A Multi-Path QKD Algorithm with Multiple Segments

Cheng Liu, Xuanxuan Che, Jianshe Xie
and Yumin Dong*

College of Computer and Information Science, Chongqing Normal University, Chongqing, 401331, China
E-mail: dym@cqnu.edu.cn
**Corresponding Author*

Received 15 July 2023; Accepted 25 September 2023;
Publication 13 February 2024

Abstract

Quantum Key Distribution (QKD) provides unconditional peer-to-peer security based on the principles of quantum physics. By utilizing relay nodes, the security of QKD can be extended over longer distances. However, the introduction of relay nodes brings both security and communication success rates issues. To tackle those issues we propose an enhanced multi-path scheme. The key features of our proposal are as follows: 1. By taking the reliability of relay nodes as one of the algorithm inputs,making the scheme more suitable for partially trusted QKD (PTQKD) networks. 2. By using Multi-Segment Multi-Path approach increases the difficulty for attackers to obtain complete key information and improves the security of PTQKD. 3. The adaptive routing algorithm generates a sufficient number of diverse paths based on node contribution rate, key freshness, and reliability. We conducted

Journal of Cyber Security and Mobility, Vol. 13_2, 193–214.
doi: 10.13052/jcsm2245-1439.1321

a theoretical analysis of the algorithm,and simulation results on PTQKD demonstrate that our method outperforms traditional QKD methods in terms of security and transmission success rate. This advancement has the potential to enhance the adoption of QKD networks.

Keywords: QKD network, QKD security, segment based routing, multi-path routing.

1 Related Background

1.1 General Security System

When a secure system is designed for the transmission of data information, its main purpose is to ensure that even if an attacker steals the encrypted data, they cannot decipher the useful original information. In 1976, Shannon proposed a general model for secure systems [20], as shown in Figure 1. In this model, the sender includes two sources: the message source and the key source. The key source generates specific keys and transmits them to the receiver through a secure channel (referred to as a courier). The message source generates the data information (plaintext) to be transmitted, which is converted into ciphertext using the key through an encryption algorithm. The ciphertext is then sent to the receiver through an insecure channel, such as radio waves. The receiver uses the same key to decrypt the ciphertext back into plaintext. Even if an attacker intercepts the ciphertext on the insecure channel, they cannot recover the plaintext from it because they do not have the decryption key. Therefore, the security of the key is crucial for cryptographic systems. Consequently, securely distributing keys between the sender and receiver has become a focus of research in cryptography.

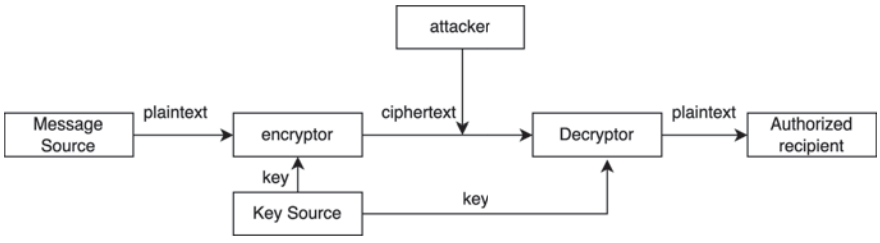


Figure 1 Schematic diagram of a general security system.

1.2 Quantum Key Distribution Technology

The first quantum key distribution (QKD) protocol, known as the BB84 protocol [1], was proposed by Bennett and Brassard in 1984. The security of this protocol relies on the Heisenberg uncertainty principle and the no-cloning principle. In 1989, the protocol was successfully implemented in an experiment, achieving a communication distance of 32 km [3]. Subsequently, in 1991, A. Ekert proposed the first entanglement-based QKD protocol, known as the E91 protocol [15]. Additionally, in 1992, Bennett introduced the B92 protocol, which is a two-state protocol. In 2000, Bennett and colleagues discovered the vulnerability of QKD protocols using weak coherent light sources to photon number splitting attacks [2]. To address this issue, in 2003, Wong-Yong Hwang proposed a decoy-state protocol that can withstand photon number splitting attacks [4]. Furthermore, in 2005, Professor Wang Xiangbin from China discussed the security and optimal secure key generation rate of QKD protocols based on decoy states [10]. In 2006, Pan Jianwei's group in China successfully conducted a quantum communication experiment based on decoy states, achieving a transmission distance of 100 km [23]. In the same year, a similar experiment was conducted in the United States, achieving a communication distance of up to 107 km [17]. In 2002, Grangier et al. proposed the GG02 protocol based on continuous variables, which has been proven to be information-theoretically secure [18]. In 2012, the measurement-device-independent (MDI) QKD protocol was first proposed, offering practicality and immunity to attacks on all detectors [9]. In 2014, the round-robin differential phase shift (RRDPS) QKD protocol was introduced, and its security was demonstrated without relying on detecting channel disturbances [5, 11–13, 21]. In 2015, Wang Xiangbin and colleagues from China proposed a measurement-device-independent QKD protocol based on four different intensities of decoy states [25]. Currently, QKD protocols are primarily categorized into three types based on the physical resources used: single-photon-based, entanglement-based, and continuous-variable-based protocols [14], as shown in Figure 2.

Figure 3 shows a QKD link using the one-time pad (OTP) encryption protocol. Between Alice and Bob, a sufficiently long symmetric encryption key is established through quantum entanglement mechanisms. Then, at the source, the message is encrypted by performing bitwise XOR operations with the shared key, ensuring secure transmission from Alice to Bob. The encrypted information is then transmitted through a classical channel. Upon receiving the encrypted message, Bob securely decrypts it by performing

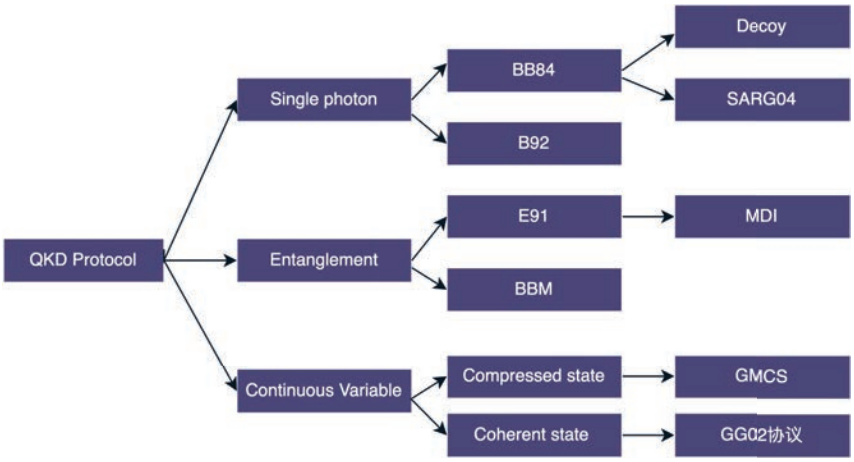


Figure 2 QKD main protocol types.

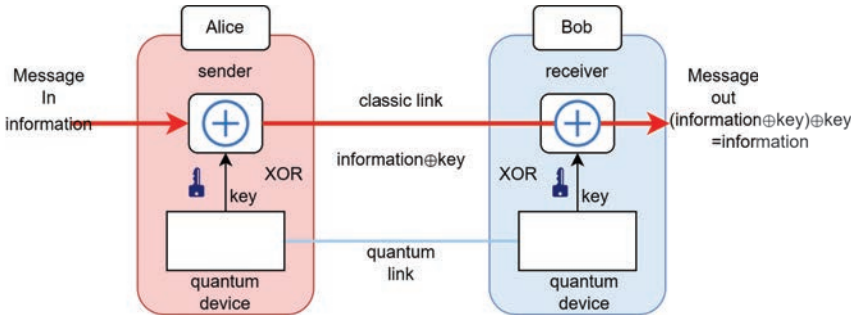


Figure 3 Schematic diagram of a point-to-point QKD link.

XOR operations. While basic QKD schemes have excellent security properties, they are limited by strict distance constraints and require the use of quantum relays for remote communication through entanglement swapping mechanisms [14]. Eavesdroppers may attempt to intercept information transmitted through traditional channels. Unfortunately, due to the challenges in creating short-term quantum memories, quantum relays have so far been unable to be constructed in a scalable and cost-effective manner. Therefore, current QKD networks employ a combination of quantum and classical links for key distribution. This approach has the advantage of providing the inherent security advantages of QKD, under the assumption that all relay nodes are completely reliable. We refer to this type of network as a trusted relay network.

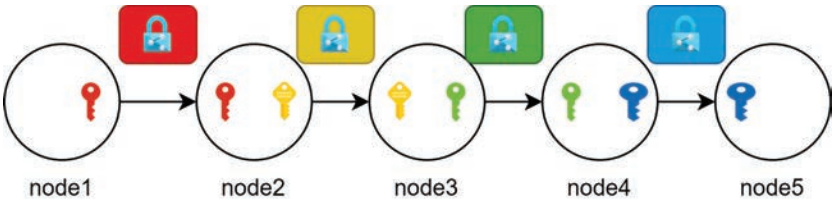


Figure 4 Schematic diagram of multi-node QKD link relay.

Table 1 The probability distributions of r for different periods of n Probability

Networks	Nodes	Relay Type
DARPA Quantum Network [8]	10	trusted relay
SECOQC Quantum Network [16]	6	trusted relay
Tokyo Quantum Network [19]	6	trusted relay
Space-Ground Quantum Network [7, 19]	32	trusted relay

Such trusted relay networks greatly expand the scope of quantum cryptography and reduce the cost of large-scale interconnection. Table 1 shows the current status of operational QKD networks, while Figure 4 illustrates the workflow of a QKD network with multiple relay nodes. Each data packet is encrypted and decrypted sequentially by trusted nodes at each intermediate hop along its path. The messages transmitted over each link are encrypted to prevent eavesdropping. However, they also have a critical vulnerability: the relay nodes must be completely trusted.

Maintaining complete trustworthiness of these relay nodes comes with high costs and may not be guaranteed. If these nodes are not entirely trusted, there is a potential risk of information leakage. Risks and benefits coexist, and for QKD networks to scale up, cost reduction becomes crucial, which means there is a high probability of allowing nodes with certain leakage risks to exist. Our goal is to mitigate these risks. Previous research has proposed a multipath QKD scheme. In a partially trusted relay QKD network, distributing a global key through a single path may lead to key leakage under eavesdropper attacks. As shown in Figure 5, Alice distributes keys through two disjoint paths, resulting in two separate keys. Bob then reconstructs the final global key through XOR operations. The global key remains secure unless the eavesdropper obtains keys from all paths. It's important to note that the multipath QKD scheme requires no common intermediate nodes, as the compromise of a common node could lead to complete key leakage [24].

However, in practical network topologies, the number of disjoint paths required for the multipath key distribution method is limited. Furthermore,

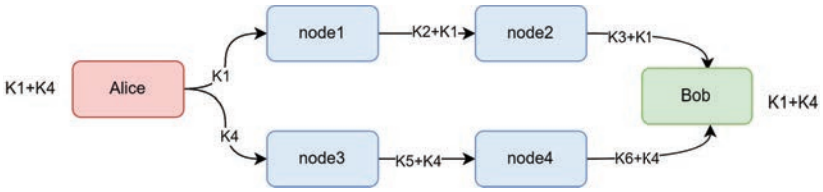


Figure 5 Schematic diagram of partially trusted relay QKD.

taking inspiration from the protection of core routers in Internet Service Provider (ISP) backbone networks, we can select certain relay nodes and provide them with enhanced protection to make them highly trusted. By segmenting the network multiple times through these protected nodes, we can achieve a higher level of trust [22]. Considering the impact of key freshness on system confidentiality, we evaluate the key generation time within these different segments to determine their security probability. Based on this security probability, we select the paths with the highest security level. Our main work is summarized as follows:

(1) By protecting certain nodes along the paths and making them highly trusted, we enhance the security of partially trusted QKD networks. Through multiple segmentations using these nodes, we achieve improved security.
(2) We employ an adaptive routing algorithm that considers the contribution of the relay nodes in the multiple paths, the freshness of the keys, and the reliability of the nodes. This algorithm generates different security probabilities based on these factors. By comparing these security probabilities, we can generate different paths.
(3) To evaluate the performance of the proposed QKD algorithm, we conducted extensive simulations in various scenarios. The results demonstrate that this method offers significantly better security compared to traditional multipath approaches.

The remaining sections of the paper are organized as follows: In Section 2: Network Model Design. This section presents the network model designed for the study. In Section 3: Multiple Segmentation of Paths. Here, the specific details of the multiple segmentation of paths are described. In Section 4: Simulation and Analysis Results. In this section, the simulation and analysis results are presented. In Section 5: Conclusion and Future Directions. The paper concludes with a summary of the work and provides insights into future directions for research.

2 Introduction to Network Models

2.1 Segmented Topology

As shown in Figure 6, our structure consists of multiple segments and trusted relays between segments. Similar to multi-path QKD key distribution, our multi-segment QKD network first divides the key k1 into k2, k3, and k4. These three keys can be reassembled into the original key k1 through XOR operations. K2, k3, and k4 are then routed through different quantum relay routers for transfer. At this point, if an eavesdropper wants to obtain our key information, they would need to intercept all three paths of the keys simultaneously, similar to multi-path key distribution. When the keys reach the trusted relays between segments, the keys are reassembled. After reassembly, the keys are further divided into k5 and k6 and transmitted through untrusted relays. Finally, they reach the destination node. Compared to traditional multi-path QKD, the underlying logic of this approach's security lies in the fact that if an eavesdropper obtains one segment of the key, they only have access to that specific segment, rather than a segment in the global context. This significantly enhances the security of QKD. Furthermore, multi-path key distribution requires the absence of common relay nodes. This is because the security of the entire QKD network would be compromised if a relay node, particularly a common one, is susceptible to information leakage. However, this issue is mitigated in our multi-segment QKD network as we have trusted relay nodes at our disposal. With these trusted nodes, we can accomplish path crossing without concerns about the aforementioned security problem. Figure 6 includes several details that have not been mentioned, such as how to select routes when there are multiple paths. Our approach involves selecting routes based on the contribution rate of the relay nodes and the freshness of the keys, which will be described in detail in the third section.

2.2 Program Design and Implementation

In terms of the implementation of the QKD network, we have developed the SIMQN Quantum Network Layer Simulator [6], which was released earlier this year. The simulator allows users to focus on the design and development of the network layer without needing to delve too much into the details of the quantum layer. With this simulator, we have various tools available that assist in generating network topologies and greatly aid in the development and design of the QKD network.

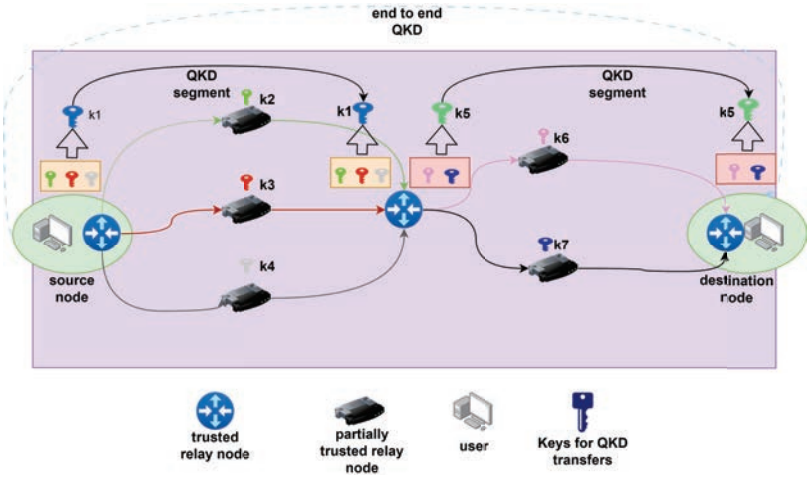


Figure 6 Schematic diagram of multiple segments based partially trusted relay QKD link.

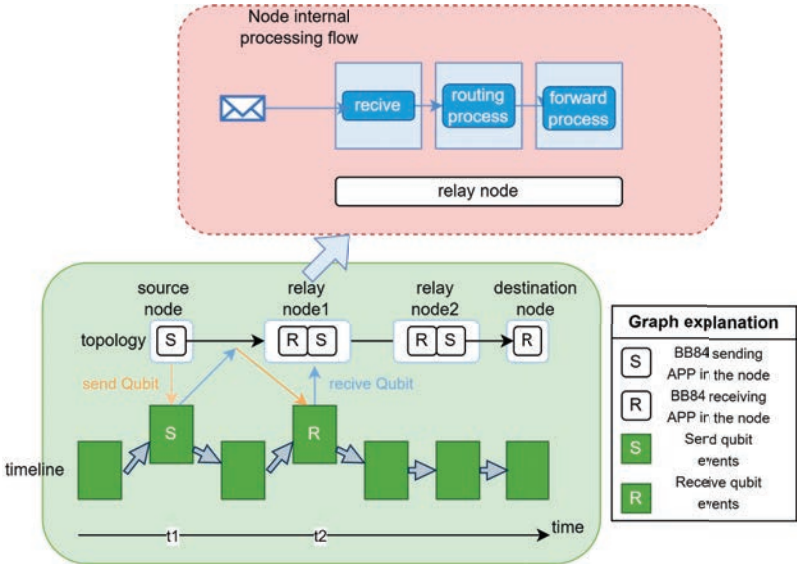


Figure 7 Schematic diagram of multiple segments based partially trusted relay QKD link.

As shown in Figure 7, the entire network consists of nodes and events. Each node can be envisioned as a desktop computer capable of installing various modules. For each relay node except the last one (as the destination node does not need to forward data), we install a transmitting app that

supports the BB84 protocol, and for all nodes except the first one, we install a receiving app that supports the BB84 protocol. If we examine the source code of these BB84 apps, we will find components for transmitting and receiving quantum bits as well as classical bits. This is because the BB84 protocol requires support from classical networks.

In our QKD network, it starts with the source node initiating a key transmission request, and the program performs routing planning based on this request. After the planning stage, multiple paths are established through BB84 forwarding requests. When a relay router receives a data packet, it examines the routing information and forwards the packet to the next hop. Once the packet reaches a trusted node in the multi-segment network, a key recombination is performed. The key is then further split and forwarded until it reaches the final destination node.

3 Multi-Segment Based Multi-path Routing Algorithm

In this section, we will provide a detailed description of the specific implementation of the route selection for multi-path routing discussed in Section 2. A partially trusted QKD network refers to a network composed of a combination of trusted and untrusted nodes, where users initiate secure communication requests and the nodes are responsible for transmitting secure keys. Previous research has confirmed that the freshness of the keys and the contribution rate of the nodes have a significant impact on the success rate of key exchange and the remaining key quantity.

In a partially trusted QKD network, it is not possible to guarantee that all nodes are secure and trustworthy, and the security of the network cannot be guaranteed with 100 certainty. Therefore, we introduce the concept of node reliability. Our goal is to design excellent algorithms that can maximize the security of the network.

By considering the reliability of the nodes and employing robust algorithms, we aim to minimize the risk of key compromise in the network. The selection of routes in the multi-path QKD network is based on evaluating the contribution rate of the relay nodes and the freshness of the keys. These factors are used to calculate the security probability of each path, and based on these probabilities, the routes with the highest security level are chosen.

The algorithm takes into account the trade-off between security and resource utilization. It aims to select paths that have both high security and efficient resource utilization. This approach allows us to enhance the

security of the QKD network while optimizing the utilization of network resources.

In the next section, we will provide a detailed explanation of the algorithm used for route selection in the Multi-Segment based Multi-path QKD network, including the considerations of node reliability, contribution rate, key freshness, and security probability calculation.

3.1 Link Cost Function

Due to the variation in the remaining key quantity of each quantum link as keys are generated and consumed, it is important to consider the adequacy of the remaining key quantity and the success rate of route selection before performing routing. When selecting routes, priority is given to links with a sufficiently large remaining key quantity, while the path length is considered secondary. Therefore, the key aspect lies in dynamically calculating the variation in the remaining key quantity of the links.

In a quantum communication network, to ensure an adequate key quantity for the selected links, this paper adopts the contribution rate $\lambda_{e_{i,j}}$ of nodes to the links to reflect the dynamic variation of the remaining key quantity. The link with the highest contribution rate is given priority, which corresponds to the link with the greatest increase in remaining key quantity after a key exchange, ensuring a balanced key quantity in each link. The contribution rate of a node to a link can be represented as Equation (1) shows:

$$\lambda_{e_{i,j}} = \frac{G_{e_{i,j}}}{C_{e_{i,j}}} \tag{1}$$

In the above formula, $\lambda_{e_{i,j}}$ represents the contribution rate of the node to the route selection,$\lambda_{G_{e_{i,j}}}$ represents the key generation quantity of the quantum link within time t, and $\lambda_{C_{e_{i,j}}}$ represents the key consumption quantity of the quantum link within time t. When $\lambda_{e_{i,j}} > 1$, it indicates that the key generation quantity of the quantum link exceeds the key consumption quantity after the key exchange, resulting in an increase in the remaining key quantity. When $\lambda_{e_{i,j}} < 1$, it indicates that the key generation quantity of the quantum link is less than the key consumption quantity, resulting in a decrease in the remaining key quantity.

In a quantum communication network, in addition to considering the contribution rate of nodes, the freshness of keys in the key pool should also be taken into account. Since the key quantity is dynamic, route selection must consider the current key quantity of each link.

This paper calculates freshness using the maximum capacity of the key pool and the remaining key quantity,as Equation (2) shows:

$$\theta_{e_{i,j}} = \frac{\min\{S_{\nu_i}, S_{\nu_j}\} - R_{e_{i,j}}}{\min\{S_{\nu_i}, S_{\nu_j}\}} \tag{2}$$

The above equation indicates that the smaller the value of $\theta_{e_{i,j}}$, the larger the remaining key quantity, implying a relatively higher key generation rate and higher key freshness. Conversely, the larger the remaining key quantity, the larger the value of $\theta_{e_{i,j}}$, indicating a relatively lower key generation rate and lower key freshness. Therefore, the quantity of remaining keys directly affects the key freshness, which refers to the number of newly generated keys and their availability.

To accurately select an optimal load-balanced multi-path route, this paper takes into account both the contribution rate of nodes and the freshness of keys. It designs a link cost function that comprehensively reflects the dynamic variation of the remaining key quantity, as Equation (3) shows:

$$\text{cost}_{e_{i,j}} = \frac{\min\left\{S_{v_i}, S_{v_j}\right\}}{\theta_{e_{ij}} + \alpha} \left(\mathbf{e}^{\lambda_{e_{i,j}}} + \alpha\right) * (1/R) \tag{3}$$

In the above formula, $\lambda_{e_{i,j}}$ represents whether the link $\lambda_{e_{i,j}}$ was selected in the previous route selection, initialized as 0, and set to 1 if selected. This ensures that each link has an equal chance of being selected, avoiding the repetition of selecting previously chosen links. R represents the security level of the node, which is a number between 0 and 1. However, since a larger cost value generally indicates higher expenses, we take the reciprocal.

The overall link cost function for the entire path can be represented as Equation (4) shows:

$$\cos t_{\text{path}(a,b)}(t) = \sum_{e_{i,j} \in \text{path}(a,b)} \frac{\min\left\{S_{\nu_i}, S_{\nu_j}\right\}}{\theta_{e_{i,j}} + \alpha} \left(e^{\lambda_{\alpha_{i,j}} + \alpha}\right) * (1/R) \tag{4}$$

3.2 Multi-segment Multi-path Routing Algorithm Based on Partially Trusted Relay

Unlike single-path routing algorithms, in multi-path routing algorithms, if the key is eavesdropped during transmission, a new secure path needs to be found. However, in multi-path routing algorithms, information is transmitted

through multiple paths, and a new path is only needed if the key is eavesdropped on every path. This increases the difficulty for attackers to eavesdrop, ensuring the security of network transmission. Our segmented multi-path approach goes a step further than traditional multi-path approaches, as even if an attacker obtains one key, it is only a key for that segment, not the global key. Unlike classical multi-path routing algorithms in traditional networks, information in quantum secure transmission is encrypted using "one-time-pad" with quantum keys. Therefore, the dynamic change of quantum keys in the link becomes a key factor in route selection. In quantum secure transmission, the remaining key quantity, freshness, and node reliability on each link are important considerations for transmission security. The above algorithm, combined with multiple segmented routing strategies, can provide higher security than ordinary randomly selected routes. There are two reasons: 1. We chose a safer path through Dijkstra. 2. By multiple segmentation, the number of key transmission paths is increased, and attackers need to attack more paths to obtain complete key information.

This paper proposes a multi-segment multi-path routing algorithm aimed at improving the success rate of key exchange and ensuring the security of information transmission. This algorithm considers factors other than path hop count, such as the remaining key quantity in the link, the key generation quantity of each routing node, and the key consumption required for transmission, as metrics. The weight of each link is calculated through a link cost function, and the optimal path is computed using a Dijkstra algorithm based on heap optimization. The traditional dijkstra algorithm has a time and spatial complexity of O(n^2),and after heap optimization (implemented with priority queues), the time complexity can reach O($nlogn$). The algorithm first calculates the optimal path, then deletes the links on that path and continues to compute suboptimal paths. Finally, when the total number of paths is less than the required number, the algorithm analyzes whether the remaining key quantity on each link of each path is sufficient. If it is insufficient, the total number of paths is set to zero, and a new route selection is performed. If it is sufficient, a new route selection is not necessary. Through this process, multiple optimal paths from the source to the specified destination can be obtained. This multi-path routing algorithm comprehensively considers multiple factors to improve the success rate of key exchange and ensure the security of information transmission. After reaching a reliable node in each intermediate of the multi-path, we need to recalculate the QKD routing information. The code for each segmented algorithm is as follows:

Algorithm 1 Each segmented algorithm

Input: The number of multipaths, the amount of remaining keys for each link, the amount of key generation, the total amount of global keys, and the reliability of different nodes.
Output: Details of the n optimal paths.
query each quantum link $e_{i,j}$ in G.
$p_n \leftarrow p/n$
  if $Re_{i,j} < p_n$:
    delete link $e_{i,j}$
  $w \leftarrow 1/cost$
$d \leftarrow 0$
while $d < n$ do
  Add the points connected to the source node to the heap and adjust the heap.
  Select the top element (u) with the minimum weight from the heap, remove it from the heap, and adjust the heap.
  while v is adjacent to u and is not visited and dist[u]+cost[e] $<$ dist[v] do
    if v in the heap
      Update dist[u] and adjust the position of v on the heap
    else
      Add v to the heap, and update the heap
    end if
end while
if u ==destination
    $d \leftarrow d + 1$
    output optimal path
    Delete each link of the optimal path in G, and update G
else
    repeat 9 and 10
    end if
end while
if $d < n$
    query each quantum link $e_{i,j}$ in G
    $p_n \leftarrow p/d$
if $Re_{i,j} < p_n$
$n \leftarrow d$
    continue from 3 execute
    end if
end if

4 Performance Evaluation and Analysis

To validate the performance of our proposed algorithm, we conducted numerical simulations and compared it with existing random path algorithm (RP), traditional multi-path algorithm (TMR), and segment-based flexible key reconstruction algorithm (SMR) under various scenarios. We used the

SIMQN simulation platform, and for constructing the network topology, we utilized the Waxman-Salama model built into SIMQN, with a selected number of 100 nodes.

We set the initial key quantity in the key pool to 600 kb and the key generation rate to 15 kb/s, which is comparable to the rate of key generation in existing backbone networks per second. Each key pool had a capacity of 10 M. Throughout all the experiments, we assumed that the required key quantity for communication between two users was 768 Kb. In the case of selecting 3 paths, each relay node on the path had a minimum key quantity of 256 Kb. In the case of selecting 2 paths, each relay node on the path had a minimum key quantity of 384 Kb. While maintaining generality, we assumed that the security probability of each untrusted relay node was the same.

Next, we evaluated and discussed the influence of different numbers of trusted relay nodes, and different security probabilities of untrusted relays on the security and key exchange success rate during the key distribution process.

Through these tests, we gained in-depth insights into the performance of our proposed algorithm in different scenarios and conducted a comprehensive analysis of security, resource consumption, and distribution efficiency.

Before beginning and comparing with other QKD routing algorithms, we first validate the impact of three factors—key freshness, security of untrusted relay nodes, and the number of trusted relay nodes—on our multi-segment routing experimental results. As shown in Figure 8(a), if we don't consider the security of untrusted relay nodes, the end-to-end security is significantly affected. This is related to the previously mentioned link cost calculation formula. Similarly, neglecting key freshness, which can lead to key expiration, impacts the success rate of QKD, aligning with the conclusions in Figure 8(b). Figure 8(c) and Figure 8(d) demonstrate that increasing the number of trusted relay nodes enhances overall security.

4.1 Impact of Security Probability of Untrusted Relay on Performance

In our initial simulation, we examined the influence of the security probability of untrusted relay nodes on key distribution security, key consumption, and efficiency. We conducted 10,000 simulation experiments, and as shown in Figure 9, the end-to-end security probability increases as the security probability of untrusted relays increases. The values obtained by our proposed

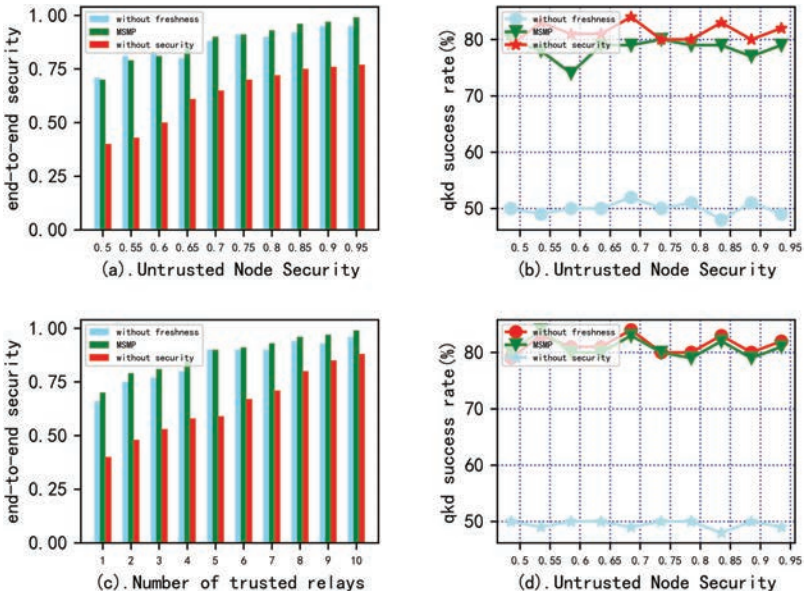


Figure 8 The impact of partially trusted node security on end-to-end security.

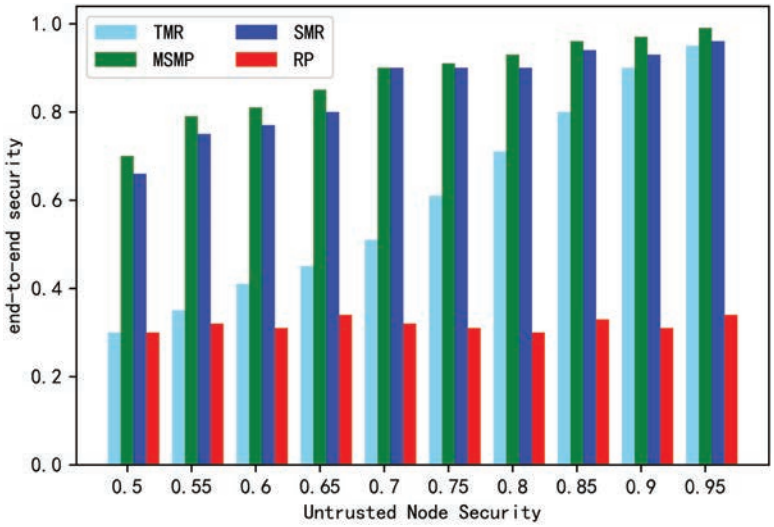


Figure 9 The impact of partially trusted node security on end-to-end security.

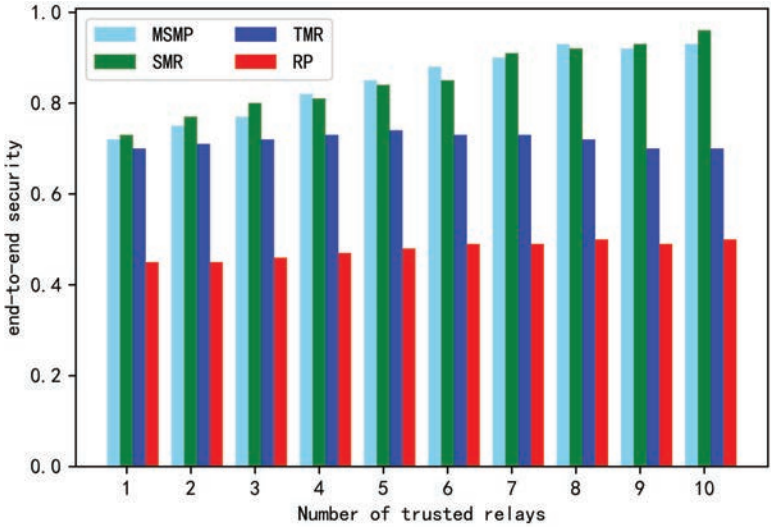


Figure 10 Average transmission success rate for 10,000 experiments.

Multi-Segment Multi-Path (MSMP) algorithm are close to those of the Segment-Based Flexible Key Reconstruction (SMR) algorithm.

Furthermore, in terms of resource consumption, our routing algorithm, which can find more balanced paths, results in lower key consumption for segment-based multi-path routing. As a result, and as shown in Figure 10 our key exchange success rate is higher, similar to the Traditional Multi-Path (TMR) algorithm, but our algorithm demonstrates better stability compared to TMR.

4.2 Impact of Number of Trusted Relays on Performance

We conducted simulations to evaluate the impact of different numbers of trusted relay nodes on system performance. As shown in Figure 11, the end-to-end security probability increases as the number of trusted relay nodes increases. However, even with the increase in trusted relay nodes, the security level achieved by the MSMP algorithm is comparable to that of the SMR algorithm.

In terms of resource consumption, our proposed routing algorithm takes into account load balancing, which allows for more efficient key consumption and higher key exchange success rates. As shown in Figure 12 by considering load balancing, our algorithm optimizes the key consumption, leading to improved overall system performance.

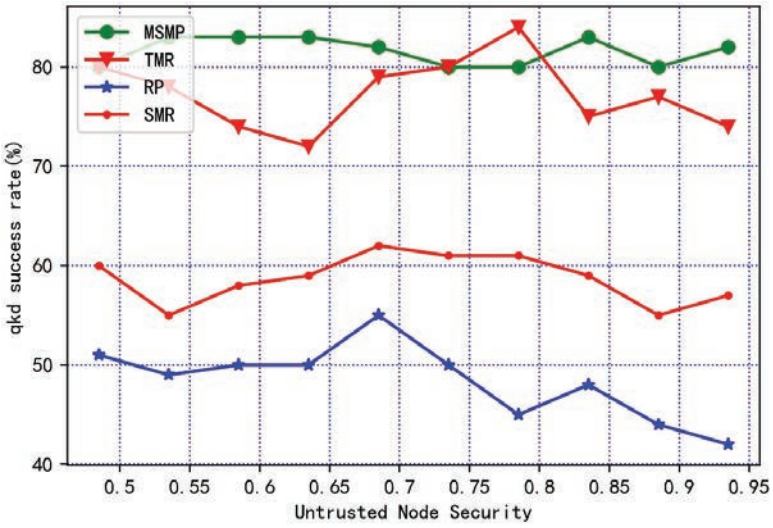


Figure 11 The impact of number of trusted relays on end-to-end security.

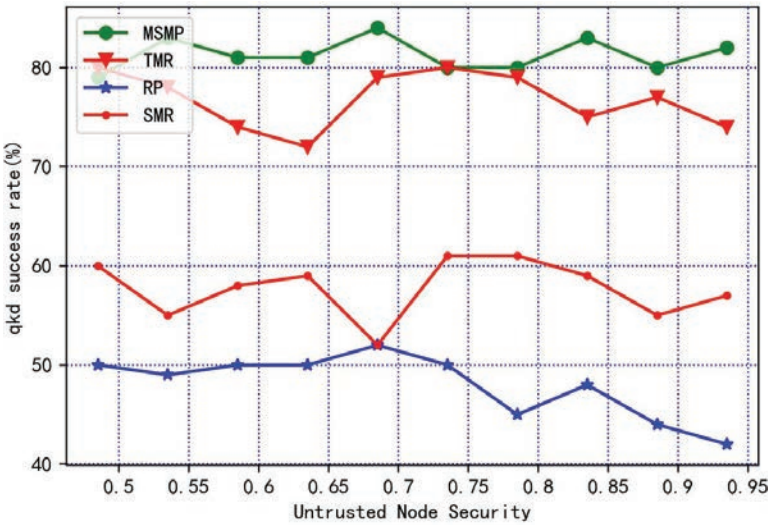


Figure 12 Average transmission success rate for 10,000 experiments.

5 Discussion and Conclusion

In this paper, we have studied potential eavesdropping attacks in partially trusted relay-based quantum key distribution (QKD) networks and analyzed

the issues that may arise during the key distribution process. To overcome the limitations of existing work and address these security concerns, we have designed a multi-segment multi-path key distribution method that leverages trusted relay nodes within the paths to maximize the security of the key distribution process. Additionally, we have incorporated the contribution rate of relay nodes in multiple paths and the freshness of keys to enhance the load balancing of the QKD network. Extensive simulation results have demonstrated that our method outperforms traditional multi-path key distribution methods in terms of security, resource consumption, and distribution efficiency.

In the future, we plan to further investigate the impact of the number and placement of trusted relay nodes in the network, as well as the length of keys transmitted in each session, and provide possible solutions.

As quantum information technology continues to advance, we envision the establishment of a quantum internet, enabling quantum computing and quantum communication. As an important application in the quantum internet, quantum key distribution provides unconditional security for classical networks. However, attacks against relay nodes and low key distribution success rates greatly affect the availability of remote QKD. Our simulation results demonstrate that our proposed method can effectively enhance the security and success rate of key distribution, providing assistance for the construction of large-scale quantum networks in the future.

Acknowledgement

This work was supported by the Open Fund of Advanced Cryptography and System Security Key Laboratory of Sichuan Province (Grant No. SKLACSS–202208) and National Natural Science Foundation of China (No. 61772295).

References

[1] Akwasi Adu-Kyere, Ethiopia Nigussie, and Jouni Isoaho. Quantum key distribution: Modeling and simulation through bb84 protocol using python3. *Sensors*, 22(16):6284, 2022.

[2] Charles H Bennett. Quantum cryptography using any two nonorthogonal states. *Physical review letters*, 68(21):3121, 1992.

[3] Charles H Bennett, François Bessette, Gilles Brassard, Louis Salvail, and John Smolin. Experimental quantum cryptography. *Journal of cryptology*, 5:3–28, 1992.

[4] Gilles Brassard, Norbert Lütkenhaus, Tal Mor, and Barry C Sanders. Limitations on practical quantum cryptography. *Physical review letters*, 85(6):1330, 2000.

[5] Chih-Yu Chen and Tzonelih Hwang. Mediated authenticated differential phase shift quantum key distribution. *Optik*, 272:170239, 2023.

[6] Lutong Chen, Kaiping Xue, Jian Li, Nenghai Yu, Ruidong Li, Qibin Sun, and Jun Lu. Simqn: A network-layer simulator for the quantum network investigation. *IEEE Network*, 2023.

[7] Yu-Ao Chen, Qiang Zhang, Teng-Yun Chen, Wen-Qi Cai, Sheng-Kai Liao, Jun Zhang, Kai Chen, Juan Yin, Ji-Gang Ren, Zhu Chen, et al. An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature*, 589(7841):214–219, 2021.

[8] Chip Elliott, Alexander Colvin, David Pearson, Oleksiy Pikalo, John Schlafer, and Henry Yeh. Current status of the darpa quantum network. In *Quantum Information and computation III*, volume 5815, pages 138–149. SPIE, 2005.

[9] Frédéric Grosshans and Philippe Grangier. Continuous variable quantum cryptography using coherent states. *Physical review letters*, 88(5):057902, 2002.

[10] Won-Young Hwang. Quantum key distribution with high loss: toward global secure communication. *Physical review letters*, 91(5):057901, 2003.

[11] Qiang Liu, Yinming Huang, Yongqiang Du, Zhengeng Zhao, Minming Geng, Zhenrong Zhang, and Kejin Wei. Advances in chip-based quantum key distribution. *Entropy*, 24(10):1334, 2022.

[12] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. Measurement-device-independent quantum key distribution. *Physical review letters*, 108(13):130503, 2012.

[13] Akihiro Mizutani, Yuki Takeuchi, and Kiyoshi Tamaki. Finite-key security analysis of differential-phase-shift quantum key distribution. *Physical Review Research*, 5(2):023132, 2023.

[14] William J Munro, Koji Azuma, Kiyoshi Tamaki, and Kae Nemoto. Inside quantum repeaters. *IEEE Journal of Selected Topics in Quantum Electronics*, 21(3):78–90, 2015.

[15] Melis Pahalı, Kadir Durak, and Utku Tefek. Photon budget optimization in an e91 quantum key distribution protocol. *arXiv preprint arXiv:2212.13837*, 2022.

[16] Momtchil Peev, Christoph Pacher, Romain Alléaume, Claudio Barreiro, Jan Bouda, W Boxleitner, Thierry Debuisschert, Eleni Diamanti,

Mehrdad Dianati, JF Dynes, et al. The secoqc quantum key distribution network in vienna. *New Journal of Physics*, 11(7):075001, 2009.

[17] Cheng-Zhi Peng, Jun Zhang, Dong Yang, Wei-Bo Gao, Huai-Xin Ma, Hao Yin, He-Ping Zeng, Tao Yang, Xiang-Bin Wang, and Jian-Wei Pan. Experimental long-distance decoy-state quantum key distribution based on polarization encoding. *Physical review letters*, 98(1):010505, 2007.

[18] Danna Rosenberg, Jim W Harrington, Patrick R Rice, Philip A Hiskett, Charles G Peterson, Richard J Hughes, Adriana E Lita, Sae Woo Nam, and Jane E Nordholt. Long-distance decoy-state quantum key distribution in optical fiber. *Physical review letters*, 98(1):010503, 2007.

[19] Masahide Sasaki, Mikio Fujiwara, H Ishizuka, W Klaus, K Wakui, M Takeoka, S Miki, T Yamashita, Z Wang, A Tanaka, et al. Field test of quantum key distribution in the tokyo qkd network. *Optics express*, 19(11):10387–10409, 2011.

[20] Claude E Shannon. Communication theory of secrecy systems. *The Bell system technical journal*, 28(4):656–715, 1949.

[21] Gautam Shaw, Shyam Sridharan, Shashank Ranu, Foram Shingala, Prabha Mandayam, and Anil Prabhakar. Time-bin superposition methods for dps-qkd. *IEEE Photonics Journal*, 14(5):1–7, 2022.

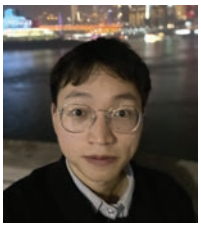
[22] Mingjun Wang, Jian Li, Kaiping Xue, Ruidong Li, Nenghai Yu, Yangyang Li, Yifeng Liu, Qibin Sun, and Jun Lu. A segment-based multipath distribution method in partially-trusted relay quantum networks. *IEEE Communications Magazine*, 2023.

[23] Xiang-Bin Wang. Beating the photon-number-splitting attack in practical quantum cryptography. *Physical review letters*, 94(23):230503, 2005.

[24] Hao Wen, ZhengFu Han, YiBo Zhao, GuangCan Guo, and PeiLin Hong. Multiple stochastic paths scheme on partially-trusted relay quantum key distribution network. *Science in China Series F: Information Sciences*, 52(1):18–22, 2009.

[25] Yi-Heng Zhou, Zong-Wen Yu, and Xiang-Bin Wang. Making the decoy-state measurement-device-independent quantum key distribution practically useful. *Physical Review A*, 93(4):042324, 2016.

Biographies



Cheng Liu received a Bachelor's degree in Network Engineering from Chongqing University of Posts and Telecommunications in 2019. Currently, he is pursuing a Master's degree in Computer Application Technology at Chongqing Normal University. His primary research areas include quantum computing and quantum communication.

Xuanxuan Che is a graduate student of Chongqing Normal University, researching in the direction of quantum computing.

Jianshe Xie is a current Master of Science student in Computer Software and Theory at Chongqing Normal University, School of Computer Information

and Science. His research focuses on the optimization of variational quantum algorithms and the computational advantages of hybrid quantum algorithms.

Yumin Dong, (Member, IEEE) was born in Jianping County, Liaoning, China, in 1966. He received the bachelor's degree in physics radio from Liaoning University, in 1988, the master's degree in computer application from Northeast University, in 1997, and the Ph.D. degree in control theory and control engineering from the East China University of Science and Technology, in 2007. He was a Computer Application Professional Engineer with Dongfeng Chaoyang Diesel Engine Company, from 1988 to 1998, and the ERP Development System Analyst of Beijing UFIDA Soft-ware Company Ltd., from 1999 to 2000. He was a Professor and a Master Supervisor with the School of Computer Science, Qingdao University of Technology, from 2001 to 2018. Since 2018, he has been a Professor and a Master Supervisor with the School of Computer Science, Chongqing Normal University. He has published more than 80 articles, two invention patents, presided over three NSFC projects, participated in three NSFC projects, presided over one provincial NSFC Project, and presided over five other projects. His scientific research interests include quantum information, artificial intelligence, computer application, ERP, and parallel computing.