applied sciences

MDPI

Article

Wide Area Key Distribution Network Based on a Quantum Key Distribution System

Hua Dong [1,2,3,†], Yaqi Song [4,†] and Li Yang [1,2,3,*]

1 State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China; donghua@iie.ac.cn
2 State Key Laboratory of Cryptology, P.O.Box 5159, Beijing 100878, China
3 School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China
4 China Academy of Electronics and Information Technology, Beijing 100041, China; songyaqi@iie.ac.cn
* Correspondence: yangli@iie.ac.cn; Tel.: +86-133-0132-0389
† These authors contributed equally to this work.

Received: 16 January 2019; Accepted: 6 March 2019; Published: 14 March 2019

Abstract: The point-to-point quantum key distribution (QKD) system is limited by the transmission distance. So, the wide area QKD network with multiple endpoints is the research focus of this study. The relay-node scenario and key relay protocols provide the solutions to the QKD network. The early key relay protocols require the relay nodes to be reliable. Once the relay nodes become compromised, the whole network is insecure. In this paper, we extend the chain structure of the public-XOR(exclusive OR)-key scheme with two endpoints to the complex network with multiple endpoints. The relay nodes in our scheme do not need encryption actions, decryption actions, or storage XOR keys, which simplifies the system compared with other key distribution schemes based on trusted relay nodes. Our scheme not only improves the practical performance and simplifies the system's complexity, but it also ensures that the security is not reduced. Specifically, we rigorously demonstrate that an eavesdropper can never access the key shared by the users of the network as long as the process of generating XOR keys and destroying the original keys is secure. In addition, we discuss the information leakage of the practical QKD network from the perspective of the unicity distance.

Keywords: quantum key distribution; key distribution network; relay node; unicity distance

1. Introduction

To ensure the security of communications on the internet, an effective solution is to use cryptographic techniques. The security of the most classical cryptosystems depends on the computational complexity of the algorithms. With the fast development of quantum computation and quantum algorithms, communication security based on the above algorithms is greatly compromised. In conventional cryptography, a typical cryptosystem not based on the computational assumptions is the one-time-pad, which is unconditionally secure and free from the threat of quantum computing. In one-time-pad, the length of the keys and the messages is the same, and the keys can only be used once. Both communicating parties need to share the keys in advance. The security of one-time-pad should be completely dependent on the confidentiality of the pre-shared keys. It is too expensive to realize and too difficult to apply in practice. Thus, how to realize the unconditionally secure key distribution becomes a critical problem, which motivates the development of quantum key distribution (QKD). In 1984, Bennett and Brassard proposed the concept of QKD [1], which achieves the unconditionally secure key distribution based on quantum mechanics. It enables both parties of communication to generate and share a random and secure key. Then a series of QKD protocols have been proposed [2–5]. More importantly, the unconditional security of QKD protocol has been strictly proved [6–9].

The early implementations of QKD systems mainly focus on the communication between two endpoints. The point-to-point QKD system is limited by the transmission distance, which is limited by the key rate. So, the development of a wide area QKD network is a challenging issue. Some countries and regions have deployed QKD networks for last years. The first experiment of QKD network was designed by Townsend [10]. Some QKD network projects [11–18] have been completed successfully, such as the defense advanced research projects agency (DARPA) quantum network [11] set up by the USA in 2004, secure communication based on quantum cryptography (SECOQC) designed by the European project [13], the commercial telecommunication fiber network in China [12], the SwissQuantum QKD network project launched in Geneva [14], and the live video conference through a high-speed QKD network in Tokyo [16]. Satellite communications are also building QKD networks, such as the international QKD channel created by the QUESS space mission [19,20] and the world's first space-ground quantum network [21,22]. These projects supported by different underlying devices can be divided into three categories: (1) satellite communications; (2) quantum relaying; (3) classical trusted relay. In the light of the present situation, the satellite-based method is not realistic, and the research of quantum relay equipment is not perfect. Thus, determining how to establish a practical and secure QKD network based on the trusted relay is the key problem.

The approach of using trusted relays in QKD networks was proposed in 2002 [23]. This allows both endpoints to access a series of trusted relays to expand the arbitrary distance. The BBN key relay protocol has been operating continuously in the DARPA quantum network since 2003 [24]. In the protocol, the endpoints create a new random number R and send R through the trusted relay nodes by one-time-pad encryption. Each trusted relay node of the chosen path decrypts the ciphertext with the QKD keys shared with the upstream node and encrypts R with the QKD keys shared with the downstream node. In 2012, Los Alamos National Laboratory set up a trusted hub-and-spoke QKD network [18]. To communicate, each node sends a one-time pad to the hub, which it then uses to communicate securely over a classical link. The entire network is secure only if the central hub is secure. In these relay nodes-based key distribution schemes, if one of the relay nodes gets compromised, the whole network is insecure. Additionally, the relay nodes need encryption actions, decryption actions and storage of function, which increase the complexity of the system. In [25], Schartner and Rass proposed a re-encryption key distribution scheme for relay QKD system, which is introduced in Section 2.1. Compared with BBN key relay protocol, the re-encryption scheme reduces the damage in case of the compromised node and reduces the storage memory of keys for relay nodes. However, in re-encryption scheme, the relay nodes still need to keep the XOR (exclusive OR) value of the QKD keys secretly, and the successive communications between adjacent relay nodes is also required. In 2013, "Beijing–Shanghai Line" of quantum secrecy communication is based on the public-XOR-key scheme, where each trusted relay node publicly announces the XOR key it holds, enabling the endpoints to share a key. Compared with the re-encryption scheme, the scheme simplifies the system's complexity and eases the traffic of the relay nodes. In 2014, William Stacey et al. proposed a simplified trusted relay (STR) protocol for point-to-point [26]. It is similar to public-XOR-key scheme. The two endpoints of STR are connected by a series of trusted relays that announce the XOR keys, but the rest of the classic QKD post-processing needs to be performed based on data from its original terminal, which comes at the cost of a low key rate.

Contributions: considering the key rate and the requirements of the long-distance communications with multiple endpoints, the public-XOR-key scheme is more efficient and practical than the BBN protocol, re-encryption protocol and STR. We extend the chain structure of the public-XOR-key scheme with two endpoints to the complex network with multiple endpoints. Our contributions are as follows.

- Our scheme can reduce the memory complexity and heavy traffic of communications for relay nodes in real implementation. It is appropriate for the remote communications of the complex networks with multiple endpoints. Compared with other key distribution schemes based on relay nodes, our scheme reduces the complexity of the system and eases the traffic of the relay nodes.

- Compared with the re-encryption schemes that does not announce the XOR value, our scheme not only improves the actual performance and simplifies the complexity of the system, it also does not weaken the security of the system. To analyze the security, we build the threat model and the security model of the public-XOR-key scheme. We rigorously demonstrate that the scheme is as secure as the re-encryption scheme under the same adversary model. In addition, we analyze the information leakage of practical QKD network from the perspective of Shannon's ciphertext-only attack model by exploring the theory of unicity distance and applying it to the model of practical QKD networks.

2. Preliminaries

In this section, we review two cryptographic primitives that are necessary for understanding the proposed complex QKD network scheme, including the re-encryption key distribution scheme and the theory of unicity distance for discussing information leakage of practical key distribution scheme.

2.1. Re-Encryption Scheme for QKD Network

In re-encryption scheme, a secret message is encrypted by sender's local random key s. The delivery of the random key s can be executed by the following protocol. After the protocol, two endpoints can share the key s. The following is the main steps of the re-encryption protocol with two endpoints.

Protocol 1: re-encryption scheme for the relay QKD network:

1. Each node executes QKD protocol with its neighbor nodes, which generates n pairs of QKD keys Qk_i as shown in Figure 1.
2. Alice encrypts the random key s with her QKD key Qk_1, which is shared with the first relay node. Calculate the first ciphertext $c_1 = s \oplus Qk_1$, where $\oplus$ denotes bitwise module-2 addition.
3. The relay nodes do the XOR operation with the QKD keys, which are shared with the upstream relay nodes and the downstream relay node, to obtain the XOR keys a_i, i.e., $a_i = Qk_i \oplus Qk_{i+1}$, then immediately dismiss the QKD keys, Qk_i, $Qk_i + 1$. When relay node i receives the incoming ciphertext, it calculates $c_{i+1} = c_i \oplus a_i$. It is easy to see that $c_i = s \oplus Qk_i$.
4. When Bob receives the incoming ciphertext, $c_n = s \oplus Qk_n$, he decrypts the ciphertext with his QKD key Qk_n to obtain s. Then Alice and Bob share the common key s. Alice can transmit the message secretly to Bob with the key latter.

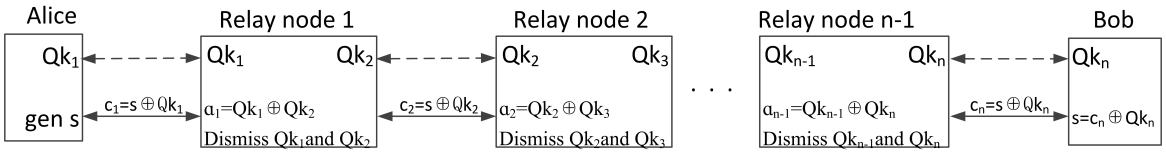

Figure 1. The model of re-encryption key distribution scheme for the relay QKD system. The dotted arrow stands for the quantum key distribution (QKD) process. The solid arrow stands for the re-encryption process. Relay node i re-encrypts the ciphertext c_i and transfers $c_{i+1} = c_i \oplus a_i$ to the next node.

2.2. The Theory of Unicity Distance

In order to discuss the information leakage of the practical QKD network, we study it from a perspective of the unicity distance. Shannon laid the foundations of communication theory of secrecy system in [27]. In the second part of the paper, he put forward the concept of unicity distance, which gave a way of calculating approximately how many ciphertexts are required to obtain the key of a secrecy system. The adversary tries each possible key to decrypt the intercepted ciphertexts, and records the keys which make the deciphered messages meaningful in the original language. Only one of the record keys is the correct one, others are spurious keys.

In Shannon's ciphertext-only attack model, suppose there is a symmetric cryptosystem (M, C, K, E, D), where $|C| = |M|$. In the cryptosystem, M denotes plaintext space, C denotes ciphertext space, K denotes key space, E denotes the encryption algorithms and D denotes the decryption algorithms. For $m \in M$, $k \in K$, the encryption algorithm is $E_k(m_i) = c_i$. Suppose the plaintexts are in language L, the rate(entropy) is

$$H_L = \lim_{n\to\infty} \frac{H(A^n)}{n}. \tag{1}$$

The redundancy of the language L is defined as

$$R_L = 1 - \frac{H_L}{\log_2 |A|}, \tag{2}$$

where A is the word set, $|A|$ is the number of words in language L, A^n is the totality of all plaintext n-alphabets, and H_L denotes the average information bits of the each word in language L. R_L measures the degree of statistical constraint imposed by language L.

For $Y \in C^n$, $K(Y)$ is defined as a set of all possible key with the given ciphertext Y, $p(Y)$ is the probability of the events Y occurring. The expected number of spurious key is

$$\overline{S_n} = \sum_{Y\in C^n} p(Y)\left(|K(Y)| - 1\right) = \sum_{Y\in C^n} p(Y)|K(Y)| - 1. \tag{3}$$

When n is sufficiently large, the relationship between the redundancy of the language R_L and the plaintext M is

$$H(M^n) \approx n(1 - R_L)\log_2 |M|. \tag{4}$$

Since $H\left(K|C^n\right) = H(K) + H\left(M^n\right) - H\left(C^n\right)$, $H\left(C^n\right) \le n\log_2 |C|$, where C^n is the totality of all ciphertext n-alphabets. Then

$$H\left(K|C^n\right) \ge H(K) - nR_L \log_2 |M|. \tag{5}$$

According to Jensen's inequality and Equation (3), the conditional entropy is

$$\begin{aligned} H\left(K|C^n\right) &= \sum_{Y\in C^n} p(Y)H\left(K|Y\right) \le \sum_{Y\in C^n} p(Y)\log_2 |K(Y)| \\ &\le \log_2 \sum_{Y\in C^n} p(Y)|K(Y)| = \log_2\left(\overline{S_n} - 1\right). \end{aligned} \tag{6}$$

Therefore, the expected number of spurious key $\overline{S_n}$ satisfies that

$$\overline{S_n} \ge \frac{2^{H(K)}}{|M|^{nR_L}} - 1. \tag{7}$$

When the length of the ciphertext is N_0, the expectation of the number of spurious key is null. N_0 is defined as the unicity distance of the system,

$$N_0 \approx \frac{H(K)}{R_L \log_2 |M|}, \tag{8}$$

where the entropy $H(K)$ measures the uncertainty of the value of k.

3. Public-XOR-Key Scheme for QKD Network

In this section, we extend the chain structure of the public-XOR-key scheme with two endpoints to the complex network with multiple endpoints. The scheme is secure as long as the XOR keys are generated securely. In this scheme, there are no re-generation keys and the relay nodes need not perform the encryption operation or store any key material, which reduces the complexity of the

system. There is no need to communicate between adjacent relay node, which avoids communication failure caused by network congestion.

3.1. The Public-XOR-Key Scheme with Chain Structure

First, we introduce the chain structure of two endpoints. In the scheme, each relay node has only two connections with the upstream node and the downstream node. Assume the whole chain network contains $n+1$ nodes. Each node executes QKD protocol with the neighbor nodes. The $n+1$ nodes make up n point-to-point QKD systems. There are two endpoints, $n-1$ relay nodes and n pairs of QKD keys Qk_i for $i = 1, 2, ..., n$.

Protocol 2: public-XOR-key scheme for the relay QKD system:

1. *Each node executes QKD protocol with the neighbor nodes, which generates n pairs of QKD keys Qk_i for $i = 1, 2, ..., n$ as shown in Figure 2.*
2. *Each relay node does the XOR operation with the QKD keys, which are shared with the upstream relay node and the downstream relay node, to obtain the XOR keys. For relay node i, its XOR key is $a_i = Qk_i \oplus Qk_{i+1}$, where Qk_i is the QKD key shared by relay node $i-1$ and relay node i, $Qk_{i=1}$ is the QKD key shared by relay node i and relay node $i+1$. Then each relay node immediately dismisses the QKD keys and publishes the XOR keys. We assume that the process of dismissing QKD keys is secure.*
3. *Bob calculates the final key with all of the public-XOR-key and his QKD key Qk_n. That is, $\bigoplus_{i=1}^{n-1} a_i \oplus Qk_n = Qk_1$. Then Alice and Bob share the common key Qk_1. Alice can transmit the message secretly to Bob with the key Qk_1 latter.*

Remark 1. *There is a security assumption in the protocol that the process of dismissing QKD keys is secure. For the practical realization of the assumption, we give a kind of method as follows. Use the physical isolation to protect XOR operation and the process of dismissing the original QKD keys from the outside world to access its physical devices, so that even if the relay node is compromised, the adversary can not get the original key.*

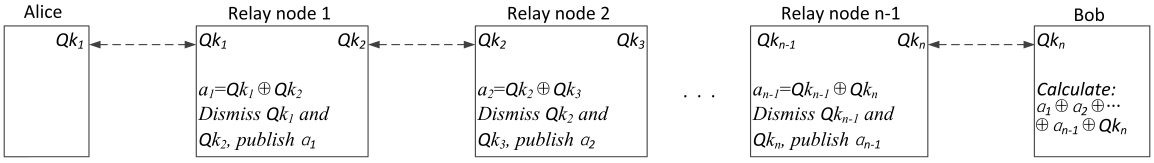

Figure 2. The model of public-XOR-key scheme with two endpoints. The dotted arrow stands for the QKD process. Relay node *i* calculates and publishes $a_i = Qk_i \oplus Qk_{i+1}$, then dismisses the QKD keys immediately. The final key shared by Alice and Bob is $Qk_1 = a_1 \oplus a_2 \oplus ... \oplus a_{n-1} \oplus Qk_n$.

Correctness: Bob calculates the final key with a_i and Qk_n, where $a_i = Qk_i \oplus Qk_{i+1}$. Then he gets

$$\bigoplus_{i=1}^{n-1} a_i \oplus Qk_n = (Qk_1 \oplus Qk_2) \oplus (Qk_2 \oplus Qk_3) \oplus ... \oplus (Qk_{n-1} \oplus Qk_n) \oplus Qk_n = Qk_1, \quad (9)$$

which ensures the correctness of the key distribution scheme.

3.2. The Complex QKD Network Scheme with Multiple Endpoints

We have described the public-XOR-key scheme in the chain network with two endpoints. The following approach is used to solve the key distribution in a wide area network with multiple endpoints. A communication chain is formed between any two endpoints, and multiple communication chains constitute all kinds of network structures. No matter how complex the structures are, there will always be a chain between the two endpoints. As long as the pair of endpoints is in a connected graph, the key distribution scheme is similar to that of Protocol 2. The difference between the communications in the chain network and other complex networks is that some relay nodes have more than two connections

with other nodes. Additionally, the simplest model is the chain structure (each connecting relay node has only two ports). In general networks, there are not only two ports connecting the relay nodes. Since there may be various topological structures in the actual network, we abstract the complex network into simplified model with three-port relay nodes, as shown in Figure 3. The more complex multiple endpoints models are similar to this, as long as it conforms to the principle of one-time padding. Firstly, consider a simplified model that a relay node has three connections that are connected with three endpoints: Alice, Bob and Charlie. Each pair of endpoints is in a chain network. When they execute the original process of Protocol 2, the communications of Alice and Bob, Alice and Charlie are shown in Figure 3. Qk_A is the QKD key shared by Alice and the relay node, Qk_B is the QKD key shared by Bob and the relay node, Qk_C is the QKD key shared by Charlie and the relay node. The relay node calculates and publishes $Qk_{AB} = Qk_A \oplus Qk_B$, $Qk_{AC} = Qk_A \oplus Qk_C$, $Qk_{BC} = Qk_B \oplus Qk_C$, then dismisses the QKD keys immediately. Bob calculates $Q_{AB} \oplus Qk_B$, which is equal to Qk_A. Then Bob and Alice share the same key Qk_A. Charlie calculates $Q_{AC} \oplus Qk_C$, which is equal to Qk_A. Then Charlie and Alice share the same key Qk_A.

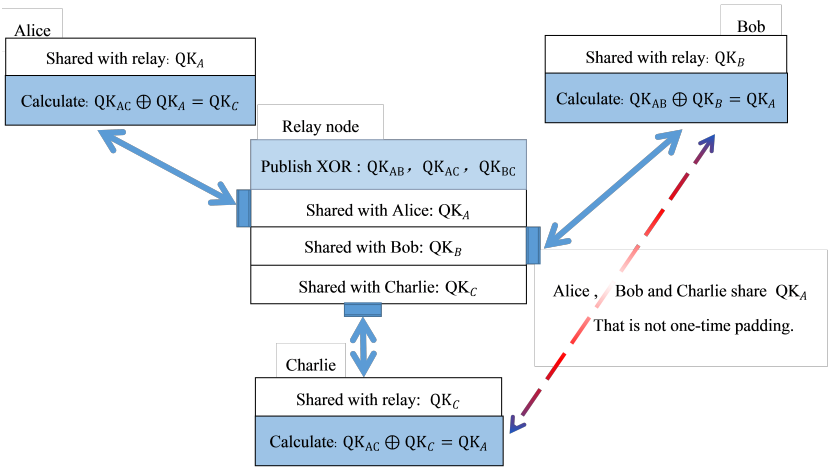

Figure 3. The communications of three endpoints with Protocol 2 with repeated keys. The solid line stands for the QKD process. The relay node calculates and publishes $Qk_{AB} = Qk_A \oplus Qk_B$, $Qk_{AC} = Qk_A \oplus Qk_C$, $Qk_{BC} = Qk_B \oplus Qk_C$, and then dismisses the QKD keys immediately. The dotted line shows the internal attack, where the shared key is not one-time-pad.

However, a key distribution scheme is secure if and only if the shared keys are not known by the third party. In the above scenario, Alice, Bob and Charlie share the same key Qk_A. If Bob or Charlie is the internal attacker, he can get the keys shared by Alice and the other user, which threatens the security.

In order to guarantee the security against the internal attacker, all of the QKD keys should be used only once. The improved key distribution scheme for three endpoints is shown in Figure 4. Qk_{A_1} and Qk_{A_2} are the QKD keys shared by Alice and the relay node, Qk_{B_1} and Qk_{B_2} are the QKD keys shared by Bob and the relay node, Qk_{C_1} and Qk_{C_2} are the QKD keys shared by Charlie and the relay node. Each QKD key is independent of the others. The relay node calculates and publishes $Qk_{A_1B_1} = Qk_{A_1} \oplus Qk_{B_1}$, $Qk_{A_2C_2} = Qk_{A_2} \oplus Qk_{C_2}$, $Qk_{B_2C_1} = Qk_{B_2} \oplus Qk_{C_1}$, and then dismisses the QKD keys immediately. Alice calculates $Qk_{A_2C_2} \oplus Qk_{A_2}$ to get the key Qk_{C_2}, which is the final key shared with Charlie. Bob calculates $Qk_{A_1B_1} \oplus Qk_{B_1}$ to get the key Qk_{A_1}, which is the final key shared with Alice. Charlie calculates $Qk_{B_2C_1} \oplus Qk_{C_1}$ to get the key Qk_{B_2}, which is the final key shared with Bob. Since all QKD keys are used only once and are independent of each other, the third party can never access the keys he should not have.

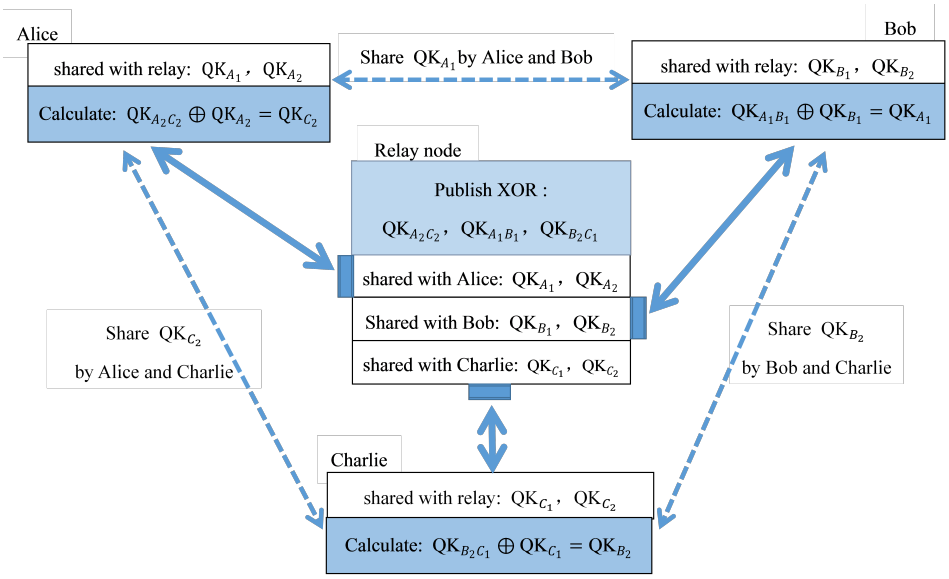

Figure 4. The QKD network scheme with three endpoints based on the public-XOR-key scheme. The solid arrow stands for the QKD process. The dotted arrow indicates the key shared by each pair of endpoints. Relay node calculates and publishes $Qk_{A_1B_1} = Qk_{A_1} \oplus Qk_{B_1}$, $Qk_{A_2C_2} = Qk_{A_2} \oplus Qk_{C_2}$, $Qk_{B_2C_1} = Qk_{B_2} \oplus Qk_{C_1}$, and then dismisses the QKD keys immediately. Finally, Alice and Bob share the key Qk_{A_1}, Alice and Charlie share the key Qk_{C_2}, Bob and Charlie share the key Qk_{B_2}.

3.3. The Advantages of the Public-XOR-Key Scheme

The function of wide area key distribution network based on relay nodes is to distribute keys for multiple endpoints. The relay nodes are set up for helping the pairs of remote endpoints to share keys. Therefore, the less functions and devices the relay nodes have, the simpler the whole system is. In real implementation, our scheme has the following practical advantages.

1. The relay nodes do not need to store the QKD keys in our scheme. In the BBN key relay scheme, each relay node recovers the plaintext with QKD keys shared with the upstream node, encrypts it with QKD keys shared with the downstream node and then transfers it to the downstream node. Once the relay nodes have been broken, the adversary can access all plaintext transferred through this relay node. The relay nodes destroy the original QKD keys securely right after the QKD keys shared with upstream node and downstream node are immediately sent to the cipher machine to do XOR operations. The adversary has no chance to access the original QKD keys or plaintext. Compared with BBN scheme, our scheme reduces the storage of QKD keys and increases the security of the system.
2. The relay nodes do not need to store the XOR results of the QKD keys secretly in our scheme. Key buffers and corresponding preventive measures are needed for the secret storage, such as anti-electromagnetic radiation devices and video surveillance system. In our scheme, the XOR results are public. The way of publishing depends on the actual network. For example, the XOR results are saved in the relay nodes without protection, sent to endpoints directly, or broadcast to the users over the network. It is difficult for the actual networks to ensure the absolute security of the data storage. The system of our scheme simplifies the defence.
3. There are no re-generation keys in our scheme. In re-encryption scheme and BBN scheme, one of the endpoints firstly generates a local random number and encrypts the random number with the help of relay nodes. Finally, the pair of endpoints shares the random number. In our scheme, the keys shared by endpoints are exactly the QKD keys and there is no need to generate random numbers from point to point.
4. In our scheme, the shared keys do not need to be encrypted by each relay node over the path. When two endpoints want to share keys in re-encryption scheme, the ciphertext of the random

number generated by one endpoint is re-encryption and transferred by one relay node after another. There are multiple endpoints to communicate simultaneously in reality. Some relay nodes may be included in plenty of communications. The communications may hang or fail due to the heavy traffic. In our scheme, the relay nodes no longer participate in the communications after publishing XOR results. When endpoints want to share keys, either of the endpoints just calculates the key directly, which eases the traffic of the relay nodes.

4. The Security of the Public-XOR-Key Scheme

We described the complex QKD network scheme with multiple endpoints and analyzed its advantages in Section 3. Compared with the re-encryption scheme that does not announce the XOR value, our scheme can improve the actual performance and simplify the complexity of the system. In this section, we analyze our scheme from the security perspective. We analyze the security of the scheme by building the threat model of adversaries and strictly demonstrate its security under the threat model. As described in Section 3.2, there is always a chain between any two endpoints in all kinds of networks. So, we can use the chain QKD network as an example and build the security model. In addition, by comparing the security of our scheme with that of the re-encryption scheme, we prove that our scheme has the same security with that of the re-encryption scheme under the same assumption of adversary's capacity, while our scheme achieves simplification in implementation.

4.1. The Security Analysis of the Public-XOR-Key Scheme

Threat model: we model the capacity of the adversary, Eve. Assume the destruction of the original QKD keys in the relay nodes is secure and Eve cannot access the original QKD keys even if she compromises the relay nodes. Assume the relay nodes never play the role as the internal attacker. QKD protocols have been proved to be unconditionally secure in theory. However, limited by the development of technology, there are attacks on QKD system in practice [28–32]. As a result of this defense, Eve cannot get all the information about QKD keys. However, there still exists some leaked information. In the chain network with n point-to-point QKD systems, the amount of leaked information may be large. Assume leaked information about each point-to-point QKD system is the same, which is denoted as I_0. The information obtained by Eve in the point-to-point QKD system is

$$I_0 \equiv 1 - H(p), \tag{10}$$

where $H(p)$ is the entropy of QKD key QK_i in each point-to-point QKD system. For $Qk_i \in \{0,1\}$, Eve knows that it has bias "0" or "1" with the probability of p. To simplify the following calculating, assume $p(Qk_i = 0) = p$ for each $i = 1, 2, ..., n$, where $0 < p < 1$.

The amount of information about the shared key Qk_1 obtained by Eve is

$$I_{key} = 1 - H(Qk_1|a_i), \tag{11}$$

where a_i is the public XOR value. A new parameter $b_i \in \{0,1\}$ is defined from the public a_i,

$$b_i \equiv a_1 \oplus a_2 \oplus ... \oplus a_i = Qk_1 \oplus Qk_{i+1}, \;\; i = 1, 2, ..., n-1. \tag{12}$$

The number of elements b_i is $n-1$ and they form a Boolean vector b. The random variable of b_i is defined as B_i, the random variable of $b \equiv (b_1 b_2 ... b_{n-1})$ is $B \equiv (B_1 B_2 ... B_{n-1})$, and the random variable of Qk_i is QK_i. $H(Qk_1|a_1)$ can be treated as $H(QK_1|B)$ for more obvious analysis. That is, the information obtained by Eve is $I_{key} = 1 - H(QK_1|B)$. From the definition of b_i, it can be seen that the QKD key Qk_1 is encrypted by other different QKD keys $n-1$ times, which is similar to the random key s encrypted by QKD keys in the re-encryption scheme.

Analyzing the security of the public-XOR-key scheme is equivalent to calculating how much information Eve obtains. We first analyze the conditional entropy of QK_1 in the threat model.

Theorem 1. *In the assumption model of key distribution network using public-XOR-key scheme, the value of the conditional entropy $H(QK_1|B)$ is*

$$H(QK_1|B) = \sum_{w=0}^{n-1} \left\{ C_{n-1}^{w} \left[p^{n-w}(1-p)^{w} + (1-p)^{n-w} p^{w} \right] H\left[\frac{p^{n-w}(1-p)^{w}}{p^{n-w}(1-p)^{w} + (1-p)^{n-w} p^{w}} \right] \right\}. \tag{13}$$

where p is the probability of $Qk_i = 0$ for all $i = 1, 2, ..., n$, and C_{n-1}^{w} is the binomial coefficient.

Proof of Theorem 1. According to the definition of conditional entropy,

$$\begin{aligned} & H(QK_1|B) \\ = & \sum_{b} p(B=b) H(QK_1|B=b) \\ = & -\sum_{b} \left[p(B=b) \sum_{Qk_1} p(QK_1 = Qk_1|B=b) \log p(QK_1 = Qk_1|B=b) \right]. \end{aligned} \tag{14}$$

Then we analyze the properties of the terms in the sum. For $Qk_1 \in \{0,1\}$, the corresponding random variable satisfies that

$$p(QK_1 = 0) = p, \;\; p(QK_1 = 1) = 1 - p. \tag{15}$$

For $B \in \{0,1\}^{n-1}$, there are 2^{n-1} values of B. Consider classifying B by the number of zeros or ones. This kind of classification is exactly the hamming weight of the B, which is creative in cryptanalysis. Then Equation (14) becomes

$$\begin{aligned} & H(QK_1|B) \\ = & -\sum_{b} \left[p(B=b) \sum_{Qk_1} p(QK_1 = Qk_1|B=b) \log p(QK_1 = Qk_1|B=b) \right] \\ = & -\sum_{w=0}^{n-1} \left[C_{n-1}^{w} p(B=b_w) \sum_{Qk_1} p(QK_1 = Qk_1|B=b_w) \log p(QK_1 = Qk_1|B=b_w) \right], \end{aligned} \tag{16}$$

where b_w denotes a particular vector with hamming weight w. According to Bayesian formula, the conditional probability of $QK_1 = 0$ in Equation (16) is

$$p(QK_1 = 0|B=b_w) = \frac{p(B=b_w|QK_1=0) \cdot p(QK_1=0)}{p(B=b_w)}. \tag{17}$$

According to the formula of total probability,

$$p(B=b_w) = p(B=b_w|QK_1=0)p(QK_1=0) + p(B=b_w|QK_1=1)p(QK_1=1). \tag{18}$$

Since $b_i = Qk_1 \oplus Qk_{i+1}$, the distribution of b_i depends on Qk_{i+1} and Qk_1. When the random variable $QK_1 = 0$, there is $B_i = QK_{i+1}$. Then

$$p(B=b_w|QK_1=0) = p(QK' = b_w|QK_1=0) = p(QK' = b_w), \tag{19}$$

where $QK' \equiv (QK_2\ QK_3\ ...\ QK_n)$ is a random variable with the length of $n-1$. The difference between the random variables QK and QK' is that QK' does not contain QK_1. Therefore, the random variables QK' and QK_1 are independent of each other and the second equality of the above equation holds. Similarly, when $QK_1 = 1$, there is $B_i = QK_{i+1} \oplus 1$. Then

$$p(B=b_w|QK_1=1) = p(QK' = \overline{b_w}|QK_1=1) = p(QK' = \overline{b_w}), \tag{20}$$

where $\overline{b} \equiv \left(\overline{b_1} \ldots \overline{b_i} \ldots \overline{b_n}\right)$, $\overline{b_i} = b_i \oplus 1$. According to Equation (18),

$$p(B = b_w) = p \cdot p(QK' = b_w) + (1 - p) \cdot p(QK' = \overline{b_w}). \tag{21}$$

When $QK' = b_w$, there is w number of ones, and $n - w - 1$ number of zeros in the random variable QK'. When $QK' = \overline{b_w}$, there are w zeros and $n - w - 1$ ones. Then

$$\begin{aligned} & p(B = b_w) \\ =& p \cdot p(QK' = b_w) + (1 - p) \cdot p(QK' = \overline{b_w}) \\ =& p^{n-w}(1 - p)^w + p^w(1 - p)^{n-w}. \end{aligned} \tag{22}$$

Therefore, the conditional probability of $QK_1 = 0$ is

$$p(QK_1 = 0|B = b_w) = \frac{p^{n-w}(1 - p)^w}{p^{n-w}(1 - p)^w + p^w(1 - p)^{n-w}}. \tag{23}$$

Similarly, the conditional probability of $QK_1 = 1$ is

$$p(QK_1 = 1|B = b_w) = \frac{p^w(1 - p)^{n-w}}{p^{n-w}(1 - p)^w + p^w(1 - p)^{n-w}}. \tag{24}$$

Then the conditional entropy $H\,(QK_1|B)$ is

$$H(QK_1|B) = \sum_{w=0}^{n-1} \left\{ C_{n-1}^w \left[p^{n-w}(1 - p)^w + (1 - p)^{n-w} p^w \right] H\left[\frac{p^{n-w}(1 - p)^w}{p^{n-w}(1 - p)^w + (1 - p)^{n-w} p^w} \right] \right\}. \tag{25}$$

□

The equivocation $H(QK_1|B)$ measures the uncertainty of the QKD key Qk_1 when given the public XOR keys. If and only if $p = 0$ or $p = 1$, the conditional entropy is null. Actually the security of point-to-point QKD systems guarantees that $0 < p < 1$. Therefore, $H(QK_1|B)$ cannot be null and Eve can never confirm the value of Qk_1. The public-XOR-key scheme is secure against the adversary under the above assumption.

4.2. Comparison of the Security of the Public-XOR-Key Scheme and Re-Encryption Scheme

We have already analyzed the security of the public-XOR-key scheme. Now we contrast its security with that of re-encryption scheme. We first model the re-encryption scheme and analyze the information obtained by Eve in the scheme, then contrast it with the result in Section 4.

The endpoint transfers the message encrypted by local random key s. We denote the cryptosystem of QKD network using the re-encryption scheme as (S, C, QK, E'', D''). A local random key s is encrypted n times with Qk_i by Alice and the relay nodes. To simplify the model, suppose the local random key, QKD keys, ciphertexts are all binary words with the length of 1. The encryption algorithm is the simplest XOR, that is

$$E''_{Qk_i}(s) = s \oplus Qk_i = c_i. \tag{26}$$

The ciphertexts c_i, for $i = 1, 2, ..., n$ are available to Eve. The assumption of the capacity of Eve about the QKD keys is the same as the decryption of the threat model in Section 4.

For a chain network, which contains n point-to-point QKD systems, the local random key s is encrypted n times with Qk_i. The QKD keys can be analyzed as a Boolean vector Qk with the length of n. The ciphertext can be analyzed as a Boolean vector c with the length of n. Let $QK, C \in \{0, 1\}^n$, $S \in \{0, 1\}$ denote the random variables of the vectors of QKD keys, ciphertexts and local random key, respectively. The equivocation of the local random key $H(S|C)$ measures the uncertainty of the local random key s when given ciphertexts. When $H(S|C)$ is null, Eve gets the random key s.

Theorem 2. *In the assumption model of key distribution network using re-encryption scheme, the value of the conditional entropy $H(S|C)$ is*

$$H(S|C)=\frac{1}{2}\sum_{w=0}^{n}\left\{C_n^w\left[p^{n-w}(1-p)^w+(1-p)^{n-w}p^w\right]H\left[\frac{p^{n-w}(1-p)^w}{p^{n-w}(1-p)^w+(1-p)^{n-w}p^w}\right]\right\}. \tag{27}$$

Proof of Theorem 2. According to the definition of conditional entropy,

$$\begin{aligned}&H(S|C)\\=&\sum_c p(C=c)H(S|C=c)\\=&-\sum_c\left[p(C=c)\sum_s p(S=s|C=c)\log p(S=s|C=c)\right].\end{aligned} \tag{28}$$

Then we analyze the properties of the terms in the sum. In order to guarantee the randomness of the local random key s, there is

$$p(S=0)=p(S=1)=\frac{1}{2}. \tag{29}$$

For the Boolean vector $C\in\{0,1\}^n$, there are 2^n values. Classify C by the hamming weight. Equation (28) becomes

$$\begin{aligned}&H(S|C)\\=&-\sum_c\left[p(C=c)\sum_s p(S=s|C=c)\log p(S=s|C=c)\right]\\=&-\sum_{w=0}^{n}\left[C_n^w p(C=c_w)\sum_s p(S=s|C=c_w)\log p(S=s|C=c_w)\right],\end{aligned} \tag{30}$$

where c_w denotes a particular vector of length n with hamming weight w. According to Bayesian formula, when $C=c_w$, the conditional probability of $S=0$ in Equation (30) is

$$p(S=0|C=c_w)=\frac{p(C=c_w|S=0)\cdot p(S=0)}{p(C=c_w)}. \tag{31}$$

Since $c_i=s\oplus Qk_i$, the distribution of c_i depends on Qk_i and s. When random variable $S=0$, there is $QK_i=C_i$. Then

$$p(C=c_w|S=0)=p(QK=c_w|S=0)=p(QK=c_w)=p^{n-w}(1-p)^w. \tag{32}$$

When random variable $S=1$, there is $QK_i=C_i\oplus 1$. Then

$$p(C=c_w|S=1)=p(QK=\overline{c_w}|S=1)=p(QK=\overline{c_w})=p^w(1-p)^{n-w}. \tag{33}$$

In Equations (32) and (33), the second equality holds because the random variables QK and S are independent of each other. According to the formula of total probability,

$$\begin{aligned}&p(C=c_w)\\=&p(C=c_w|S=0)p(S=0)+p(C=c_w|S=1)p(S=1)\\=&\frac{1}{2}p^{n-w}(1-p)^w+\frac{1}{2}p^w(1-p)^{n-w}.\end{aligned} \tag{34}$$

From Equations (32) and (34), the conditional probability of $S = 0$ is

$$p(S = 0|C = c_w) = \frac{p^{n-w}(1-p)^w}{p^{n-w}(1-p)^w + p^w(1-p)^{n-w}}. \tag{35}$$

Similarly, the conditional probability of $S = 1$ is

$$p(S = 1|C = c_w) = \frac{p^w(1-p)^{n-w}}{p^{n-w}(1-p)^w + p^w(1-p)^{n-w}}. \tag{36}$$

Therefore, the conditional entropy $H(S|C)$

$$H(S|C) = \frac{1}{2}\sum_{w=0}^{n}\left\{C_n^w\left[p^{n-w}(1-p)^w + (1-p)^{n-w}p^w\right]H\left[\frac{p^{n-w}(1-p)^w}{p^{n-w}(1-p)^w + (1-p)^{n-w}p^w}\right]\right\}. \tag{37}$$

□

In this model, the information about the Alice's random key s obtained by Eve is $I_s = 1 - H(S|C)$. Then we contrast the information leakage of the public-XOR-key scheme and re-encryption scheme.

Theorem 3. *For the adversary with the same capacity, the information leakage of re-encryption scheme and public-XOR-key scheme are the same, i.e., $I_{key} = I_s$.*

Proof of Theorem 3. Define two functions Δ and $f_p(w)$ as follows,

$$\Delta \equiv I_{key} - I_s = H(S|C) - H(QK_1|B),$$

$$f_p(w) = \left[p^{n-w}(1-p)^w + (1-p)^{n-w}p^w\right] \cdot H\left[\frac{p^{n-w}(1-p)^w}{p^{n-w}(1-p)^w + (1-p)^{n-w}p^w}\right].$$

It can be seen that $f_p(i) = f_p(n-i)$. The difference between I_{key} and I_s is

$$\begin{aligned}
\Delta =& H(S|C) - H(QK_1|B) \\
=& \sum_{w=0}^{n}\left[\frac{1}{2}C_n^w f_p(w)\right] - \sum_{w=0}^{n-1}\left[C_{n-1}^w f_p(w)\right] \\
=& \left(\frac{1}{2}C_n^0 - C_{n-1}^0\right)f_p(0) + \sum_{w=1}^{n-1}\left(\frac{1}{2}C_n^w - C_{n-1}^w\right)f_p(w) + \frac{1}{2}C_n^n f_p(n) \\
=& -\frac{1}{2}f_p(0) + \frac{1}{2}f_p(n) + \sum_{w=1}^{n-1}\left(\frac{1}{2}C_n^w - C_{n-1}^w\right)f_p(w) \\
=& \sum_{w=1}^{n-1}\left(\frac{1}{2}C_n^w - C_{n-1}^w\right)f_p(w)
\end{aligned} \tag{38}$$

Sum the ith term and the $(n-i)$th term in Equation (38),

$$\begin{aligned}
&\sum_{w=i,n-i}\left(\frac{1}{2}C_n^w - C_{n-1}^w\right)f_p(w) \\
=& \left(\frac{1}{2}C_n^i - C_{n-1}^i\right)f_p(i) + \left(\frac{1}{2}C_n^{n-i} - C_{n-1}^{n-i}\right)f_p(n-i) \\
=& \left[\left(\frac{1}{2}C_n^i - C_{n-1}^i\right) + \left(\frac{1}{2}C_n^{n-i} - C_{n-1}^{n-i}\right)\right]f_p(i).
\end{aligned} \tag{39}$$

It is easy to check that

$$\frac{1}{2}C_n^i - C_{n-1}^i = \frac{1}{2}\left(C_{n-1}^{i-1} - C_{n-1}^i\right), \ \frac{1}{2}C_n^{n-i} - C_{n-1}^{n-i} = \frac{1}{2}\left(C_{n-1}^{n-i-1} - C_{n-1}^{n-i}\right). \tag{40}$$

Therefore Equation (39) is

$$\begin{aligned} &\sum_{w=i,n-i}\left(\frac{1}{2}C_n^w - C_{n-1}^w\right) f_p(w) \\ =&\frac{1}{2}\left[\left(C_{n-1}^{i-1} - C_{n-1}^i\right) + \left(C_{n-1}^{n-i-1} - C_{n-1}^{n-i}\right)\right] f_p(i) \\ =&\frac{1}{2}\left[\left(C_{n-1}^{i-1} - C_{n-1}^{n-i}\right) + \left(C_{n-1}^{n-i-1} - C_{n-1}^{i}\right)\right] f_p(i) = \quad 0. \end{aligned} \tag{41}$$

Substitute Equation (41) into Equation (38), if n is an odd number, there is $\Delta = 0$. If n is an even number, there is

$$\begin{aligned} \Delta &= \left(\frac{1}{2}C_n^{\frac{n}{2}} - C_{n-1}^{\frac{n}{2}}\right) f_p\left(\frac{n}{2}\right) \\ &= \frac{1}{2}\left(C_{n-1}^{\frac{n}{2}-1} - C_{n-1}^{\frac{n}{2}}\right) f_p\left(\frac{n}{2}\right) = 0. \end{aligned} \tag{42}$$

Therefore, for all values of n, there is $\Delta = 0$, i.e., $I_{key} = I_s$. □

Accordingly, for the same assumption of Eve's capacity, the security of the key distribution scheme we proposed is equivalent to that of the re-encryption scheme. The public-XOR-key scheme can not only improve the practical performance and simplify the system's complexity, but also ensure that it does not reduce the security.

5. Discussion about Information Leakage of the Key Distribution Network from the Perspective of Unicity Distance

In the model of key distribution network using re-encryption scheme or public-XOR-key scheme, a secret key s or Qk_1 is encrypted with other QKD keys several times. In Shannon's ciphertext-only attack model, the plaintexts are encrypted with the same key multiple times. In this section, we analyze the practical QKD networks from the perspective of Shannon's ciphertext-only attack model, which is an in-depth discussion of unicity distance. Since the security of the re-encryption scheme is equivalent to that of public-XOR-key scheme, we only analyze one of them.

In the simplified model of re-encryption scheme with parameters (S, C, QK, E'', D''), the encryption algorithm is the simplest XOR, i.e., $E''_{Qk_i}(s) = s \oplus Qk_i = c_i$. In the model of Shannon's ciphertext-only attack model, the simplest encryption algorithm is $E_k(m_i) = m_i \oplus k = c_i$. Therefore, the local random key s could be treated as the key in Shannon's model, the QKD keys Qk_i can be treated as the plaintext in Shannon's model. The unicity distance N_0' is the number of ciphertext required to obtain the local random key s, according to Equation (8),

$$N_0' \approx \frac{H(S)}{R_L} = \frac{1}{R_L}. \tag{43}$$

The adversary Eve attacks each point-to-point QKD system. Assume the information about the value of Qk_i that Eve obtains from each point-to-point QKD system is the same, and that it is equal to $I_0 = 1 - H(p)$, where $H(p)$ is the entropy of the QKD key in each point-to-point QKD system. It seems that the physical interpretation of $H(p)$ and H_L, I_0 and R_L are equivalent. When n is sufficiently large, according to Equation (4), the relationship between $H(p)$ and the quantum keys with the length of n is

$$H(K^n) \approx nH(p). \tag{44}$$

The unicity distance N_0' of the relay QKD system is

$$N_0' \approx \frac{1}{I_0} = \frac{1}{1 - H(p)}, \tag{45}$$

which means that if Eve attacks N_0' point-to-point QKD systems and gets N_0' ciphertext, she can obtain the random key s. The contrast between the parameters of Shannon's model and those of the model of the QKD network is shown in Table 1.

Table 1. The contrast between Shannon's model and the model of the quantum key distribution (QKD) network.

Parameters	Shannon's Model	Model of QKD Network
Keys	K	S
Plaintext	M	QK
Ciphertext	C	C
Rate of language	H_L	$H(p)$
Redundancy of language	R_L	I_0
Unicity distance	$1/R_L$	$1/I_0$

However, in Sections 4 and 5 we show that the conditional entropy $H(S|C)$ cannot be null as long as $0 < p < 1$, which reflects that Eve cannot obtain the exact key s no matter how many ciphertexts she has in the real world. This result conflicts with the unicity distance that was analyzed above.

We hold the view that there are two reasons for the difference. Firstly, although $H(p)$ and H_L, I_0 and R_L have very similar physical interpretation, actually they are not equivalent. In Shannon's model, H_L denotes the rate of each word in language L, which is an average value with a sufficiently large n. In the model of QKD network, $H(p)$ is the real entropy of the QKD key in each point-to-point QKD system rather than an average value. Since each QKD key encrypts the same random key s, with the known c_i each point-to-point QKD system is not completely independent. Suppose the rate of each point-to-point QKD system is H_K,

$$H_K = \lim_{n \to \infty} \frac{H(K^n)}{n} \neq H(p). \tag{46}$$

The second reason is that the unicity distance N_0 is an approximate and minimum value in theory. In the derivation of the value of unicity distance, there are some approximations and inequalities. When n is sufficiently large, Equation (4) holds. In practical QKD network, n cannot be large enough, the value of which is usually just several dozens. Equation (8), denoting the approximation of N_0, actually is its minimum value. Even if Eve gets the ciphertext with the length of $H(K)/R_L \log_2 |M|$, there still exist spurious keys and she cannot get the real key.

Through the above analysis, we find the reasons why the unicity distance of the practical QKD network is different from that in theory. It indicates that the theoretical value of unicity distance has a certain gap with the practical system. In addition, the unicity distance of the relay QKD system is infinity, which indicates the adversary in the model can never obtain the entire secret message.

6. Discussion and Conclusions

Considering the key rate and the requirements of multiple-endpoint long-distance communication, the public-XOR-key scheme is more efficient and practical than the BBN protocol, re-encryption protocol and STR. In this paper, we extend the chain structure of the public-XOR-key scheme with two endpoints to the complex network with multiple endpoints. In the complex network with multiple endpoints, the practical contributions are as follows: (1) The relay nodes do not need to store the QKD keys. (2) The relay nodes do not need to store the XOR results of the QKD keys secretly, which reduces the storage. (3) The relay nodes do not participate in the transmission of the key, which

reduces the communication traffic to a certain extent. A particularly important contribution is the proof of the security of the scheme. On the one hand, compared with the security of re-encryption key distribution scheme whose XOR keys are not announced, the security of the key distribution scheme we proposed and the re-encryption scheme is equivalent. Our scheme can not only improve the practical performance and simplify the system's complexity, but also ensure that the security is not reduced. Even though the adversary obtains partial information about the QKD keys in our scheme, she cannot confirm the shared key. On the other hand, we discuss the information leakage of the practical key distribution networks from the perspective of the unicity distance. The unicity distance of the practical QKD network is infinity, which bears out that our scheme is secure and Eve can never obtain the shared key.

The major advantages of our scheme are as follows.

- The superiority of the practical performance: (i) The relay nodes need not store the QKD keys. Even if Eve attacks the relay nodes, she cannot access the QKD keys and plaintext. The scheme reduces the storage of QKD keys and increases the practical security of the system. (ii) The relay nodes need not store the XOR results of the QKD keys secretly, which reduces the storage. It is difficult for actual network to ensure the absolute security of the data storage. The secret storage is avoided in our scheme. (iii) There is no re-generation keys in our scheme. In our scheme, the keys shared by endpoints are exactly the QKD keys and it is no need to generated random numbers from point to point. (iv) The relay nodes do not participate in the transmission of the key, which reduces the communication traffic to a certain extent.
- The superiority of security: (i) we analyze the information leakage of public-XOR-key scheme and re-encryption scheme in the threat model and prove the security of the schemes. Even though the adversary obtains partial information about the QKD keys, she cannot confirm the shared key. (ii) We discuss the information leakage of the practical key distribution networks from the perspective of the unicity distance. The unicity distance of the practical QKD network is infinity, which bears out that our scheme is secure and Eve can never obtain the shared key. The security analysis of complex network structures are worthy for the further study.

In addition, we analyze the reason why the unicity distance of the practical system is different from that in theory. In fact, this system is a typical example of that the same plaintext is encrypted with different keys. It can be analyzed as Shannon's ciphertext-only attack model because the encryption and decryption algorithms are XOR, where the order of operations can be exchanged. The unicity distance of the systems with other complicated encryption and decryption algorithms is left as an open question for future work.

Author Contributions: Conceptualization, L.Y.; methodology, L.Y.; validation, H.D. and Y.S.; formal analysis, H.D. and Y.S.; investigation, H.D. and Y.S.; writing—original draft preparation, Y.S.; writing—review and editing, H.D.; project administration, L.Y.

Funding: This research was funded by National Natural Science Foundation of China under Grant No. 61672517 and National Cryptography Development Fund under Grant No. MMJJ20170108.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Bennett, C.H. Quantum Cryptgraphy: Public Key Distribution and Coin Tossing. In Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 10–12 December 1984; pp. 175–179.
2. Ekert, A.K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **1991**, *67*, 661. [CrossRef] [PubMed]
3. Bennett, C.H. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.* **1992**, *68*, 3121. [CrossRef] [PubMed]

4. Bruss, D. Optimal eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett.* **1998**, *81*, 3018–3021. [CrossRef]
5. Scarani, V.; Antonio, A.; Ribordy, G.; Gisin, N. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys. Rev. Lett.* **2004**, *92*, 057901. [CrossRef] [PubMed]
6. Mayers, D. *Quantum Key Distribution and String Oblivious Transfer in Noisy Channels*; Springer: Berlin/Heidelberg, Germany, 1996; pp. 343–357.
7. Lo, H.K.; Chau, H.F. Unconditional security of quantum key distribution over arbitrarily long distances. *Science* **1998**, *283*, 2050–2056. [CrossRef]
8. Shor, P.W.; Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **2000**, *85*, 441–444. [CrossRef]
9. Renner, R. Security of quantum key distribution. *Int. J. Quantum Inf.* **2008**, *6*, 1–127. [CrossRef]
10. Townsend, P.D. Quantum cryptography on multiuser optical fibre networks. *Nature* **1997**, *385*, 47–49. [CrossRef]
11. Elliott, C. The DARPA quantum network. In *Quantum Communications and Cryptography*; CRC Press: Boca Raton, FL, USA, 2005; pp. 91–110.
12. Chen, W.; Han, Z.F.; Zhang, T.; Wen, H.; Yin, Z.Q.; Xu, F.X.; Wu, Q.L.; Liu, Y.; Zhang, Y.; Mo, X.F.; et al. Field experiment on a "star type" metropolitan quantum key distribution network. *IEEE Photonics Technol. Lett.* **2009**, *21*, 575–577. [CrossRef]
13. Happe, A.; Poppe, A.; Peev, M.; Maurhart, O.; Lorünser, T.; Länger, T.; Themel, T. The SECOQC Quantum-Key-Distribution Network in Vienna. *New J. Phys.* **2009**, *11*, 075001.
14. Stucki, D.; Legré, M.; Buntschu, F.; Clausen, B.; Felber, N.; Gisin, N.; Henzen, L.; Junod, P.; Litzistorf, G.; Monbaron, P. Long-term performance of the SwissQuantum quantum key distribution network in a field environment. *New J. Phys.* **2011**, *13*, 123001. [CrossRef]
15. Chen, T.Y.; Wang, J.; Liang, H.; Liu, W.Y.; Liu, Y.; Jiang, X.; Wang, Y.; Wan, X.; Cai, W.Q.; Ju, L.; et al. Metropolitan all-pass and inter-city quantum communication network. *Opt. Express* **2010**, *18*, 27217–27225. [CrossRef]
16. Sasaki, M.; Fujiwara, M.; Ishizuka, H.; Klaus, W.; Wakui, K.; Takeoka, M.; Miki, S.; Yamashita, T.; Wang, Z.; Tanaka, A.; et al. Field test of quantum key distribution in the Tokyo QKD Network. *Opt. Express* **2011**, *19*, 10387–10409. [CrossRef]
17. 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.; et al. Field and long-term demonstration of a wide area quantum key distribution network. *Opt. Express* **2014**, *22*, 21739–21756. [CrossRef]
18. Hughes, R.J.; Nordholt, J.E.; Mccabe, K.P.; Newell, R.T.; Peterson, C.G.; Somma, R.D. Network-Centric Quantum Communications with Application to Critical Infrastructure Protection. *arXiv* **2013**, arXiv:1305.0305.
19. Gibney, E. One giant step for quantum internet. *Nature* **2016**, *535*, 478–479. [CrossRef]
20. Nordum, A. China demonstrates quantum encryption by hosting a video call. *IEEE Spectrum* **2017**, *3*, 16–19.
21. Liao, S.K.; Cai, W.Q.; Handsteiner, J.; Liu, B.; Yin, J.; Zhang, L.; Rauch, D.; Fink, M.; Ren, J.G.; Liu, W.Y. Satellite-Relayed Intercontinental Quantum Network. *Phys. Rev. Lett* **2018**, *120*, 030501. [CrossRef]
22. Liao, S.K.; Cai, W.Q.; Liu, W.Y.; Zhang, L.; Li, Y.; Ren, J.G.; Yin, J.; Shen, Q.; Cao, Y.; Li, Z.P. Satellite-to-ground quantum key distribution. *Nature* **2017**, *549*, 43. [CrossRef]
23. Elliott, C. Building the quantum network. *New J. Phys.* **2002**, *4*, 46. [CrossRef]
24. Elliott, C. Quantum cryptography. *IEEE Secur. Priv.* **2004**, *2*, 57–61. [CrossRef]
25. Schartner, P.; Rass, S. How to overcome the 'Trusted Node Model' in Quantum Cryptography. In Proceedings of the International Conference on Computational Science and Engineering, Vancouver, BC, Canada, 29–31 August 2009; pp. 259–262.
26. Stacey, W.; Annabestani, R.; Ma, X.; Lütkenhaus, N. Security of quantum key distribution using a simplified trusted relay. *Phys. Rev. A* **2015**, *91*, 012338. [CrossRef]
27. Shannon, C.E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **2014**, *28*, 656–715. [CrossRef]
28. Huttner, B.; Imoto, N.; Gisin, N.; Mor, T. Quantum cryptography with coherent states. *Phys. Rev. A* **1995**, *51*, 1863–1869. [CrossRef]
29. Fung, C.H.F.; Qi, B.; Tamaki, K.; Lo, H.K. Phase-remapping attack in practical quantum-key-distribution systems. *Phys. Rev. A* **2007**, *75*, 032314. [CrossRef]

30. Makarov, V.; Hjelme, D.R. Faked states attack on quantum cryptosystems. *J. Mod. Opt.* **2005**, *52*, 691–705. [CrossRef]
31. Zhao, Y.; Fung, C.H.F.; Qi, B.; Chen, C.; Lo, H.K. Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems. In Proceedings of the 2009 APS March Meeting, Pittsburgh, PA, USA, 16–20 March 2009; pp. 4702–4705.
32. Yang, L.; Zhu, B. Dissipation attack on Bennett-Brassard 1984 protocol in practical quantum key distribution system. *arXiv* **2013**, arXiv:1305.5744.