ustc.edu.cn) received his bachelor's degree from the Department of Electronics and Information Engineering, Anhui University, in 2015, and received his Ph.D degree from the Department of Electronic Engineering and Information Science (EEIS), University of Science and Technology of China (USTC), in 2020. He is currently a Post-Doctoral fellow with the School of Cyber Science and Technology, USTC. His research interests include future Internet architecture design and quantum networking.

KAIPING XUE [M'09-SM'15] (kpxue@ustc.edu.cn) received his bachelor's degree from the Department of Information Security, University of Science and Technology of China (USTC), in 2003 and received his Ph.D. degree from the Department of Electronic Engineering and Information Science (EEIS), USTC, in 2007. Currently, he is a Professor in the School of Cyber Science and Technology, USTC. His research interests include future Internet architecture design, transmission optimization, and network security.

RRUIDONG LI [SM'07] (lrd@se.kanazawa-u.ac.jp) received his bachelor's degree in engineering from Zhejiang University, China, in 2001, and received his Ph.D degree from the University of Tsukuba in 2008. Currently, he is an associate professor in College of Science and Engineering, Kanazawa University, Japan. His research interests include big data networking, information-centric network, network security, and quantum Internet.

NENGHAI YU (ynh@ustc.edu.cn) received his bachelor's degree from Nanjing University of Posts and Telecommunications, Nanjing, China, in 1987, the M.E. degree from Tsinghua University, Beijing, China, in 1992, and his Ph.D. degree from the Department of Electronic Engineering and Information Science (EEIS), University of Science and Technology of China (USTC), Hefei, China, in 2004. Currently, he is a Professor in the School of Cyber Science and Technology, USTC. His research interests include multimedia security and quantum networking.

YANGYANG LI (liyangyang@cetc.com.cn) received the B.S. degree from Nanjing University of Information Science and Technology, Nanjing, China, in 2009, and the Ph.D. degree in computer science from Beijing University of Posts and Telecommunications, Beijing, China, in 2015. He is currently a Senior Engineer with the National Engineering Laboratory for Risk Perception and Prevention (NEL-RPP), Beijing. His research interests include data science, social network, and network security.

YIFENG LIU (liuyufeng3@cetc.com.cn) is currently a senior engineer in the National Engineering Laboratory for Risk Perception and Prevention (NEL-RPP), CAEIT, Beijing, China. His research interests include data science, social network, and network security.

QIBIN SUN (F'11) (qibinsun@ustc.edu.cn) received the Ph.D. degree from the Department of Electronic Engineering and Information Science (EEIS), University of Science and Technology of China (USTC), in 1997. He is currently a professor in the School of Cyber Science and Technology, USTC. His research interests include multimedia security, network intelligence and security and so on. He has published more than 120 papers in international journals and conferences. He is a fellow of the IEEE.

JUN LU (lujun2019@ustc.edu.cn) received his bachelor's degree from Southeast University in 1985 and his master's degree from the Department of Electronic Engineering and Information Science (EEIS), University of Science and Technology of China (USTC), in 1988. He is currently a professor in the School of Cyber Security and Technology and the Department of EEIS, USTC. His research interests include theoretical research and system development in the field of integrated electronic information systems. He is an Academician of the Chinese Academy of Engineering (CAE).