Key-Recycling Strategies in Quantum-Key-Distribution Networks

Xinying Li 1, Yongli Zhao 1*, Avishek Nag 2, Xiaosong Yu 1 and Jie Zhang 1

1 State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China; xixinying@bupt.edu.cn (X.L.); xiaosongyu@bupt.edu.cn (X.Y.); lgr24@bupt.edu.cn (J.Z.); Correspondence: yonglizhao@bupt.edu.cn; Tel.: (086) +010-61198108

2 The School of Electrical and Electronic Engineering, University College Dublin, Belfield, Dublin 999015, Ireland; avishek.nag@ucd.ie

Received: 11 April 2020; Accepted: 25 May 2020; Published: 28 May 2020

Abstract: Quantum-key-distribution (QKD) networks can provide absolutely secure keys for the entire communication system in theory. At present, the key-distribution rate is relatively low, and the key-distribution rate decreases exponentially as the distribution distance increases. The trusted-relay scheme commonly used in existing QKD networks achieves the purpose of extending the security distance by consuming additional keys. Since the channel is unreliable, the key-relay process will accumulate system errors to a certain extent, increasing the probability of key-relay failure. In some high-bit-error-rate network scenarios such as wireless networks and disaster environments, the channel-error rate is as high as 30%–50%. And in these scenarios, there are usually a large number of confidential messages that need to be delivered. However, the key-management mechanism of the current QKD system does not consider the scenario of key-relay failure. If the key is not successfully relayed, all the keys participating in the relay process will be destroyed, including the key that has been successfully relayed before. This situation causes the key to be wasted and reduces the encryption capability of the system. In this paper, we proposed the quantum-key-recycling (QKR) mechanism to increase the number of keys available in the network and introduced a secure service grading mechanism to properly reuse the recycled keys. The QKR mechanism can be regarded as a key-management mechanism acting on the point-to-point QKD system, and the mechanism is designed for a classical channel to reuse the key resources. A post-processing method for recycled keys is proposed to improve the security of the keys. Simulation results show that the QKD network using the key-recycling strategy is about 20% higher in key-utilization rate than the traditional QKD network without the QKR mechanism, and about 10% higher in-service security coverage.

Keywords: Quantum key distribution (QKD); quantum key recycling; service security level

1. Introduction

With the development of technologies such as 5G, big data, and cloud computing, large amounts of data need to be generated, sent, and stored every day [1]. These data include sensitive personal finances, health information, and business and state secrets. Once the data is leaked, it will cause an unpredictable loss. In conventional encryption systems, data security relies on the cryptographic algorithms, public-key and symmetric, based on computational complexity.
However, the emergence of quantum computers will allow breaking currently used public-key cryptosystems and thereby put an end to the secure distribution of business secrets, banking information, health data, and so on, over the Internet.

Even though the current quantum-computing technology is immature, the data related to census, military technology, and other sensible information must be kept secret from the eavesdropper. The eavesdropper can wait for the arrival of the quantum computing by “saving at first and then decrypting”. QKD makes full use of the advantages of quantum mechanical signals’ no-cloning theorem and uncertainty principle, which makes it impossible for an eavesdropper to keep a transcript of quantum signals sent in a QKD process. Therefore, it is a promising method to distribute a cryptographic key, which can be used in conjunction with one-time pad (OTP) for absolutely secure communication theoretically, between a legal sender and a receiver without making assumptions on the computational power of a potential eavesdropper [2–5].

A separate point-to-point QKD link does not support some applications very well, and therefore, QKD network structures must be considered in order to enable access by a greater number of users and also to extend the reach and geographical coverage [6]. However, point-to-point quantum-key-generation rate is limited by distance. Some schemes are designed to extend the distance of secure QKD [7,8]. Among them, the trusted-relay scheme is the easiest and most convenient, and has been used as a standard for existing QKD networks [9,10].

Some studies are carried out based on the trusted-relay QKD network. By constructing a quantum key pool (QKP) to allocate and manage quantum keys, the optimizations of survivability [11], cost [12,13], and resource utilization [14] in QKD networks have been realized. However, research on QKP management always focuses on how to use the keys that are relayed successfully, and rarely cares about the keys that are in the failed relay process. In terms of key recycling, some researches focus on the reuse of authentication keys in quantum channels [15] and theoretically prove the security of the keys recycled [16]. The QKR mechanism based on QKD is a classical protocol, and the existing classical-channel security [17] and intrusion-detection technology [18] cannot guarantee that the signals be immune to eavesdropping. However, quantum channels can theoretically detect all eavesdropping behaviors, which is very different from the classical channels. Therefore, the keys recycling in the classical channel cannot directly reuse all the recycled keys.

In this paper, we focus on how to manage, recycle, and securely reuse keys that are failed to be relayed under abnormal circumstances. The main contributions in this work are three-fold: (1) The idea of recycling the relay key is proposed, and a QKP communication mechanism based on QKD-over-optical-network architecture is proposed to synchronize algorithm information; (2) The types of keys that can be recycled are defined, the QKR mechanism and three specific implementation algorithms are proposed and the service-security-classification method is adopted to use different keys for different security needs of the service; and (3) The simulation shows that the QKD system with QKR is superior to the QKD system without QKR mechanism in terms of key-utilization rate and service-security coverage.

The rest of this paper is organized as follows. Section 2 introduces some related technologies and the basis of the key-recycling mechanism. Section 3 describes the problem. Section 4 gives the basic settings and related notations. Three QKR mechanisms are proposed and described in Section 5 and the performance evaluation and analysis for the QKR mechanisms are discussed in Section 6. Section 7 concludes this study.

2. QKD Networks with QKP

This section focuses on some key technologies that support QKD networks. First, a classic point-to-point QKD scheme is presented. Then, based on the objective to increase the key rate, an easy-to-implement QKD distance-extension scheme is introduced. Finally, the QKD-over-optical-network
architecture is revealed, and the quantum-key-pool negotiation mechanism is proposed on the architecture.

2.1. Point-to-Point QKD System

The four-state protocol originally proposed by Bennett and Brassard in 1984, called BB84 [19], is marked as the beginning of the development of QKD technology and most widely implemented in the world. As shown in Figure 1, in the BB84 protocol, Z base is composed of $|H\rangle$ and $|V\rangle$ ($Z = |H\rangle\langle H| + |V\rangle\langle V|$) and X base is composed of $|+\rangle$ and $|-\rangle$ ($X = |+\rangle\langle +| + |-\rangle\langle -|)$. Therefore, if the Z-base is used to measure $|H\rangle$ and $|V\rangle$, a definitive result will be obtained, while the measures $|+\rangle$ and $|-\rangle$ will lead to uncertain results. Based on the above principles, the main part of BB84 protocol is described in the following three steps.

2.2.1. Modulate bit to qbit

Alice selects two sets of binary random sequences and perform corresponding quantum state preparation according to the values of two sets of random numbers. One of the random sequence named raw keys determines the classical bits corresponding to the modulated quantum state as denoted by step (1) in Figure 1. Another random sequence, called named base sequence, determines which base the modulated quantum state belongs to, such as 0 for the Z base and 1 for the X base (step 2). For example, when the classical bit is 0, it is modulated to $|H\rangle$ or $|\rangle$, and when the classical bit is 1, it is modulated to $|V\rangle$ or $|\rangle$. Alice transmits a prepared single photon sequence to Bob through the quantum channel (step 3).

2.2.2. Measuring qbit

Bob uses a single photon detector to receive quantum signals on the quantum channel and measures quantum polarization states independently. Bob generates a sequence of random numbers called named base sequence B, which determines the measurement base according to its value. Similar to the mechanism of base sequence A, when the value is 0, the X base is selected by Bob to measure the quantum state, and when the value is 1, the Z base is selected (step 4). After the measurement, Bob records the photon polarization state of each measurement and its corresponding bit information. When the measurement result is $|H\rangle$ or $|\rangle$, the classic bit is 0, and when the measurement result is $|V\rangle$ or $|\rangle$, the classic bit is 1 (step 5). Due to the inevitable attenuation problem of the quantum channel and the detection deviation of the device, the number of quantum states received and measured by Bob may not necessarily equal to the number of quantum states sent by Alice. A clock channel is needed here to achieve the accurate synchronization of the qubit transmission and reception.

2.2.3. Matching base

Alice and Bob match the bases in the public channel, then discard the corresponding bits when the code base and measurement are different (steps 6 and 7). On average, Alice and Bob will have about half the length of the original bit sequence, because the probability of Alice and Bob using a different polarization base is 1/2.

At this time, the random sequence shared by Alice and Bob is a rough quantum key (8), and after a series of post-processing steps, such as error estimation, error correction, and secret amplification, a sequence of secure keys are obtained.
2.2. Trusted Repeaters for Distance Extension

In 2002, Elliott et al. proposed the idea of using trusted nodes for quantum-key-distribution networking [20]. On the basis of the point-to-point QKD system, the “one-time-pad” cryptographic algorithm is used to realize the key distribution of both parties in the long-distance communication through the “hop-by-hop” encryption method. At present, many quantum-key networks based on key relay have been built in countries around the world. In 2008, the European countries established the famous SECOQC (secure communication based on quantum cryptography) network. In 2010, Japan established a six-node QKD network in Tokyo. China has also established several quantum-key networks, and the world’s first wide-area quantum key network - "Beijing-Shanghai trunk line" also uses key-trusted repeaters to generate end-to-end keys.

The specific implementation process is shown in Figure 2. Alice and Bob need to share the key $K_A$ on the premise that the point-to-point key distribution is completed. First, key sequences $K_a$ and $K_b$ are shared by Alice-trusted relay pair and Bob-trusted relay pair, respectively (step ①). Then a bit-by-bit exclusive-or (XOR) with $K_a$ and $K_b$ is executed at the trusted relay node. The encrypted bit sequence is sent to Bob (step ②). Finally, Bob receives the bit sequence and decrypts it using $K_b$. $K_A$ was shared by Alice and Bob successfully (step ③). Since the relay node also knows the $K_A$ when relaying, the relay node is required to be trusted. Subsequently, schemes such as bit transmission, random routing, multipath transmission, and XOR storage are proposed to reduce or even eliminate the requirement for node credibility.

![Figure 1. Point-to-point quantum-key-distribution (QKD) mechanism based on the four-state protocol originally proposed by Bennett and Brassard in 1984 (BB84)](image)

![Figure 2. Trusted relays are used to extend QKD distance and ultimately generate end-to-end quantum keys.](image)

2.3. QKD over Optical Network Architecture

The photonic network is an emerging infrastructure of optical communication similar to the IP-over-optical networks. According to the QKD key technology, QKD-over-optical network...
architecture is depicted in Figure 3. According to the supply and demand relationship of the key, the whole architecture is logically divided into a key-supply part (blue area) and a key-consumption part (yellow area).

![Figure 3. QKD over Optical Network Architecture.](image)

The key-supply part is divided into QKD plane and key management plane from bottom to up. The QKD plane consists of optical links and quantum nodes that integrates one or more sets of quantum transceivers, and the channel type is QCh. The point-to-point QKD protocols such as BB84, GG02, MDI runs on the plane to provide point-to-point quantum keys for the upper layer. In key management plane, the quantum key pool (QKP) acts as a node, and its physical implementation can be thought as a server that stores and manages keys deployed on the nodes. Nodes are fully connected through the logical channels which are based on classic data channels. The quantum key is stored in the QKP in the form of binary bits. The key-management plane provides end-to-end quantum keys for the upper layer by means of hop-by-hop relay routing. The PCh required by the QKD plane and key management plane in this architecture is provided by the data channel (DCh) of the key-consumption part.

The key-consumption part is divided into Optical network and IP network from bottom to up. The optical network is a WDM network and the nodes are facilitated with optical cross-connects (OXC)s with wavelength switching capabilities. In the IP network, the router is connected to the OXC directly, so the services can be dealt with all-optical processing. Therefore, if the quantum node is deployed on the OXC, the QKD network will provide the secure keys for both the IP network and the optical network [21,22].

3. Problem Statement

The relaying process of quantum keys can be implemented by transmitting information through a public data channel. As shown in Figure 4, Alice and Bob need to share the keys by using the trusted relay, where the Alice-Repeater pair and the Repeater-Bob pair have shared the keys $K_{Ai}$ and $K_{Bi}$ ($i, j \in N$), respectively. Due to the differences in the relay-routing algorithm, the keys $K_{Ai}$ and $K_{Bi}$ may have separately experienced different numbers (the number may be 0) of trusted-relay nodes before sharing to the Repeater. According to the trusted-relay and the one-time-pad principle, in order to share one united end-to-end key, each node that is selected by the relay route will consume the same number of point-to-point keys. It is assumed that if the length of $K_{Ai}$ is $n$ and the Alice-Repeater pair needs to pass through two trusted relay nodes, sharing the $K_{Ai}$ between the Alice-Repeater pair will
require an additional 2n keys. KA1 is generated by Alice and the first relay node for point-to-point QKD. The key-relay process consumes a large number of keys, and the number of keys consumed is positively correlated with the number of relay nodes.

![Diagram](image)

**Figure 4.** In the case of multi-hop relay, when a certain relay fails, the problem caused by the traditional QKD scheme.

If Alice and Bob want to share the key pair KA1, firstly KA1 XOR KB1 is executed at the trusted relay (step ①) and then the XOR-ed result is sent to Bob. Packet loss and bit errors in actual operational IP networks may occur due to different factors like, rerouting, network congestion, cache processing, the device’s actual performance, network environment, and other factors. Packet loss (step ②) or bit error (step ②’) occurs while the key is being relayed, which may result in the key not being successfully shared. When the key KA1 is not successfully distributed, a redistribution process is performed. The key redistribution process is similar to the former process. Because the failure of the key-relay process may be caused by the eavesdropper’s activity or malicious attack. When the redistribution process occurs, in order to ensure the absolute security of the keys that need to be shared (to meet the condition that the key is used only once), the key pairs KA1 and KB1 that got successfully relayed before the current QKD, must be destroyed. The new key pairs KA2 and KB2 are used to re-relay (step ③④). The new key KA2 is shared between Alice and Bob. However, the practice of discarding the key pair KA1 and KB1 directly results in a great waste of the keys, not only the keys KA1 and KB1 are wasted, but also the relay keys used in the relay process are wasted. Further, the network key demand is increased, and the security requirements of the service are difficult to guarantee. Therefore, the idea of key recycling is proposed that collects and processes the keys that failed in similar scenarios discussed above, and reuses those keys to encrypt the services with low security level.

The probability and characteristics of packet loss and bit error are different in different network scenarios. The typical two scenarios are satellite networks and optical networks, representing networks with the characteristics of high packet loss rate (PLR) and low PLR, respectively [23–26].

The PLR in the scenario of satellite relay is as high as 30% or higher [27,28], and the QKR strategy has natural advantages in high bit error ratio (BER) scenarios. The lower PLR in optical packet switched networks is generally between 1/10,000 and 1%, [26] but it does not mean that the key-recycling strategy is not useful in this scenario. The necessity of key recovery mechanism in optical network (low BER and PLR) scenarios is analyzed from three perspectives. First, when a symmetric-encryption algorithm is used to encrypt a service, a hundred-bit key can encrypt a Gbit service, spanning seven orders of magnitude. The amount of data that can be encrypted by the wasted key is defined as follows:

\[
N_{data} = \left( V_{QKD} * P_{PLR} * \tau \right) / L_{key} * T * V_{data}
\]  
(1)
Where $V_{QKRs} \cdot P_{PLR} \cdot t$ is the amount of key wasted in time $t$, $L_{key}$ is the key length of the encryption algorithm, $T$ is update period of the key and $V_{data}$ is transmission rate of the service in the network. When $V_{QKD} = 10$ Mbps, $P_{PLR} = 1/10,000$, $L_{key} = 192$ bit (192 AES), $T = 1$s, $V_{data} = 1$ Gbps, we can estimate the amount of keys wasted every second is 1 kbit, which can guarantee the secure transmission of 1 G services for about 5 s. Second, in the optical networks, there are special cases such as rerouting caused by network failures and large-scale disasters, which are characterized by a sudden increase in BER and PLR and a large number of nodes. The QKR scheme can be used as a contingency plan in an emergency to alleviate the shortage of end-to-end key generation. Third, the application of the QKR strategy can reduce the requirements of the key-relay process on the network environment and network reliability, thereby reducing the maintenance cost of the operator.

4. Network Model and Protocol

In this section, we begin by providing the model of the QKD-over-optical network considered in this paper. Then, we describe the QKP communication mechanism as a communication protocol between QKPs to synchronize the key recycling strategy and ensure the timing of the recycled key sequence.

4.1. Network Model

The network model is described as follows: the QKD-over-WDM network is represented by a graph $G(V, E)$, where $V$ denotes the set of service nodes which are deployed with QKP and $E$ denotes the set of optical links including QCh and DCh, $(i, j) \in E$. The cost of a link denoted by $W_{(i, j)}$ depends on the length of the link denoted by $L_{(i, j)}$ and the placement interval of trusted-relay nodes denoted by $L_r$. $W_{(i, j)}$ can be expressed as:

$$W_{(i, j)} = \lceil L_{(i, j)}/L_r \rceil$$

Symbol $\lceil \cdot \rceil$ indicates ceiling function, that is, the smallest integer larger than the number in the symbol.

We assume that QKD can save and manage end-to-end keys but can only generate point-to-point keys at a certain rate through direct links $(i, j)$. Table 1 lists the notations and their definitions used in this paper.

| Notations | Definitions | Notations | Definitions |
|-----------|-------------|-----------|-------------|
| Ser $(V_{s,d}, R_{key}, L_{s,d}, b_{sd})$ | Data service request | $R_{sec}$ | Encryption level of the service |
| QKD $(V_{s,d}, L_{s,d}, P_{failure}, T_p)$ | QKD service request | $N_{rank}(k)$ | The number of keys consumed per unit time when the encryption level is $k$ |
| $N_{key,relay}$ | The number of point-to-point key generations per unit time | $L_{s,d}$ | The starting time for each data/QKD service |
| $K_{key}$ | The ratio of the original key to the key to be recycled | $b_{sd}$ | The hold time of the data service |
| $T_p$ | The type of key recycling | $N_{key,relay}$ | Number of keys that QKD service needs to relay |
| $V_{s,d}$ | The current number of key in the QKP | $P_{failure}$ | Probability of failure of QKD subprocess |
| $V_{s,d}$ | Pair of source node and destination node | |

4.2. QKP Negotiation Mechanism

In order to ensure the realization of the QKR mechanism, communication among key pools is inevitable. Therefore, based on the QKD-over-optical-network architecture a new QKP negotiation
mechanism is proposed. Some possible situations are illustrated in Figure 5, which shows the communication process among the four nodes. Each node contains a key pool, which stores the keys of different source and destiny nodes.

![QKP communication process when key relay is successful](chart1)

![QKP communication process when key relay is failure](chart2)

**Figure 5.** Quantum key pool (QKP) communication mechanism in two cases: relay success and failure.

During the key relay process, all relay nodes need to perform three operations when they receive the encrypted key. First, whether there is a transmission error is checked. Then the relay key is decrypted and cached locally. Finally, the key that needs to be relayed is encrypted and forwarded to the next hop node. When the key is successfully relayed to the destiny node, the destiny node performs the following two operations. First, it sends a relay success message to the source node and modifies the source and destiny node information of the successful relayed key. Then it broadcasts the 'delete cache' message to all relay nodes participating in this key-relay process. Information such as the serial number and size of cached keys is included in the 'delete cache' message. This information can be used to locate the key that needs to be deleted. The relay node that receives the broadcast message deletes the corresponding cached key. When a node detects a transmission error, it sends an error message to the previous hop node. The node receiving the error message checks the key-recycling characteristics. Recycling features include whether the QKR mechanism can be used and which QKR algorithm can be used. The node sends control instructions to other nodes to recycle the key according to the obtained recycling characteristics.

To meet the information sharing and operation control between key pools, two types of messages are designed as shown in Figure 6. The function of the broadcast message is to delete the cached key in batches, including seven parts, which are source address, destiny address, key group, key serial number, and key size, including destiny address and delete cache. Key group indicates the node pair to which the key belongs. Key serial number indicates the serial number of the key in the key group. Key size indicates the number of keys. When the include destiny address bit is 1, it indicates that all caches from the source node to the destiny node are deleted. When it is 0, it indicates that the source and destiny node keys are retained and other cache keys are deleted.
cache is 1, the cache is deleted. Ordinary message is the message format used in key relay. Recycle type indicates the type of key recycling, 00 indicates that key recycling is not supported. Routing hops record the number of times the key passes from the source node to the destiny node. Routing hops and key value will change with the increase of the number of relays, and will eventually be used for the key-recycling decision.

**Broadcast message**

| Source address | Destiny address | Key group | Key serial number | Key size | Include destiny address | Delete cache |
|----------------|----------------|-----------|-------------------|---------|-------------------------|-------------|

**Ordinary message**

| Source address | Destiny address | Key group | Key serial number | Key size | Recycle type | Routing hops | Key value | Text |
|----------------|----------------|-----------|-------------------|---------|--------------|--------------|-----------|------|

**Figure 6.** QKP communication message format: broadcast message format and ordinary message format.

**5. QKR Mechanism and Strategy**

Figure 7 depicts the QKR algorithm and the state changes of the QKPs. A, C, and D are QKPs deployed on nodes A, C, and D respectively. Path A→F→C→D may be selected to serve the A–D node pair to share a key sequence. When the C→D relay process fails, the initial state of the key pool is as follows: QKP A and D, respectively, have two key sequences belonging to the A–C node pair and the C–D node pair. And there are four key sequences in QKP C, two of which belong to the A–C node pair and another two key sequences belonging to the C–D node pair. There are three types of recycling methods: partial recycling, all recycling, and mixed recycling.

The partial-recycling algorithm selects a pair of key sequences between the A–C key pair and the C–D key pair to recycle according to some decision factors, including the value of the key, the degree of the node pair, and so on. And the sequence of key pair that was not selected will be destroyed.

The all-recycling algorithm is to recycle both parts of the key, and then perform some post-processing operations on the recycled key such as mixing and transformation. However, this algorithm will bring additional consumption of the original key.

The mixed-recycling algorithm can achieve the balance between the security of the recovery key and the normal encryption of the original service. The mixed-recycling algorithm analyzes the historical data of the service and selects one from the partial recycling and the all-recycling algorithms, according to the characteristics of the historical service.

**Figure 7.** QKR mechanism and three recycling methods: a) partial recycling, b) all recycling, and c) mixed recycling.
5.1. Partial Recycling

As shown in the Algorithm 2 in Table 2, when a data service arrives, a QKD service is generated, and then the key-relay path $P_{set}$ is generated by the Dijkstra algorithm. When the relay process proceeds to node_current, the relay process fails, that is, the 'node_begin-node_current' key pair encrypted by the key pair 'node_current-node_next' cannot be decrypted successfully at node_next. However, at this time, we do not know whether the relay failure process is caused by the eavesdropper's activity, and we either do not know whether the eavesdropper successfully obtained both the 'node_begin-node_current' and 'node_current-node_next' keys.

Table 2. Algorithm 1: Quantum Key Mixed Recycling.

| Input: G (V, E), Sref(Vs-D, Rsec, Ts,s, Thd), QKD(Vs-D, TQ, Nkey_relay, Pfailure, Tp), Vkey_gen, Nrank(K), Kcur |
| Output: security coverage rate of service, key utilization rate, average security index of service |

| 1: For each data service Ser (Vs-D, Rsec, Ts,s, Thd) | 12: Call Algorithm 2; |
| 2: Generate QKD (Vs-D, TQ, Nkey_relay, Pfailure, Tp); | 13: Else if the min of Nkey (i, j) > the mean of Nkey_relay(Rsec=2) && the mean of Rsec = 3 |
| 3: Storage Nkey_relay and Rsec of the service | |
| 4: For each QKD service | 14: Call Algorithm 3; |
| 5: If Nkey_relay <= Nkey (s, d) | 15: Else if the variance of Nkey_relay(Rsec=2) > thv |
| 6: The service is encrypted; | |
| 7: Else | 16: Call Algorithm 3; |
| 8: Pset ← routing computation with D algorithm; | 17: Else |
| 9: If Pfailure = 0 | 18: Call Algorithm 2; |
| 10: QKD process is successful; | 19: End if |
| 11: Else if the min of Nkey (i, j) < the mean of Nkey_relay(Rsec=2) && the mean of Rsec = 2 | 20: End if |
| 21: End for |
| 22: End for |

Algorithm 2: Quantum Key Partial Recycling

| 1: Calculate KV; | 4: Else |
| 2: If KVb-c >= KVc-n | 5: Recycle key number(c,n) = Nkey_relay; |
| 3: Recycle key number(b,c) = Nkey_relay; | 6: End if |

Algorithm 3: Quantum Key All Recycling
1: Query the current value of \( N_{key}(b,c) \) and \( N_{key}(c,n) \);  
9: \( N_{key}(c,n) = K_{or} \ast N_{key}(c,n) \);

2: If \( K_{or} \ast N_{key,relay} \geq N_{key}(b,c) \)  
10: Recycle key number \((c,n)=(1+K_{or}) \ast N_{key}(b,c)\);

3: \( N_{key}(b,c) = K_{or} \ast N_{key}(b,c) \);  
11: Else

4: Recycle key number \((b,c)=(1+K_{or}) \ast N_{key}(b,c)\);  
12: \( N_{key}(c,n) = K_{or} \ast N_{key,relay} \);

6: \( N_{key}(b,c) = K_{or} \ast N_{key,relay} \);  
13: Recycle key number \((c,n)=(1+K_{or}) \ast N_{key,relay} \);

7: End if  
14: End if

8: If \( K_{or} \ast N_{key,relay} \geq N_{key}(c,n) \)

\[ S—source, \, d—destination, \, b—\text{begin}, \, c—current, \, \text{and} \, n—next. \]

It is undoubtedly unsafe to directly recycle two pieces of keys at the same time. In this case, if the partial-recycling algorithm is used, it is necessary to define a parameter denoted by \( KV \) called 'key value' to evaluate which segment of the key needs to be recycled, which is expressed as:

\[
KV_{sd} = \sum_{i=s; \, j \neq s, \, j \neq \text{next} \atop d \rightarrow \text{pre}, \, j=d} W_{(i,j)}, (i, j) \in P_{se}
\]

(3)

The more relay nodes a key pair pass, the more relay keys are consumed, and therefore, the more the key pairs pass through the number of relay nodes, the more precious it is. Therefore, it is obviously wise to recycle the key pair with a high key value and destroy the other pair.

The advantage of this algorithm is that it has less impact on other services with encryption requirements, the recycling process is easy to implement, and the security of the recovery key is less dependent on the design of the algorithm. The disadvantage of this algorithm is that the security of the recovered key is low and some of the keys are not recycled.

Partial-recycling algorithm calls Dijkstra's algorithm once and then performs a summation calculation with complexity \( O(1) \). Thus, Partial-recycling algorithm has a complexity of \( O(V^2) \).

5.2. All Recycling

In order to improve the security of the recovery key and recover as many keys as possible, the quantum key all-recycling algorithm is designed as shown in Algorithm 3 of Table 2. In order to guarantee the security of the recycling key, the original key needs to be mixed into the recycling key. So, the first step of this algorithm is to set the mix ratio denoted by \( K_{or} \) and look up the capacity of the current original key. Then, according to the relationship:

\[ N_{key\_original} = K_{or} \ast N_{key\_recycled} \]

(4)

where the maximum number of keys that can be recycled can be calculated. Finally, the algorithm recycles the key and performs post processing.

The post-processing phase disorders the recycled keys by linear adjustment or non-linear mapping to improve the security of the recycling key. Therefore, the security of the post-processing algorithm determines the security of the quantum key recycling algorithm and the post-processing algorithm brings the cost of the recovery algorithm to the use of the original key. The S-box has the following three characteristics: Each row of the table can traverse all possible values. Changing an input bit, changes at least two output bits, and the input and output are statistically independent.
Therefore, in this paper, the design method of the S-box in the data encryption standard (DES) algorithm is used as a post-processing method for recycling the keys [29,30]. It is important that the two key pools that manage a pair of keys must perform the same post-processing strategy.

Post-processing is divided into three steps as shown in Figure 8. Step 1: The key is mixed, and a certain proportion of the original key is inserted into the recycling key sequence according to the predefined insertion rules. Step 2: Extend the key mix sequence according to the rule of extended permutation table (2). Each 4-bit key is divided into a group (dark yellow area in the dotted line), and then a bit is added at the beginning and the end of the key group (light yellow area outside the dotted line). Step 3: The extended key sequence is nonlinearly compressed according to the rules of the S-box (3).

![Figure 8. QKR post processing algorithm.](image)

The advantage of the algorithm is that all keys are recycled as much as possible and the security of the recycled keys is high. The disadvantage of the algorithm is that the security of the recycled keys is mainly dependent on the design of the post-processing algorithm. And the post-processing algorithm may introduce the consumption of the original key, which may result in the original high-security-level service being unable to be encrypted.

The complexity of the all-recycling algorithm is mainly due to the call of Dijkstra’s algorithm and a post processing algorithm. The former can be achieved at a complexity of O (V²), and the latter has a complexity of O (Nkey), where Nkey is the number of keys being recycled. Thus, all-recycling algorithm has a complexity of max [O (V²), O (Nkey)].

5.3. Mixed Recycling

The mixed QKR algorithm is proposed to maximize the average security of the service without affecting the original high security level of the service. As shown in Algorithm 1 of Table 2, the joint parameters obtained by analyzing historical traffic characteristics and used for adaptive selective-key-recovery algorithms are \( R_{sec} \), \( N_{key\_relay} (R_{sec} = 2) \), and \( \sigma_{N_{sec\_relay}} (R_{sec} = 2) \), respectively. \( x \) services before the current failed service are analyzed, where \( x \) is the number of historical data. \( \sigma_{N_{sec\_relay}} (R_{sec} = 2) \) represents the weighted average security level of the service. a, b, c, and d are weighting coefficients. The closer the arrival time of the service is to the current time, the greater the weight.
\[ N(k) = a \sum_{i=0}^{\frac{k}{4}-1} \text{Ser}(i, R_{\text{sec}} = k) + b \sum_{i=\frac{k}{4}}^{\frac{k}{2}-1} \text{Ser}(i, R_{\text{sec}} = k) + \\
\frac{1}{x} \sum_{i=x/4}^{\frac{k}{2}-1} \text{Ser}(i, R_{\text{sec}} = k) + d \sum_{i=x/4}^{k-1} \text{Ser}(i, R_{\text{sec}} = k) \]  

(5)

\[
\overline{R_{\text{sec}}} = \begin{cases} 
2, & \text{if } N(k = 2) > N(k = 3) \\
3, & \text{otherwise} 
\end{cases}
\]  

(6)

\[ \overline{N_{\text{key}_\text{relay}}(R_{\text{sec}} = 2)} \] represents the average demand for keys for a service with a security level of two in the history.

\[ \overline{N_{\text{key}_\text{relay}}(R_{\text{sec}} = 2)} = \frac{x}{x} \sum_{i=0}^{x} N_{\text{key}_\text{relay}}(i) / x \]  

(7)

\[ \sigma_{N_{\text{key}_\text{relay}}(R_{\text{sec}} = 2)} \] represents the variance of the key demand for the service with security level two.

\[ \sigma_{N_{\text{key}_\text{relay}}(R_{\text{sec}} = 2)} = \sqrt{\frac{1}{x} \sum_{i=0}^{x} (N_{\text{key}_\text{relay}}(i) - \overline{N_{\text{key}_\text{relay}}})^2} \]  

(8)

The interplay between Algorithm 2 and Algorithm 3 can be changed by adjusting the calculation method and weighting coefficient of related parameters. The essence of the algorithm is a compromise algorithm, which relies on the analysis of historical services and adaptively makes the optimal recycling decision for the current network. Subsequent algorithm optimization can start with historical business analysis.

The complexity of the mixed-recycling algorithm consists of the analysis of historical services and the maximum complexity between Algorithm 2 and 3. To analyze historical services one needs to traverse the historical services twice, of which total amount is \( N_{\text{hist}_\text{ser}} \). Algorithm 2 has a complexity of \( O(N_{\text{hist}_\text{ser}}) \), and the complexity of Algorithm 3 is \( O(V^2) \). Thus, mixed-recycling algorithm has a complexity of \( \max\{O(N_{\text{hist}_\text{ser}}), O(V^2) + O(N_{\text{key}})\} \).

6. Performance Evaluation and Analysis

In order to evaluate the performance of the key recovery algorithms, 14-nodes national science fund network (NSFNET) topology is used in simulation, as shown in Figure 9. The costs of the links are related to the values of \( L_r \).

![NSFNET topology with 14 nodes](image)

Figure 9. NSFNET topology with 14 nodes, which is the network topologies used in simulation.

The classification and characteristics of the services in the simulation are shown in Table 3. Among the different service types, only low security level services can be encrypted using the recycled key in order to ensure the security quality. And when both the original key and the recycled key satisfy the encryption requirements of the service, the recycled key is used preferentially.
Table 3. Characteristic of Service.

| Rsec | Service Type         | Key Type      | Encryption Algorithm |
|------|----------------------|---------------|----------------------|
| 1    | QKD service          | Original key  | One time pad          |
| 2    | High security level service | Original key | 192bit AES            |
| 3    | Low security level service | Recycled key | 192bit AES            |
| 3    | Low security level service | Original key | 128bit AES            |

Table 4 shows the relative security factors for different types of keys. From the perspective of the source of the key, the original key is generated directly by QKD, so the original key is the safest and should be set to 1 compared to the recycled key. Part of the mixed-recycling key comes from the all-recycling key, and the other part comes from the partial-recycling key, so its relative security factor should be between the all-recycling-key security factor and the partial-recycling key security factor. The specific value is related to the decision ratio of the mixed-recycling algorithm.

Table 4. Relative Security Factor of the Key.

| Key Type      | Original Key | All Recycling | Mixed Recycling | Partial Recycling |
|---------------|--------------|---------------|-----------------|-------------------|
| Relative security factor | 1 | 0.9 | [0.9, 0.06] | 0.6 |

In order to reflect the value and cost of the QKR algorithm, the simulation results are divided into two categories. The first category expresses how the QKR algorithm optimizes the QKD network by showing the impact of different service failure rates (SFRs) and demonstrates the cost of deploying the QKR algorithm by showing the relative security level. The second category shows how the different algorithms are affected by the ratio of different security requirements and the rate of key generation. It also shows the balance of the algorithms and provides ideas for further optimization.

6.1. Comparative Analysis about Whether QKR Mechanism is Employed

Key utilization rate (KUR) and security coverage rate of service (SCR) were established as two indicators to evaluate QKD network performance. Key utilization rate indicates the ratio of the key used by the business to the total key amount, which is expressed as:

\[ KUR = (N_{key\_used} + N_{key\_leftover}) / N_{key\_generated} \] (9)

\( N_{key\_used} \) indicates the number of keys successfully used by the service. \( N_{key\_leftover} \) indicates the key stock of QKP at the end of the simulation and \( N_{key\_generated} \) represents the amount of key generation for the entire run cycle of the simulation. Security coverage rate of service indicates the ratio between the number of services that the encryption requirement has satisfied and all services with encryption requirements, and is expressed as:

\[ SCR = N_{ser\_encrypted} / N_{ser} \] (10)

\( N_{ser} \) indicates the total amount of service with security requirements. \( N_{ser\_encrypted} \) indicates the number of services that were successfully encrypted.

Figure 10(a) shows the trend of KUR and SCR with different service intensity (inflow of service per unit). It is obvious that regardless of the value of the service intensity, the KUR and SCR of the network are far superior to the algorithm without the QKR strategy than when using the QKR strategy. With the increase of service intensity, whether or not the QKR strategy is
adopted, KUR is declining. Furthermore, the partial-recycling algorithm always stays ahead. On the other hand, the change in service intensity has no significant impact on the SCR for the algorithm of no recycling. However, as the service intensity grows, the SCR indicator of the key recycling algorithm is also growing.

Figure 10(b) indicates that the effect of SFR increase on KUR and SCR under all recycling, partial recycling, mixed recycling, and no-recycling algorithms. In the case of different SFRs, the three key-recycling algorithms are better than no recycling in both KUR and SCR.

![Figure 10](image)

**Figure 10.** (a) The impact of service intensity on key utilization rate (KUR) and security coverage rate of service (SCR) of QKD networks with different QKR mechanisms and traditional QKD networks, when \( V_{\text{key,gen}} \) is 120 and service failure rate (SFR) is 30%. (b) The impact of SFR on KUR and SCR of QKD networks with different QKR mechanisms and traditional QKD networks, when \( V_{\text{key,gen}} \) is 120.

Referring to the setting of the service security factor in Table 4, Figure 11 shows the relative security index of the service under different service numbers. The red line indicates that when no recycling is used, the relative security index of the service is always 1. This means that the key recycled by the QKR algorithm may not be as secure as the key directly generated by the traditional QKD. But it can provide encryption services for some businesses with low security requirements. Furthermore, the average relative security capability of the business has no obvious relationship with the number of services.

![Figure 11](image)

**Figure 11.** Relative security index of different QKR mechanisms compared to the no-recycling algorithm of traditional QKD networks

6.2. Comparative Analysis between Different QKR Algorithms
In this section, the performance gap between the three key-recovery algorithms of all recycling, partial recycling, and mixed recycling is compared. Figure 12(a) illustrates that when the key-generation rate increases, no matter which recycling method is adopted, the security coverage of the service will increase. This is because the increase in key-generation rate means that more quantum keys can be used to provide security services. The partial-recycling algorithm performs best in this case because direct recycling does not affect the originally high security level of the business. Also, because the recycling key affects the original normal encryption service, the all-recycling algorithm performs the worst.

Figure 12(b) illustrates that the change in key-generation rate has no significant effect on key-utilization rate. This indicates that the key-generation rate is not the main factor affecting key utilization. However, it is obvious that the key-utilization rate of the three algorithms is higher than 90%. Partial recycling and mixed recycling performances are similar and slightly higher than all recycling.

![Figure 12. (a) The effect of $V_{key,gen}$ on SCR and (b) KUR of QKD networks with different QKR mechanisms, when SFR is 30%.](image)

As shown in Figure 13(a), the horizontal axis represents the ratio of the number of low-security-level data services to the number of high-security-level services. The larger the horizontal axis, the larger the proportion of low security level services. Both mixed recycling and all recycling show similar performances for KUR and SCR indicators. It may be because the decision made by the mixed algorithm based on the historical data service information tends to all recycling, resulting in a decrease in the proportion of the partial-recycling algorithm being adopted during the entire key-recovery process. In addition, SCR embodies the proportion of services successfully encrypted in the network, the granularity of the service is larger than the key, so the jitter of the SCR is greater than KUR.

Figure 13 (b) present the balance of the key amount in the network after 100,000 data services. Both the x-axis and the y-axis represent the node number, and the xy plane determines the logical position of the QKP. The z-axis represents the ratio of the QKP key amount to the minimum key amount of all QKPs. In general, due to the design of the key-relay routing algorithm, three recycling methods do not perform well in terms of balance. However, compared to the other two recycling algorithms, the mixed-recycling algorithm performs best in terms of balance, while the all-recycling algorithm performs the worst. For the all-recycling algorithm, the poor equalization provides an optimized direction for the optimization of the algorithm. Since the most important factor affecting the performance of the all-recycling algorithm is the consumption of the original key, the unbalanced key amount can just provide
the original for the all-recycling algorithm through the relay, thereby improving the performance of the algorithm.

![Figure 13](image.png)

**Figure 13.** (a) The impact of service mix ratios of different security levels on KUR and SCR of QKD networks with different QKR mechanisms, when $V_{key,pool}$ is 120, SFR is 30%, and service intensity is 250. (b) The number of remaining keys in the key pool of each node after the simulation.

7. Conclusions

With the fundamental purpose of improving key utilization, this paper proposes quantum-key recycling mechanisms in QKD network to increase the number of available keys in the system and further improve the security-coverage rate of the service. The paper also establishes different service security levels, and match different levels of keys and encryption algorithms for services of different security levels, so that the keys are effectively used. Compared with the traditional QKD network with no-recycling algorithm, partial recycling and all recycling have obvious advantages for both KUR and SCR under different service strengths and business failure rates. The performance improvement for KUR indicators is higher than 10%, and the SCR index is increased by about 20%. The mixed-key-recycling strategy is superior to all-key-recycling mechanisms in terms of KUR and SCR, and is equal to or slightly lower than that of partial-key-recycling mechanisms. In order to measure the impact of the key recycling mechanism on network security, a key security factor is designed. The security factor for three key recycling algorithms are all higher than 0.9, and the mixed-key recycling mechanism is higher than the partial-key recovery mechanisms. The three key-recycling algorithms are not optimized for the load balancing of the security services of the network. Some key pools carry a small number of services, resulting in a large number of key accumulations. These accumulated keys can be used to provide the original key for partial-key recycling. While improving the key-recycling rate and reducing the service-blocking rate, it is one of the subsequent optimization directions of the QKR mechanism.

**Author Contributions:** The writing of the draft was by X.L., the review, editing of the draft were responsible by Y.Z., the language improvement of the draft was by A.N, the suggestions for idea were made by X.Y., and the experimental equipment was provided by J.Z. All authors have read and agreed to the published version of the manuscript.

**Funding:** This work has been supported in part by National Natural Science Foundation of China (NSFC) (61601052, 61822105), the Fundamental Research Funds for the Central Universities (2019XD-A05), State Key Laboratory of Information Photonics and Optical Communications of China (IPOC2019ZR01).

**Conflicts of Interest:** No conflict of interest.
References

1. Y. Zhao; B. Yan; Z. Li; W. Wang; Y. Wang; J. Zhang. Coordination between Control Layer AI and On-Board AI in Optical Transport Networks. *IEEE OSA J. Opt. Commun. Netw.* 2019, 12, A49–A57.

2. Scarani, V.; Bechmann-Pasquinucci, H.; Cerf, N.J.; Dušek, M.; Lütkenhaus, N.; Peev, M.. The security of practical quantum key distribution. *Rev. Mod. Phys.* 2009, 81, 1301–1350.

3. Takeoka, M.; Guha,S.; Wilde, MM. Fundamental rate-loss tradeoff for optical quantum key distribution. *Nat. Commun.* 2014, 5, 5235.

4. Bäuml, S.; Christandl, M.; Horodecki, K.; Winter, A.. Limitations on quantum key repeaters. *Nat. Commun.* 2015, 6, 6908.

5. Yin, H.L.; Fu, Y.. Measurement-Device-Independent Twin-Field Quantum Key Distribution. *Sci. Rep.* 2019, 9, 3045.

6. Diamanti, E.; Lo, H.; Qi, B.; Yuan, Z. L.. Practical challenges in quantum key distribution. *npj Quantum Inform.* 2016, 2, 16025.

7. Azuma, K.; Tamaki, K.; Lo, H.-K. All-photonic quantum repeaters. *Nat. Commun.* 2015, 6, 6787.

8. Bourgoin, J.; Higgins, B. L.; Gigov, N.; Holloway, C.; Pugh, C. J.; Kaiser, S. Cranmer, M.; Jennewein, T.. Free-space quantum key distribution to a moving receiver. *Opt. Express.* 2015, 23, 33437–33447.

9. Peem, M.; Pacher, C.; Alleaume, R.; Barreiro, C.; Bouda, J.; Boxleitner, W.; Debuisschert, T.; Diamanti, E.; Dianati, M.; Dynes,JF; et al. The SECOQC quantum key distribution in Vienna. *New J. Phys.* 2009, 11, 075001.

10. 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.

11. Wang, H.; Zhao, Y.; Yu, X.; Ma, Z.; Wang, J.; Nag, A.; Yi, L.; Zhang, J. Protection Schemes for Key Service in Optical Networks Secured by Quantum Key Distribution (QKD). *J. Opt. Commun. Netw.* 2019, 11, 67–78.

12. Cao, Y.; Zhao, Y.; Wang, J.; Yu, X.; Ma, Z.; Zhang, J. Cost-Efficient Quantum Key Distribution (QKD) Over WDM Networks. *J. Opt. Commun. Netw.* 2019, 11, 285–298.

13. Cao, Y.; Zhao, Y.; Lin, R.; Yu, X.; Zhang, J.; Chen, J. Multi-tenant secret-key assignment over quantum key distribution networks. *Opt. Express.* 2019, 27, 2544–2561.

14. Cao, Y.; Zhao, Y.; Yu, X.; Wu, Y. Resource Assignment Strategy in Optical Networks Integrated With Quantum Key Distribution. *J. Opt. Commun. Netw.* 2017, 9, 995–1004.

15. Portmann, C. Key Recycling in Authentication. *IEEE T. Inform. Theory.* 2014, 60, 4383–4396.

16. Fehr, S.; et al. Quantum authentication; encryption with key recycling. In Proceedings of the Annual International Conference on the Theory; Applications of Cryptographic Techniques, Springer: Berlin/Heidelberg, Germany, 30 April - 4 May, 2017, 311–338.

17. Rothe, S.; Koukourakis, N.; Radner, H.; Lonngstrom, A.; Jorswieck, E. A.; Czerske, J.. Physical Layer Security in Multimode Fiber Optical Networks. *Sci. Rep.* 2019, 10, 2740.

18. Wang, F.; Zhao, Y.; Wang, W.; Liu, D.; Liu, J.; Zhang, S.; Ding, Z.; Jin, S.; Zhang, J. Machine Learning with Service Classification for Detecting Control Plane Intrusions in Software Defined Optical Networks. In Proceedings of the 2018 23rd Opto-Electronics; Communications Conference (OECC), Jeju Island, Korea, 2–6 July 2018, 1–2.

19. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *arXiv Preprint 1984,* arXiv:2003.06557.

20. Elliott, C. Building the quantum network. *J. New Journal of Physics* 2002, 4, 46–46.

21. Sasaki, M.; Fujiwara, M.; Jin, R.; Takeoka, M.; Han, T. S.; Endo, H.; Yoshino, K.; Ochi, T.; Asami, S.; Tajima, A. Quantum Photonic Network: Concept, Basic Tools, and Future Issues. *IEEE J. Sel. Top. Quant.* 2014, 21, 49–61.

22. Cao, Y.; Zhao, Y.; Wu, Y.; Yu, X.; Zhang, J. Time-Scheduled Quantum Key Distribution (QKD) Over WDM Networks. *J. Lightwave Technol.* 2018, 36, 3382–3395.

23. Li, F.; Wang, X.; Pan, T.; Yang, J.. Packet delay, loss and reordering in IPv6 world: A case study. In Proceedings of the 2016 International Conference on Computing, Networking and Communications (ICNC), Kauai, Hawaii, USA, February 15-18, 2016, 1–6.

24. Merazka, F. Packet loss concealment using piggybacking for speech over IP network services. In Proceedings of the 2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS), Berlin, Germany, 12-14 September, 2013, 1, 509–512.
25. Mitić, D.; Lebl, A. Packet loss in the local network of IRITEL. In Proceedings of The 33rd International Convention MIPRO, Opatija, Croatia, 24-28 May, 2010; 534–538.
26. Overby, H. Packet loss rate differentiation in slotted optical packet switched networks. *IEEE Photon. Tech. Lett.*, 2005, 17, 2469–2471.
27. Kawamoto, Y.; Nishiyama, H.; Kato, N.; Kadowaki, N. A Traffic Distribution Technique to Minimize Packet Delivery Delay in Multilayered Satellite Networks. *IEEE T. Veh. Technol.*, 2013, 62, 3315–3324.
28. Bisio, I.; Delucchi, S.; Lavagetto, F.; Marchese, M. Lp-Problem-Based Transmission Rate Allocation with Packet Loss; Power Metrics over Satellite Networks. *IEEE T. Veh. Technol.*, 2016, 65, 3312–3325.
29. Paar, C.; Pelzl, J. The Data Encryption Standard (DES) and Alternatives. In *Understanding Cryptography*; Springer: Berlin/Heidelberg, Germany, 2010.
30. Peter, R. The design of composite permutations with applications to DES-like S-boxes. *Des. Codes Cryptogr.*, 2007, 42, 21–42.

© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).