Multi-user quantum key distribution with collective eavesdropping detection over collective-noise channels*

Huang Wei(黄 伟)[a)b)†], Wen Qiao-Yan(温巧燕)[a)], Liu Bin(刘 斌)[a)], and Gao Fei(高 飞)[a)]

[a)] *State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*
[b)] *Science and Technology on Communication Security Laboratory, Chengdu* 610041, *China*

(Received 26 December 2014; revised manuscript received 17 February 2015; published online 29 May 2015)

A multi-user quantum key distribution protocol is proposed with single particles and the collective eavesdropping detection strategy on a star network. By utilizing this protocol, any two users of the network can accomplish quantum key distribution with the help of a serving center. Due to the utilization of the collective eavesdropping detection strategy, the users of the protocol just need to have the ability of performing certain unitary operations. Furthermore, we present three fault-tolerant versions of the proposed protocol, which can combat with the errors over different collective-noise channels. The security of all the proposed protocols is guaranteed by the theorems on quantum operation discrimination.

Keywords: quantum cryptography, quantum key distribution, collective eavesdropping detection, collective noise

PACS: 03.67.Dd, 03.67.Hk, 03.67.Pp **DOI:** 10.1088/1674-1056/24/7/070308

1. Introduction

Over the last two decades, the principles of quantum mechanics have been widely applied in the field of information, which has promoted rapid developments of quantum cryptography and quantum computation. Since the pioneering work of Bennett and Brassard in 1984,[1] quantum cryptography has attracted a great deal of attention and become one of the most promising applications of quantum information processing. There are several remarkable branches of quantum cryptography, including quantum key distribution (QKD),[1–14] quantum secure direct communication (QSDC),[15–22] quantum secret sharing (QSS),[23–28] and secure multi-party computation (SMC).[29–33] The multi-party quantum cryptographic protocols (MQCPs) which involve at least three participants, such as quantum private comparison (QPC) protocols and QSS protocols, are more complicated than the two-party ones. Therefore, more attention is needed in the research of MQCPs.

In most MQCPs, the quantum information carriers need to be transmitted more than once, and usually eavesdropping detection should be taken in every step of the transmission. However, this detection strategy, which is called step-by-step detection, always makes the protocols inefficient and complicated. First, it is known that the security analysis of the quantum cryptographic protocols is based on the error rate analysis with theories in statistics. Hence, the proportion of the detection states (i.e., states chosen for eavesdropping detection) in the transmitted states should not be too small. If the detection is taken in every step of the transmission of the quantum information carriers, a lot of states will be used for checking eavesdropping and the qubit efficiency of the corresponding protocol will decrease with the increase of the number of detections. Second, detecting in every step of the transmission usually requires all the participants in such a protocol to be equipped with many quantum devices, e.g., the quantum state measurement machine, the quantum state generation machine, and the quantum storage machine. However, based on the current technology, these quantum devices are still expensive because of their construction difficulties. As a consequence, it is uneconomical to require that every participant is equipped with most of these quantum devices. Apparently, an MQCP would be more efficient and easier to realize if the detection is taken only once in the whole procedure of the protocol. Fortunately, if an MQCP makes use of the collective eavesdropping detection strategy, it could meet such a requirement. Collective detection is an efficient and useful eavesdropping detection strategy for MQCPs. On one hand, in an MQCP which employs the collective detection strategy, the detection needs to be taken only once after the whole transmission procedure of the quantum information carriers. On the other hand, this strategy can also reduce the hardware requirement for the implementation of the protocol, since all the users (except for the center who is responsible for preparing and measuring states) only need to perform certain unitary operations in the whole executing procedure of the protocol. To date, much attention has been focused on the collective detection strategy and a lot of MQCPs have been proposed by utilizing it (for simplicity, we will call the MQCP which uses collective detection MQCP-CD),[34–41] including QKD,[34–36] QPC,[37]

*Project supported by the National Natural Science Foundation of China (Grant Nos. 61272057, 61170270, and 61309029), Beijing Higher Education Young Elite Teacher Project, China (Grant Nos. YETP0475 and YETP0477), and BUPT Excellent Ph.D. Students Foundation, China (Grant No. CX201441).

†Corresponding author. E-mail: huangwei096505@aliyun.com

© 2015 Chinese Physical Society and IOP Publishing Ltd

QSS,[38–40] and QSQC.[41]

In an MQCP-CD, all the users (except for the center) just need to be capable of performing certain unitary operations. Therefore, the operations performed by them are very important to the security of the protocol. In this paper, a method for constructing the operations needed in the MQCP-CD is presented. It is a method that can be used to construct the unitary operations which meet the security requirements of the MQCP-CD with different kinds of quantum states, such as single photons, EPR pairs, and GHZ states. Based on this method, we present a multi-user quantum key distribution (MQKD) protocol with collective detection and single particles. Our protocol is presented on a star network where any two of the involved users can execute quantum key distribution with the help of a serving center. There are several merits of this protocol. First, to establish a random key by employing this protocol, two users only need to be capable of performing certain unitary operations. Second, none of the participants (all the users and the center) in our protocol needs to be equipped with a quantum storage machine. As storing quantum qubits is still a very difficult task in reality, our protocol is more feasible than the ones[34–36] in which the quantum storage machine is required. In addition, our protocol can resist various kinds of attacks from both outside eavesdroppers and a dishonest center.

Actually, quantum states transmitted in a channel interact with the environment uncontrollably, which will introduce noise into the communication and influence both the correctness and efficiency of the communication. If the variation of the noise is slower than the time delay between the quantum states transmitted inside a time window, the states will be affected by the same noise. This kind of noise is called collective noise.[42,43] To combat the errors caused by the collective noise, we further introduce three fault-tolerant versions of our protocol with the idea of decoherence-free subspace (DFS),[44–54] which can resist the collective-dephasing noise, the collective-rotation noise, and all kinds of unitary collective noise, respectively.

The remainder of this paper is organized as follows. The next section presents our method for constructing the required unitary operations in the MQCP-CD. In Section 3, our MQKD protocol and its three fault-tolerant versions, which utilize the collective detection and block transmission, are proposed in detail. The block transmission, which was proposed firstly by Long *et al.* in Ref. [15], is one of the most important techniques for transmitting quantum states in quantum information processing. In block transmission, the quantum states are ordered and transmitted in blocks, and the eavesdropping detection is also executed on the blocks. In Section 4, the security of our proposed protocols is analyzed by using the theorems on quantum operation discrimination. Finally, a discussion as well as a short conclusion is given in Section 5.

2. Method for constructing the unitary operations required in MQCP-CD

Thus far, many MQCP-CDs[34,35,55–57] have been attacked since the unitary operations used in those protocols can be discriminated unambiguously (by a single use) if an eavesdropper utilizes some special attack strategies, such as dense-coding attack[35] and fake-signal attack.[55] It is just because there is still no effective method for constructing the required unitary operations that some improper ones were used in those protocols. In this section, we introduce a method for constructing the required unitary operations which can be used in designing a secure MQCP-CD. This method can be used to construct the required unitary operations with different kinds of quantum states. Afterwards, we prove the correctness of this method based on the conclusions on quantum operation discrimination.

2.1. The detailed method

Before presenting the method for constructing the required operations, we first briefly introduce the basic principle of the MQCP-CD.[34–41] In this kind of protocol, two mutually unbiased bases, which are denoted as $\{|a\rangle, |b\rangle\}$ and $\{|c\rangle, |d\rangle\}$, are required for secure communication. Here, $\langle a|b\rangle = \langle c|d\rangle = 0$, and $|\langle a|c\rangle|^2 = |\langle a|d\rangle|^2 = |\langle b|c\rangle|^2 = |\langle b|d\rangle|^2 = 1/2$. Besides, there should be a center who is responsible for generating and measuring the quantum states. The center first generates a sequence of states in the two bases and sends them to the first user. Then the first user processes the received states by performing four unitary operations according to his secret binary string and controlling binary string. After the operations, the first user sends the processed sequence to the next user. The following users execute procedures just like the first user one by one. When the last user finishes his operations, he sends the sequence back to the center. After the center receives the sequence, the users randomly choose some states to check eavesdropping with the information of the unitary operations performed on the chosen states and the corresponding measurement outcomes provided by the center. If the whole transmitting procedure is secure, the remaining states (or measurement outcomes) can be used to realize the main function of the protocol.

Concretely, when a user receives a sequence of quantum states, he first encodes his secret string by performing the operation I (identity operator)/U (encoding operation) on each of the received states if the corresponding bit of the secret string is 0/1. The effect of the unitary operation U is flipping a state in the same MB, i.e., $U|a\rangle = \alpha|b\rangle$, $U|b\rangle = \beta|a\rangle$, $U|c\rangle = \gamma|d\rangle$, and $U|d\rangle = \delta|c\rangle$. Here α, β, γ, and δ are global phase factors which can be ignored. After that, he disturbs the encoded

states by performing the operation I/C (controlling operator) on each of these states if the corresponding bit in his controlling string is 0/1. The effect of the unitary operation C is flipping each one of the four states in $\{|a\rangle, |b\rangle, |c\rangle, |d\rangle\}$ from one basis to the other basis. When a user encodes his secret string on the received states, each of the bits in the secret string and the controlling string will be used only once. If an eavesdropper wants to obtain some information of a bit in the secret string without leaving a trace in the eavesdropping detection, he should have the ability of discriminating between the four unitary operations I, U, C, and UC unambiguously with only one opportunity (i.e., under the condition that the device can be accessed only once). Therefore, one of the key steps in designing a secure MQCP-CD is to find appropriate unitary operations U and C which make I, U, C, and UC impossible to be discriminated unambiguously with a single use.

Now we give the method for constructing the required unitary operations. Suppose V is a d-dimensional Hilbert space. By employing the Gram–Schmidt procedure, it is easy to construct an orthonormal basis of V, $\{|0'\rangle, \ldots, |(d-1)'\rangle\}$. It can be easily proved that $\{|0'\rangle, |1'\rangle\}$ and $\{|+'\rangle, |-'\rangle\}$ are two mutually unbiased bases of a 2-dimensional subspace, where

$$|+'\rangle = \frac{1}{\sqrt{2}}(|0'\rangle - \mathrm{i}|1'\rangle), \quad |-'\rangle = \frac{1}{\sqrt{2}}(|1'\rangle - \mathrm{i}|0'\rangle). \tag{1}$$

Then the encoding operation is chosen in the form of

$$U = |0'\rangle\langle 1'| + |1'\rangle\langle 0'| + M, \tag{2}$$

where part M should meet the following two conditions. First, M should be in a proper form to make U be a unitary operation, i.e., $U^\dagger U = UU^\dagger = I$. Second, M should be orthogonal to both $|0'\rangle$ and $|1'\rangle$. It can be easily verified that the operation U could flip each one of the states in $\{|0'\rangle, |1'\rangle, |+'\rangle, |-'\rangle\}$ in its own basis when M is in the required form. There are many feasible choices for the form of M, such as $M = |2'\rangle\langle 2'| + \cdots + |(d-1)'\rangle\langle (d-1)'|$ and $M = |2'\rangle\langle 3'| + |3'\rangle\langle 4'| + \cdots + |(d-1)'\rangle\langle 2'|$. After getting the encoding operation U, we choose one of the square roots of U as the controlling operation, which could flip each one of the states in $\{|0'\rangle, |1'\rangle, |+'\rangle, |-'\rangle\}$ from one basis to the other basis, i.e., $C = \sqrt{U}$. The selection method for the operation C will be given in the following proof section. Thus, a method for constructing the required encoding operation and controlling operation has been introduced. In other words, if operations U and C are constructed by this method, the four unitary operations I, U, C, and UC cannot be discriminated unambiguously with only one opportunity.

2.2. Proof of the proposed method

Herein we demonstrate that the four unitary operations I, U, C, and UC cannot be discriminated unambiguously with a single use if U and C are constructed by our method. Before giving the proof, we first introduce an important theorem on quantum operation discrimination.

Theorem 1[58] Under the condition that the device can be accessed only once, the minimum error probability to discriminate two unitary operations U_1 and U_2 is

$$P_{\mathrm{e}} = \frac{1}{2}\left[1 - \sqrt{1 - 4p_1p_2r(U_1^\dagger U_2)^2}\right], \tag{3}$$

where $r(U_1^\dagger U_2)$ stands for the distance between the origin of the complex plane and the polygon whose vertices are the eigenvalues of the unitary operator $U_1^\dagger U_2$ (see also Fig. 1), and $U^\dagger$ is the adjoint matrix of U.

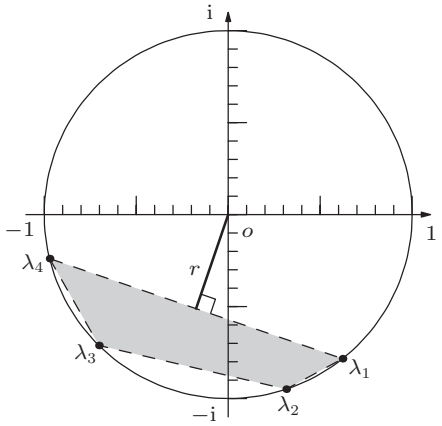


Fig. 1. Definition of the function $r(U) = r$, where λ_1, λ_2, λ_3, and λ_4 are eigenvalues of the matrix U, and r is the distance between the origin of the complex plane o and the polygon $\lambda_1\lambda_2\lambda_3\lambda_4$. Obviously, $r = 0$ indicates that o is in/on the polygon $\lambda_1\lambda_2\lambda_3\lambda_4$.

Corollary 1 Under the condition that the device can be accessed only once, two unitary operations U_1 and U_2 can be discriminated unambiguously if and only if $r(U_1^\dagger U_2) = 0$.

As defined in the presented method, $C = \sqrt{U}$ ($U = C^2$). It can be easily found that $r(I^\dagger C) = r(U^\dagger UC) = r(C)$, and $r(U^\dagger C) = r(U^{-1}C) = r(C^{-1}) = r(C^\dagger)$. According to Theorem 1 and Corollary 1, under the condition that the device can be accessed only once, the two operations U and C (I and C, U and UC) constructed by our method cannot be discriminated unambiguously if and only if neither $r(C^\dagger)$ and $r(C)$ equal to zero. Now we demonstrate that $r(C^\dagger) > 0$ and $r(C) > 0$. Since U is a unitary operator, all the eigenvalues of U are points on the unit circle in the complex plane. Namely, all the eigenvalues of U can be written in the form of $\mathrm{e}^{\mathrm{i}(\theta+2k\pi)}$, here $\mathrm{e}^{\mathrm{i}(\theta+2k\pi)} = \mathrm{e}^{\mathrm{i}\theta}$, $\theta \in [0, 2\pi)$, $k \in \mathbf{Z}$. Therefore, all the eigenvalues of the operator $\sqrt{U}$ should be in the form of $\mathrm{e}^{\mathrm{i}(\beta+k\pi)}$, here $\beta = \theta/2 \in [0, \pi)$, $k \in \mathbf{Z}$. It is obvious that U has more than one square root. Take the Pauli operation σ_0 as a simple example, since σ_0 can be written as either $\mathrm{e}^{\mathrm{i}\cdot 0}|0\rangle\langle 0| + \mathrm{e}^{\mathrm{i}\cdot 0}|1\rangle\langle 1|$ or $\mathrm{e}^{\mathrm{i}\cdot 0}|0\rangle\langle 0| + \mathrm{e}^{\mathrm{i}\cdot 2\pi}|1\rangle\langle 1|$, both $\mathrm{e}^{\mathrm{i}\cdot 0}|0\rangle\langle 0| + \mathrm{e}^{\mathrm{i}\cdot 0}|1\rangle\langle 1|$ and $\mathrm{e}^{\mathrm{i}\cdot 0}|0\rangle\langle 0| + \mathrm{e}^{\mathrm{i}\cdot \pi}|1\rangle\langle 1|$ are the square roots of σ_0, i.e., $\sigma_0 = \sigma_0^2 = \sigma_z^2$. Here $|0\rangle$ and $|1\rangle$ represent the horizontal and the vertical polarizations of photons, respectively.

As shown above, all the eigenvalues of the operator $\sqrt{U}$ should be in the form of $e^{i(\beta+k\pi)}$, $k \in \mathbf{Z}$. In our method, we choose the square root (of U) whose eigenvalues are all in the form of $e^{i\beta}$ (which means that the corresponding parameter k is even) as the controlling operation C. As $\beta \in [0, \pi)$, all the eigenvalues of C are points on the upper half of the unit circle (except for -1) in the complex plane and therefore $r(C) > 0$. In addition, since all the eigenvalues of C are points on the upper half of the unit circle (except for -1), it is evident that all the eigenvalues of $C^\dagger$ are points on the bottom half of the unit circle (except for -1), which means $r(C^\dagger) > 0$. That is to say, the two operations U and C (I and C, U and UC) constructed by our method cannot be discriminated unambiguously under the condition that the device can be accessed only once.

Till now, we have proved that the four unitary operations I, U, C, and UC constructed by our method cannot be discriminated unambiguously under the condition that the device can be accessed only once. Utilizing this method, we can construct the required unitary operations for designing a secure MQCP-CD with different kinds of quantum states.

2.3. Role of the proposed method

If someone wants to design an MQCP-CD using a certain kind of quantum state in his favor, one of the most important things he should do first is to find the corresponding encoding operation U and controlling operation C which satisfy the security requirement of the MQCP-CD. Obviously, the method we just proposed can be used to construct such unitary operations. For example, if he wants to design an MQCP-CD with single photons, a natural choice for one of the two bases could be $\{|0\rangle, |1\rangle\}$. By employing our method, the other basis could be chosen as $\{|+\rangle, |-\rangle\}$, where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle - \mathrm{i}|1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|1\rangle - \mathrm{i}|0\rangle)$, and the corresponding encoding operation U_s and controlling operation C_s can be constructed as

$$U_\mathrm{s} = |0\rangle\langle 1| + |1\rangle\langle 0| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$
$$C_\mathrm{s} = \sqrt{U_\mathrm{s}} = \frac{1+\mathrm{i}}{2}\begin{pmatrix} 1 & -\mathrm{i} \\ -\mathrm{i} & 1 \end{pmatrix}. \quad (4)$$

It can be easily verified that $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$ form two mutually unbiased bases. The effect of the operations U_s and C_s on the four states can be illustrated as

$$\begin{aligned} &U_\mathrm{s}|0\rangle = |1\rangle, \quad U_\mathrm{s}|1\rangle = |0\rangle, \\ &U_\mathrm{s}|+\rangle = |-\rangle, \quad U_\mathrm{s}|-\rangle = |+\rangle, \\ &C_\mathrm{s}|0\rangle = \left(\frac{1+\mathrm{i}}{\sqrt{2}}\right)|+\rangle, \quad C_\mathrm{s}|1\rangle = \left(\frac{1+\mathrm{i}}{\sqrt{2}}\right)|-\rangle, \\ &C_\mathrm{s}|+\rangle = \left(\frac{1-\mathrm{i}}{\sqrt{2}}\right)|1\rangle, \quad C_\mathrm{s}|-\rangle = \left(\frac{1-\mathrm{i}}{\sqrt{2}}\right)|0\rangle. \end{aligned} \quad (5)$$

Utilizing the two bases and two operations (U_s and C_s) given above, one can design different kinds of MQCP-CDs (QSS, QPC, etc.) with single photons. Evidently, there are still some other choices for the two operations if other single particles are chosen to be the quantum information carriers. To date, in order to improve the qubit efficiency or reduce the hardware requirement, some MQCP-CDs [34–41] have been proposed with single photons. Unfortunately, all of those protocols need to store the quantum qubits, which is still a difficult task in reality. To make use of the collective detection under the current techniques, we present a more feasible MQKD protocol without employing a quantum storage machine in the next section. More importantly, we also enhance the proposed protocol to be immune to the errors over different collective-noise channels based on the above method.

3. The proposed MQKD protocols

In this section, we present an MQKD protocol by employing single particles and the collective detection on a star network (see Fig. 2). In this protocol, there is a center who is responsible for generating and measuring quantum states. With the help of the center, any two users involved in the network can securely establish a random key just by performing unitary operations on the states transmitted to them. If user i wants to share a random key with user j, they can encode their random binary strings into the states produced by the center, and then they are able to deduce a random key with the measurement outcomes published by the center, where $1 \le i, j \le n$. In this circumstance, users i and j only need to hide their secrets in the transmitted states with proper unitary operations. In the network, we assume that any two of the participants (the center and all the users) can transmit quantum states between them. Similar to most of the previous quantum cryptographic protocols, the classical channels involved in this protocol are supposed to be authenticated. Compared with the existing MQKD

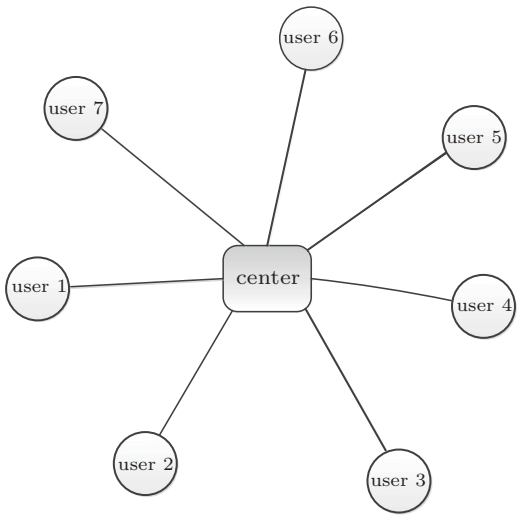


Fig. 2. A simple illustration of the MQKD with seven users on a star network. In this network, any two of the seven users can establish a shared secret key only with unitary operations.

protocols which also utilize the collective detection,[34–36] our protocol has the following two advantages. First, it is secure against attacks from both outside eavesdroppers and a dishonest center. Second, it does not need a quantum storage machine, which indicates that our protocol is more feasible in practice under current techniques. By utilizing the method presented in Section 2, two fault-tolerant versions of the proposed protocol are proposed by using two-qubit states: one is immune to the collective-dephasing noise, and the other is immune to the collective-rotation noise. Then we also present a more robust version of the protocol, which can resist all kinds of unitary collective noise by using four-qubit states.

3.1. The proposed MQKD protocol with single particles

If two users in the network, say Alice and Bob, want to share a random key, they can execute the MQKD protocol as described below (see also Fig. 3).

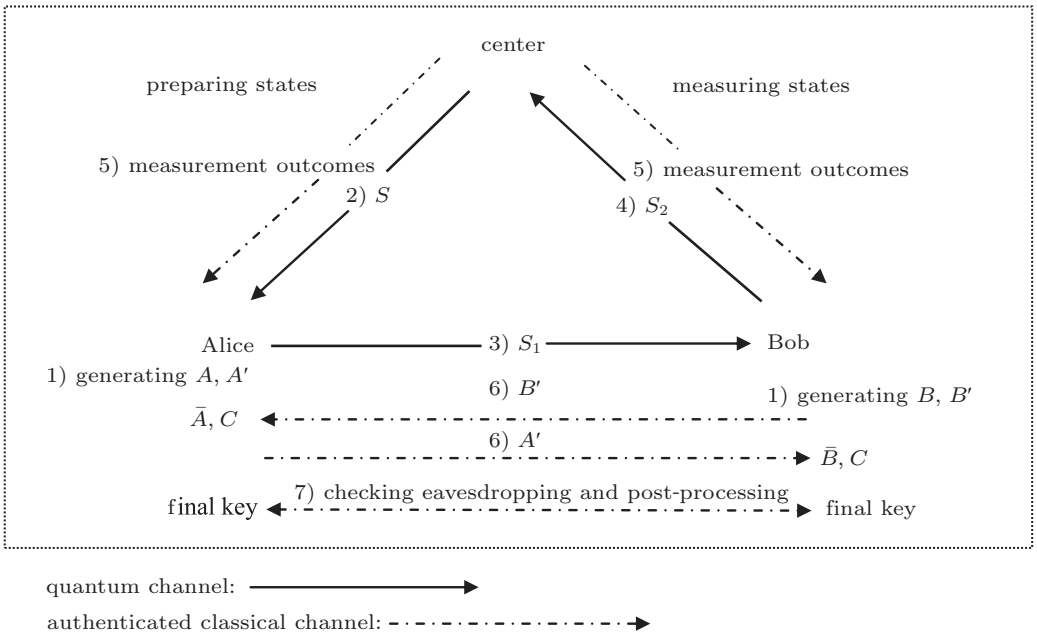


Fig. 3. The subsystem of the presented QKD network with single particles.

1) Alice generates two random binary strings of length $4n$, which are denoted as A and A', respectively. Similarly, Bob generates two random binary strings of length $4n$, which are denoted as B and B', respectively. After that, Alice informs the center that she wants to establish a random key with Bob.

2) The center receives Alice's request, prepares a sequence of $4n$ single particles which are all in the state $|0\rangle$ (denoted as sequence S), and sends it to Alice.

3) Once receiving S, Alice performs the unitary operations U^{A_i} and $C^{A'_i}$ on the i-th particle in S for $1 \leq i \leq 4n$. Here, A_i and A'_i are respectively the i-th bit in strings A and A', $U^1 = U_s$, $C^1 = C_s$, and $U^0 = C^0 = I_s$ is the identity density operator on the two-dimensional Hilbert space, i.e., $I_s = |0\rangle\langle 0| + |1\rangle\langle 1|$. After that, she sends the new sequence (denoted as S_1) to Bob.

4) Upon receiving the sequence S_1, Bob performs operations U^{B_i} and $C^{B'_i}$ on the i-th particle in S_1 for $1 \leq i \leq 4n$. Then he sends the new sequence (denoted as S_2) back to the center.

5) Once receiving S_2, the center makes a measurement on each of the particles randomly in σ_z-basis or σ_y-basis, and then publishes the measurement outcome of each of the particles in S_2, where σ_z-basis $= \{|0\rangle, |1\rangle\}$ and σ_y-basis $= \{|+\rangle, |-\rangle\}$. According to the i-th measurement outcome announced by the center, Alice and Bob could learn which of the two bases was used to measure the i-th particle in S_2. Concretely, if the measurement outcome is $|0\rangle$ or $|1\rangle$ ($|+\rangle$ or $|-\rangle$), the σ_z-basis (σ_y-basis) was used.

6) After the center announced the measurement outcomes of all the particles in S_2, Alice and Bob publish A' and B', respectively, where A'_i (B'_i) indicates whether Alice (Bob) has performed C_s on the i-th particle in the travelling sequence. Based on the announced information, Alice and Bob are able to determine which of the particles in S_2 were measured in correct bases. Here measuring the i-th particle in the correct basis represents that the i-th measurement outcome is $|0\rangle$ or $|1\rangle$ ($|+\rangle$ or $|-\rangle$) under the condition that $A'_i + B'_i$ is 0 or 2 (1). According to the probabilistic theory, half of the particles in S_2 (i.e., $2n$ particles in S_2) have been measured by the center with correct measuring bases. For the positions of the measurement outcomes obtained from incorrect measuring bases, Alice and Bob discard the corresponding bits in A, B, A', and B', where the new strings are denoted as $\bar{A}$, $\bar{B}$, $\bar{A}'$, and $\bar{B}'$, respectively. Then Alice and Bob can deduce a $2n$-bit string

C with the measurement outcomes obtained with the correct measuring bases. Concretely, if the measurement outcome is $|0\rangle$ or $|+\rangle$ ($|1\rangle$ or $|-\rangle$), the corresponding bit of C is 0 (1). The relationship among the values of $\bar{A}_j$, $\bar{B}_j$, $\bar{A}'_j+\bar{B}'_j$, and C_j when no error occurs is shown in Table 4, where $1 \le j \le 2n$ and $\oplus$ denotes the additional module 2.

7) To check eavesdropping, Bob randomly chooses n positions in string C and requires Alice to tell him the corresponding bits in $\bar{A}$. According to the information announced by Alice and Table 1, Bob checks whether the corresponding bits in C are in accordance with the theoretical values. If the error rate is higher than acceptable, they abort the results; otherwise, Bob can trust the transmission and deduce the rest n bits of $\bar{A}$ with the corresponding bits of C and $\bar{B}$. At last, Alice and Bob utilize error correction and privacy amplification[59,60] to establish a secure session key.

Table 1. The relationship among the values of $\bar{A}_j$, $\bar{B}_j$, $\bar{A}'_j+\bar{B}'_j$, and C_j when no errors occur.

$\bar{A}_j$	$\bar{B}_j$	$\bar{A}'_j+\bar{B}'_j$	C_j
$\bar{A}_j$	$\bar{B}_j$	0 or 1	$\bar{A}_j \oplus \bar{B}_j$
$\bar{A}_j$	$\bar{B}_j$	2	$\bar{A}_j \oplus \bar{B}_j \oplus 1$

In this protocol, with the help of the center, any two of the involved users can establish a random key with only unitary operations. Although the qubit efficiency of our protocol is half of that of the protocols in Refs. [34]–[36], our protocol does not need to store quantum qubits. Hence, our protocol is more feasible with the current techniques. Besides, users should set up a filter and a beam splitter to prevent a Trojan horse attack and an invisible-photon attack.[61,62]

3.2. Fault-tolerant MQKD protocols against collective noise

Herein we introduce three fault-tolerant versions of the proposed MQKD protocol based on the method in Section 2 and the idea of DFS, which can be immune to the collective-dephasing noise, the collective-rotation noise, and all kinds of unitary collective noise, respectively.

3.2.1. Fault-tolerant MQKD protocol against collective-dephasing noise

The collective-dephasing noise[42,45,63] can be described as

$$|0\rangle \longrightarrow |0\rangle, \quad |1\rangle \longrightarrow \mathrm{e}^{\mathrm{i}\phi}|1\rangle, \tag{6}$$

where ϕ is the noise parameter and fluctuates with time. A logical qubit, which is composed of two physical qubits with antiparallel parity as

$$|0\rangle_{\mathrm{L}} = |0\rangle|1\rangle, \quad |1\rangle_{\mathrm{L}} = |1\rangle|0\rangle, \tag{7}$$

is immune to the collective-dephasing noise, as both qubits obtain the same phase factor $\mathrm{e}^{\mathrm{i}\phi}$ through this kind of channel. To communicate securely, at least two non-orthogonal measuring bases are required. According to the presented method, one basis could be $\{|0\rangle_{\mathrm{L}}, |0\rangle_{\mathrm{L}}\}$, and the other one is $\{|+\rangle_{\mathrm{L}}, |-\rangle_{\mathrm{L}}\}$, where

$$|+\rangle_{\mathrm{L}} = \frac{1}{\sqrt{2}}(|0\rangle_{\mathrm{L}} - \mathrm{i}|1\rangle_{\mathrm{L}}), \quad |-\rangle_{\mathrm{L}} = \frac{1}{\sqrt{2}}(|1\rangle_{\mathrm{L}} - \mathrm{i}|0\rangle_{\mathrm{L}}). \tag{8}$$

It is straightforward to verify that $|\langle+|0\rangle_{\mathrm{L}}|^2 = |\langle+|1\rangle_{\mathrm{L}}|^2 = |\langle-|0\rangle_{\mathrm{L}}|^2 = |\langle-|1\rangle_{\mathrm{L}}|^2 = 1/2$, which indicates that $\{|0\rangle_{\mathrm{L}}, |1\rangle_{\mathrm{L}}\}$ and $\{|+\rangle_{\mathrm{L}}, |-\rangle_{\mathrm{L}}\}$ form two mutually unbiased bases. Based on the method given in Section 2, we construct the following encoding operation U_{dp} and controlling operation C_{dp} for our MQKD protocol which can resist the collective-dephasing noise:

$$\begin{aligned} U_{\mathrm{dp}} &= |0\rangle_{\mathrm{LL}}\langle 1| + |1\rangle_{\mathrm{LL}}\langle 0| + M \\ &= |01\rangle\langle 10| + |10\rangle\langle 01| + |00\rangle\langle 11| + |11\rangle\langle 00| \\ &= \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \\ C_{\mathrm{dp}} &= \sqrt{U_{\mathrm{dp}}} = \frac{1+\mathrm{i}}{2} \begin{pmatrix} 1 & 0 & 0 & -\mathrm{i} \\ 0 & 1 & -\mathrm{i} & 0 \\ 0 & -\mathrm{i} & 1 & 0 \\ -\mathrm{i} & 0 & 0 & 1 \end{pmatrix}. \end{aligned} \tag{9}$$

The effect of the operations U_{dp} and C_{dp} on the four states can be illustrated as

$$\begin{aligned} &U_{\mathrm{dp}}|0\rangle_{\mathrm{L}} = |1\rangle_{\mathrm{L}}, && U_{\mathrm{dp}}|1\rangle_{\mathrm{L}} = |0\rangle_{\mathrm{L}}, \\ &U_{\mathrm{dp}}|+\rangle_{\mathrm{L}} = |-\rangle_{\mathrm{L}}, && U_{\mathrm{dp}}|-\rangle_{\mathrm{L}} = |+\rangle_{\mathrm{L}}, \\ &C_{\mathrm{dp}}|0\rangle_{\mathrm{L}} = \left(\frac{1+\mathrm{i}}{\sqrt{2}}\right)|+\rangle_{\mathrm{L}}, && C_{\mathrm{dp}}|+\rangle_{\mathrm{L}} = \left(\frac{1-\mathrm{i}}{\sqrt{2}}\right)|1\rangle_{\mathrm{L}}, \\ &C_{\mathrm{dp}}|1\rangle_{\mathrm{L}} = \left(\frac{1+\mathrm{i}}{\sqrt{2}}\right)|-\rangle_{\mathrm{L}}, && C_{\mathrm{dp}}|-\rangle_{\mathrm{L}} = \left(\frac{1-\mathrm{i}}{\sqrt{2}}\right)|0\rangle_{\mathrm{L}}. \end{aligned} \tag{10}$$

In this case, with the help of the center, any two of the involved users can establish a shared secret key over the collective-dephasing channel with the same steps of the protocol given in Subsection 3.1. Certainly, there are some differences between these two cases. First, the four states $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|-\rangle$ should be respectively replaced by $|0\rangle_{\mathrm{L}}$, $|1\rangle_{\mathrm{L}}$, $|+\rangle_{\mathrm{L}}$, and $|-\rangle_{\mathrm{L}}$. Second, the unitary operations I_{s}, U_{s}, and C_{s} should be substituted with $I_{\mathrm{s}}^{\otimes 2}$, U_{dp}, and C_{dp}, respectively, where $I_{\mathrm{s}}^{\otimes 2} = I_{\mathrm{s}} \otimes I_{\mathrm{s}}$. Accordingly, the measuring bases used by the center in step 5) should be replaced by $\{|0\rangle_{\mathrm{L}}, |1\rangle_{\mathrm{L}}\}$ and $\{|+\rangle_{\mathrm{L}}, |-\rangle_{\mathrm{L}}\}$.

3.2.2. Fault-tolerant MQKD protocol against collective-rotation noise

The collective-rotation noise[42,45,63] can be described as

$$\begin{aligned} &|0\rangle \longrightarrow \cos\theta|0\rangle + \sin\theta|1\rangle, \\ &|1\rangle \longrightarrow -\sin\theta|0\rangle + \cos\theta|1\rangle, \end{aligned} \tag{11}$$

where θ is the parameter of noise which fluctuates with time. Two Bell states, $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$, are invariant under this collective-rotation noise. Naturally, logical qubits in this case can be chosen as

$$|0_{\rm r}\rangle_{\rm L} = |\Phi^+\rangle, \quad |1_{\rm r}\rangle_{\rm L} = |\Psi^-\rangle. \tag{12}$$

For secure communication, at least two non-orthogonal measuring bases are required. According to the presented method, one basis could be $\{|0_{\rm r}\rangle_{\rm L}, |0_{\rm r}\rangle_{\rm L}\}$, and the other one is $\{|+_{\rm r}\rangle_{\rm L}, |-_{\rm r}\rangle_{\rm L}\}$, where

$$\begin{aligned} |+_{\rm r}\rangle_{\rm L} &= \frac{1}{\sqrt{2}}(|0_{\rm r}\rangle_{\rm L} - {\rm i}|1_{\rm r}\rangle_{\rm L}), \\ |-_{\rm r}\rangle_{\rm L} &= \frac{1}{\sqrt{2}}(|1_{\rm r}\rangle_{\rm L} - {\rm i}|0_{\rm r}\rangle_{\rm L}). \end{aligned} \tag{13}$$

It is easy to verify that $|\langle_{\rm r}+|0_{\rm r}\rangle_{\rm L}|^2 = |\langle_{\rm r}+|1_{\rm r}\rangle_{\rm L}|^2 = |\langle_{\rm r}-|0_{\rm r}\rangle_{\rm L}|^2 = |\langle_{\rm r}-|1_{\rm r}\rangle_{\rm L}|^2 = 1/2$, which indicates that $\{|0_{\rm r}\rangle_{\rm L}, |1_{\rm r}\rangle_{\rm L}\}$ and $\{|+_{\rm r}\rangle_{\rm L}, |-_{\rm r}\rangle_{\rm L}\}$ form two mutually unbiased bases. Using the method given in Section 2, we construct the encoding operation $U_{\rm r}$ and controlling operation $C_{\rm r}$ for the MQKD protocol over the collective-rotation channel as follows:

$$\begin{aligned} U_{\rm r} &= |0_{\rm r}\rangle_{\rm LL}\langle 1_{\rm r}| + |1_{\rm r}\rangle_{\rm LL}\langle_{\rm r}0| + M_{\rm r} \\ &= |\phi^+\rangle\langle\psi^-| + |\psi^-\rangle\langle\phi^+| + |\psi^+\rangle\langle\phi^-| + |\phi^-\rangle\langle\psi^+| \\ &= \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \end{pmatrix}, \\ C_{\rm r} &= \sqrt{U_{\rm r}} = \frac{1+{\rm i}}{2}\begin{pmatrix} 1 & -{\rm i} & 0 & 0 \\ -{\rm i} & 1 & 0 & 0 \\ 0 & 0 & 1 & {\rm i} \\ 0 & 0 & {\rm i} & 1 \end{pmatrix}. \end{aligned} \tag{14}$$

The effect of the operations $U_{\rm r}$ and $C_{\rm r}$ on the four states can be illustrated as

$$\begin{aligned} &U_{\rm r}|0_{\rm r}\rangle_{\rm L} = |1_{\rm r}\rangle_{\rm L}, && U_{\rm r}|1_{\rm r}\rangle_{\rm L} = |0_{\rm r}\rangle_{\rm L}, \\ &U_{\rm r}|+_{\rm r}\rangle_{\rm L} = |-_{\rm r}\rangle_{\rm L}, && U_{\rm r}|-_{\rm r}\rangle_{\rm L} = |+_{\rm r}\rangle_{\rm L}, \\ &C_{\rm r}|0_{\rm r}\rangle_{\rm L} = \left(\frac{1+{\rm i}}{\sqrt{2}}\right)|+_{\rm r}\rangle_{\rm L}, && C_{\rm r}|+_{\rm r}\rangle_{\rm L} = \left(\frac{1-{\rm i}}{\sqrt{2}}\right)|1_{\rm r}\rangle_{\rm L}, \\ &C_{\rm r}|1_{\rm r}\rangle_{\rm L} = \left(\frac{1+{\rm i}}{\sqrt{2}}\right)|-_{\rm r}\rangle_{\rm L}, && C_{\rm r}|-_{\rm r}\rangle_{\rm L} = \left(\frac{1-{\rm i}}{\sqrt{2}}\right)|0_{\rm r}\rangle_{\rm L}. \end{aligned} \tag{15}$$

In this case, with the help of the center, any two of the involved users can establish a shared secret key over the collective-rotation channel with the same steps of the protocol presented in Subsection 3.1. Of course, there are some differences between these two cases. One difference is that the four states $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|-\rangle$ should be respectively replaced by $|0_{\rm r}\rangle_{\rm L}$, $|1_{\rm r}\rangle_{\rm L}$, $|+_{\rm r}\rangle_{\rm L}$, and $|-_{\rm r}\rangle_{\rm L}$. Another difference is that the unitary operations $I_{\rm s}$, $U_{\rm s}$, and $C_{\rm s}$ should be substituted with $I_{\rm s}^{\otimes 2}$, $U_{\rm r}$, and $C_{\rm r}$, respectively. Accordingly, the measuring bases used by the center in step 5 should be replaced by bases $\{|0_{\rm r}\rangle_{\rm L}, |1_{\rm r}\rangle_{\rm L}\}$ and $\{|+_{\rm r}\rangle_{\rm L}, |-_{\rm r}\rangle_{\rm L}\}$.

3.2.3. Fault-tolerant MQKD protocol against all kinds of unitary collective noise

Decoherence-free (DF) states[43,54] are a type of state which is changeless under any n-lateral unitary transformation (i.e., $U^{\otimes n}|\psi^-\rangle = |\psi^-\rangle$, where $U^{\otimes n} = U \otimes \cdots \otimes U$ denotes the tensor product of n unitary transformations U). The amount of quantum information that a given N-qubit DFS is able to protect depends on the number of its qubits. If N is even, the DFS spanned by the eigenstates of the whole Hamiltonian of the qubit–bath system has dimension[43,50]

$$d(N) = \frac{N!}{(N/2)!(N/2+1)!}. \tag{16}$$

For $N = 2$, there exists only one DF state, the singlet state $|\psi^-\rangle$. For $N = 4$, the dimension of the DFS is 2. Hence, 4 qubits are sufficient to fully protect one arbitrary logical qubit from all kinds of unitary collective noise.[50] A natural choice for the orthogonal basis of the 4-qubit DFS is

$$\begin{aligned} |\bar{0}\rangle_{\rm L} &= |\psi^-\rangle_{12}|\psi^-\rangle_{34} = \frac{1}{2}(|0101\rangle + |1010\rangle \\ &\quad - |0110\rangle - |1001\rangle)_{1234}, \\ |\bar{1}\rangle_{\rm L} &= \frac{1}{2\sqrt{3}}(2|0011\rangle + 2|1100\rangle - |0101\rangle \\ &\quad - |1010\rangle - |0110\rangle - |1001\rangle)_{1234}. \end{aligned} \tag{17}$$

To communicate securely, at least two non-orthogonal measuring bases are required. According to the presented method, One basis could be $\{|\bar{0}\rangle_{\rm L}, |\bar{1}\rangle_{\rm L}\}$, and the other one should be chosen as $\{|\bar{+}\rangle_{\rm L}, |\bar{-}\rangle_{\rm L}\}$, where

$$|\bar{+}\rangle_{\rm L} = \frac{1}{\sqrt{2}}(|\bar{0}\rangle_{\rm L} - {\rm i}|\bar{1}\rangle_{\rm L}), \quad |\bar{-}\rangle_{\rm L} = \frac{1}{\sqrt{2}}(|\bar{1}\rangle_{\rm L} - {\rm i}|\bar{0}\rangle_{\rm L}). \tag{18}$$

It can be easily verified that $|\langle\bar{+}|\bar{0}\rangle_{\rm L}|^2 = |\langle\bar{+}|\bar{1}\rangle_{\rm L}|^2 = |\langle\bar{-}|\bar{0}\rangle_{\rm L}|^2 = |\langle\bar{-}|\bar{1}\rangle_{\rm L}|^2 = 1/2$, which means $\{|\bar{0}\rangle_{\rm L}, |\bar{1}\rangle_{\rm L}\}$ and $\{|\bar{+}\rangle_{\rm L}, |\bar{-}\rangle_{\rm L}\}$ form two mutually unbiased bases. Let us suppose that W is the 4-qubit Hilbert space whose dimension is 16, then we are able to find an orthonormal basis $\{|\bar{0}\rangle_{\rm L}, |\bar{1}\rangle_{\rm L}, \ldots, |\bar{15}\rangle\}$ for W by employing the Gram–Schmidt procedure. For the sake of simplicity, we do not give the concrete form of the states $|\bar{2}\rangle_{\rm L}$, $|\bar{3}\rangle_{\rm L}$, …, $|\bar{15}\rangle$ as the well known Gram–Schmidt procedure is not complicated. Once obtaining all the states of the orthonormal basis, we can construct the corresponding encoding operation $\bar{U}$ and controlling operation $\bar{C}$ for our robust MQKD protocol based the presented method. The encoding operation $\bar{U}$ and controlling operation $\bar{C}$ are in the forms

$$\bar{U} = |\bar{0}\rangle\langle\bar{1}| + |\bar{1}\rangle\langle\bar{0}| + O, \quad \bar{C} = \sqrt{\bar{U}}. \tag{19}$$

Here, we have many feasible choices for O, such as $O = |\bar{2}\rangle\langle\bar{2}| + \cdots + |\bar{15}\rangle\langle\bar{15}|$ and $O = |\bar{2}\rangle\langle\bar{3}| + |\bar{3}\rangle\langle\bar{4}| + \cdots + |\bar{15}\rangle\langle\bar{2}|$.

When $O = |\bar{2}\rangle\langle\bar{3}| + |\bar{3}\rangle\langle\bar{4}| + \cdots + |\bar{1}\bar{5}\rangle\langle\bar{2}|$, the effect of operations $\bar{U}$ and $\bar{C}$ on the states can be illustrated as

$$\begin{aligned}
&\bar{U}|\bar{0}\rangle_{\rm L} = |\bar{1}\rangle_{\rm L}, && \bar{U}|\bar{1}\rangle_{\rm L} = |\bar{0}\rangle_{\rm L},\\
&\bar{U}|\bar{+}\rangle_{\rm L} = |\bar{-}\rangle_{\rm L}, && \bar{U}|\bar{-}\rangle_{\rm L} = |\bar{+}\rangle_{\rm L},\\
&\bar{C}|\bar{0}\rangle_{\rm L} = \left(\frac{1+{\rm i}}{\sqrt{2}}\right)|\bar{+}\rangle_{\rm L}, && \bar{C}|\bar{+}\rangle_{\rm L} = \left(\frac{1-{\rm i}}{\sqrt{2}}\right)|\bar{1}\rangle_{\rm L},\\
&\bar{C}|\bar{1}\rangle_{\rm L} = \left(\frac{1+{\rm i}}{\sqrt{2}}\right)|\bar{-}\rangle_{\rm L}, && \bar{C}|\bar{-}\rangle_{\rm L} = \left(\frac{1-{\rm i}}{\sqrt{2}}\right)|\bar{0}\rangle_{\rm L}. \quad (20)
\end{aligned}$$

In this case, with the help of the center, any two of the involved users can establish a shared secret key over the channel with all kinds of collective-noise with the same steps described in the protocol proposed in Subsection 3.1. Certainly, there are some differences between these two cases. That is, the four states $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|-\rangle$ should be respectively substituted with $|\bar{0}\rangle_{\rm L}$, $|\bar{1}\rangle_{\rm L}$, $|\bar{+}\rangle_{\rm L}$, and $|\bar{-}\rangle_{\rm L}$, and the unitary operations $I_{\rm s}$, $U_{\rm dp}$, and $C_{\rm dp}$ should be replaced by $I_{\rm s}^{\otimes 4}$, $\bar{U}$, and $\bar{C}$, respectively. Accordingly, the center should utilize the bases $\{|\bar{0}\rangle_{\rm L}, |\bar{1}\rangle_{\rm L}\}$ and $\{|\bar{+}\rangle_{\rm L}, |\bar{-}\rangle_{\rm L}\}$ to measure each of the states in S_2 in step 5.

4. Security analysis

In this section, we analyze the security of the MQKD protocol with single particles. For the security of the ones over collective-noise channels, it can be analyzed in the same way. For clarity, we first consider the attacks from outside eavesdroppers. After that, we take into account the situation in which the center tries to eavesdrop the key.

4.1. Security against outside attacks

Let us assume that Eve is an attacker who wants to eavesdrop the users' secret key without being noticed in the eavesdropping detection. Eve could intercept the traveling particles sent to the receiver and replace them with the ones prepared by herself,[55] or she can entangle the travelling particles with additional states and try to extract information from these states.[64] Since the secret strings of the users are encoded on the travelling particles via the operations performed, the action to eavesdrop on the users' secret strings is equivalent to discriminating between the operations that they have performed. For instance, if Eve wants to obtain the value of A_i $(1 \leq i \leq 4n)$, she should know which one of the operations $I_{\rm s}$, $U_{\rm s}$, $C_{\rm s}$, and $U_{\rm s}C_{\rm s}$ Alice has performed on the corresponding particle. In other words, Eve should be capable of discriminating between the four unitary operations. Actually, the quantum operation discrimination has been well studied. In addition to Theorem 1 and Corollary 2, here we introduce another theorem.

Theorem 3[65] The quantum operations $\gamma_1, \ldots, \gamma_n$ can be unambiguously discriminated by a single operation if and only if for any $i = 1, 2, \ldots, n$, $\mathrm{supp}(\gamma_i) \nsubseteq \mathrm{supp}(S_i)$, where $\mathrm{supp}(\gamma)$ denotes the support of quantum operation γ and $S_i = \{\gamma_j : j \neq i\}$.

In the proposed protocol with single particles, the unitary operations performed by both users (Alice and Bob) can be viewed as a whole with four unitary operations, i.e. $I_{\rm s}$, $U_{\rm s}$, $C_{\rm s}$, and $U_{\rm s}C_{\rm s}$. Here, $I_{\rm s}$ is the identity density operator on the two-dimensional Hilbert space and the operations $U_{\rm s}$ and $C_{\rm s}$ are respectively the encoding operation and controlling operation defined in Eq. (4). It can be easily found that these operations satisfy $C_{\rm s} = \frac{1+{\rm i}}{2}(1 \cdot I_{\rm s} - {\rm i} \cdot U_{\rm s} + 0 \cdot U_{\rm s}C_{\rm s}) = \frac{1+{\rm i}}{2}(I_{\rm s} - {\rm i}U_{\rm s})$, which indicates that $\mathrm{supp}\{C_{\rm s}\} \subseteq \mathrm{supp}\{I_{\rm s}, U_{\rm s}, U_{\rm s}C_{\rm s}\}$. Therefore, these four operations cannot be unambiguously discriminated by a single operation (i.e., with only one opportunity) according to Theorem 3. Moreover, we can also obtain the same conclusion according to Theorem 1. For example, the eigenvalues of the operator $U_{\rm s}^{\dagger}C_{\rm s}$ are 1 and $-{\rm i}$, therefore, $r(U_{\rm s}^{\dagger}C_{\rm s}) = 1/\sqrt{2}$ and the minimum error probability to discriminate $U_{\rm s}$ and $C_{\rm s}$ is

$$P_{\rm e}(U_{\rm s}, C_{\rm s}) = \frac{1}{2}\left[1 - \sqrt{1 - (1/\sqrt{2})^2}\right] \approx 0.15. \quad (21)$$

In the same way, we obtain the minimum error probability $P_{\rm e}(I_{\rm s}, C_{\rm s}) = P_{\rm e}(I_{\rm s}, U_{\rm s}C_{\rm s}) = P_{\rm e}(U_{\rm s}, U_{\rm s}C_{\rm s}) \approx 0.15$, which means that these operations cannot be discriminated unambiguously under the condition that the device can be accessed only once.

In the proposed protocol, the users' secret strings are encoded in the operations they performed on the states. If Eve wants to obtain a bit of a user's secret string without leaving a trace in the eavesdropping detection, she should have the ability of unambiguously finding out which of $I_{\rm s}$, $U_{\rm s}$, $C_{\rm s}$, and $U_{\rm s}C_{\rm s}$ has been performed on the corresponding particle with only one opportunity. However, as we analyzed above, the four operations cannot be unambiguously discriminated under this condition. Consequently, well-known attacks, such as the intercept-resend attack, the measurement-resend attack, the entanglement-measure attack, and the dense-coding attack, from an outside eavesdropper will inevitably be found in the eavesdropping detection.

Furthermore, as for the two special attacks of two-way communication, i.e., the Trojan horse attack and the invisible-photon attack, the users and the center can make use of the methods in Refs. [61] and [62] to protect the proposed protocols. Hence, we omit a redundant description here.

4.2. Security against the center's attacks

It is known that an attack from a dishonest participant is more powerful than those from the outside eavesdroppers. On one hand, he knows parts of the legal information. On the other hand, he could tell lies in the executing procedure of the protocol to avoid being detected. Therefore, attacks from dishonest participants should be paid more attention. Such situations should also be considered in our protocol. First, in the

case that the center has been corrupted by others, he may try to eavesdrop the random key shared between the users. Second, in some special situations, the center may be out of service and a person who has the ability of generating and measuring the quantum states may want to eavesdrop the key. That is, the one who is able to substitute the center may be dishonest. Now, we show that, if the users use the proposed protocol, a dishonest center cannot obtain the random key without leaving a trace in the eavesdropping detection,

Compared with the outside eavesdroppers, a dishonest center has the following two superiorities. First, he could replace the particles in S with whatever kind of states he wants. Second, he could modify the measurement outcomes which are announced in step 5. Nevertheless, he is still unable to obtain the key shared between the users without being noticed in the eavesdropping detection of our protocol. According to the analysis given above, no matter what kind of states the dishonest center has prepared in step 2, he is unable to unambiguously discriminate between the four unitary operations performed by the users under the condition that the device can be accessed only once. In other words, these four unitary operations cannot be precisely discriminated when they are performed on a single qubit or one qubit of any entangled state. That is to say, if the center utilizes a strategy to discriminate between these four operations, he will obtain an incorrect outcome with a non-negligible probability. In our protocol, the users will announce the controlling string A' and B' only after the center publishes the measurement outcomes of all the particles in S_2. Also the bits utilized to check eavesdropping are randomly chosen by the users after the measurement outcomes are published. Since the dishonest center cannot precisely discriminate between the four unitary operations utilized in our protocol with only one opportunity, no matter what attack strategy he employs, once he obtains part of the useful information about the secret string, he will inevitably introduce errors into the eavesdropping detection and hence be noticed by the users.

Till now, we have analyzed the security of the MQKD protocol in Subsection 3.1 to show that it is secure against attacks from both the outside eavesdroppers and the dishonest center. For the fault-tolerant MQKD protocols against collective-dephasing noise, collective-rotation noise, and all kinds of unitary collective noise, we can show that they can be immune to all the present attacks in just the same way, since the operations in $\{I^{\otimes 2}, U_{\rm dp}, C_{\rm dp}, U_{\rm dp}C_{\rm dp}\}$/ $\{I^{\otimes 2}, U_{\rm r}, C_{\rm r}, U_{\rm r}C_{\rm r}\}$/$\{I^{\otimes 4}, \bar{U}, \bar{C}, \bar{U}\bar{C}\}$ cannot be discriminated unambiguously (under the condition that the device can be accessed only once) according to the theorems given above.

5. Discussion and conclusion

5.1. Discussion

To combat the errors introduced by the collective-noise channel, Zhang has proposed a well-known fault-tolerant multiparty quantum secret sharing (MQSS) protocol.[28] It is easy to find that this MQSS protocol can also be used for MQKD. However, there are clear differences between this protocol and our protocol. First, by utilizing our protocol, two arbitrary users could establish a secret key with the help of the center, and then they could utilize this key for secure communication between each other. In this circumstance, the center is unable to obtain any useful information of the shared key. While by employing Zhang's protocol, a boss could establish a joint key with his agents. Only when all the agents collaborate can they deduce the joint key and then utilize this key for secure communication with the boss. Second, as there exists a serving center in our protocol, if two of the involved users want to establish a secret key, they only need to be capable of performing certain unitary operations. Nevertheless, in Zhang's protocol, if the boss wants to establish a joint key with his agents, the boss should be able to generate quantum states, and the agents should be capable of performing a certain unitary operation and measuring the quantum states. In addition, to establish a secret key, the quantum state sequence should be transmitted three times in our protocol, while the sequence in Zhang's protocol only needs to be transmitted twice.

In fact, with some minor modifications, the protocol proposed in Section 3 can also be used for secret sharing of a random key. Concretely, if we want this protocol to be used for QSS, the following modifications are needed. Firstly, in step 5, after the center finishes measuring all the received particles, he notifies the fact to Alice and Bob. Different to the original protocol, he no longer publishes the measurement outcomes. Secondly, in step 6, once receiving the center's notification, Alice and Bob publish $\bar{A}'$ and $\bar{B}'$. With this information, the center judges which of the received particles have been measured in correct measuring bases. Then he informs Alice and Bob of the positions of the particles which have been measured incorrectly. With the positions, Alice and Bob discard the corresponding bits in A, B, A', and B', and obtain new strings which are denoted as $\bar{A}$, $\bar{B}$, $\bar{A}'$, and $\bar{B}'$, respectively. Then the center deduces a $2n$-bit string C according to the corresponding $2n$ measurement outcomes obtained from correct measuring bases. The relationship among the bit values of $\bar{A}_j$, $\bar{B}_j$, $\bar{A}'_j + \bar{B}'_j$, and C_j is shown in Table 1, where $1 \leq j \leq 2n$. Thirdly, in step 7, the center randomly chooses n positions out of string C and requires Alice and Bob to tell him the corresponding bits in $\bar{A}$ and $\bar{B}$, respectively. According to the received information and Table 1, the center checks whether

there exists eavesdropping in the executing procedure of the protocol. If no eavesdropping exists, the center has successfully established a joint key with Alice and Bob. That is to say, only when Alice and Bob collaborate can they first establish a joint key with the center and then extract the secret messages from the center's encrypted messages later transmitted via a public channel.

So far, we have shown that the protocol proposed in Section 3 can be used for three-party QSS with some minor modifications. Nevertheless, QSS has different security requirements from QKD. On one hand, the boss (i.e., the message sender) of a QSS protocol is honest. On the other hand, the agents (i.e., sharers) of a QSS protocol may be dishonest. That is to say, some dishonest agents may cooperate to attack the protocol and try to obtain the key without the help of other agents. According to the security analysis given in Section 4, it is not hard to find that the three-party QSS we just mentioned is secure. However, when the number of agents is more than two, many more threatening attacking strategies for QSS, such as the entanglement swapping attack,[39] should be considered. That is to say, to extend the above three-party protocol to an n-party one, some extra strategies should be employed for resisting these attacks. As the related strategies have been discussed somewhere else,[40] we do not focus on this issue here.

5.2. Conclusion

We introduce a method for constructing encoding operations and controlling operations, which are required in the MQCP-CD. Then by employing single particles and collective detection, we present an MQKD protocol on a star network without storing qubits, which can resist attacks from both outside eavesdroppers and a dishonest center. Based on the proposed method and the idea of DFS, we also introduce three fault-tolerant versions of the proposed protocol against collective-dephasing noise, collective-rotation noise, and all kinds of unitary collective noise.

Obviously, the presented method is useful as it can be used to construct the unitary operations required in the MQCP-CD with different kinds of quantum states. Compared with the existing MQCP-CDs,[34–41] the protocols proposed in this paper have the following advantages. First, the proposed protocols are more feasible since they do not need to employ a quantum storage machine. Second, the proposed protocols can not only utilize the collective detection, but also be immune to the collective noise.

References

[1] Bennett C H and Brassard G 1984 *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processings* Bangalore, India, pp. 175–179
[2] Ekert A E 1991 *Phys. Rev. Lett.* **67** 661
[3] Deng F G and Long G L 2003 *Phys. Rev. A* **68** 042315
[4] Deng F G and Long G L 2004 *Phys. Rev. A* **70** 012311
[5] Li H W, Yin Z Q, Wang S, Bao W S, Guo G C and Han Z F 2011 *Chin. Phys. B* **20** 100306
[6] Phoenix S, Barnett S, Townsend P and Blow K 1995 *J. Modern Opt.* **42** 1155
[7] Lin S, Huang C and Liu X F 2013 *Phys. Scr.* **87** 035008
[8] Lo H K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[9] Tang Y L, Yin H L and Chen S J 2014 *Phys. Rev. Lett.* **113** 190501
[10] Wang Y, Bao W S, Li H W, Zhou C and Li Y 2014 *Chin. Phys. B* **23** 080303
[11] Wang X B 2007 *Phys. Rev. A* **75** 052301
[12] Tomamichel M, Lim C C W, Gisin N and Renner R 2012 *Nat. Commun.* **3** 634
[13] Zhao L Y, Li H W, Yin Z Q, Chen W, You J and Han Z F 2014 *Chin. Phys. B* **23** 100304
[14] Huang P, Fan J and Zeng G H 2014 *Phys. Rev. A* **89** 042330
[15] Long G L and Liu X S 2002 *Phys. Rev. A* **65** 032302
[16] Boström, K and Felbinger T 2002 *Phys. Rev. Lett.* **89** 187902
[17] Wang C, Deng F G, Li Y S, Liu X S and Long G L 2005 *Phys. Rev. A* **71** 044305
[18] Deng F G and Long G L 2004 *Phys. Rev. A* **69** 052319
[19] Deng F G, Long G L and Liu X S 2003 *Phys. Rev. A* **68** 042317
[20] Man Z X, Zhang Z J and Li Y 2005 *Chin. Phys. Lett.* **22** 18
[21] Gu B, Huang Y G, Fang X and Chen Y L 2013 *Int. J. Theor. Phys.* **52** 4461
[22] Ye T Y and Jiang L Z 2013 *Chin. Phys. Lett.* **30** 040305
[23] Hillery M, Bužek V and Bérthiaume A 1999 *Phys. Rev. A* **59** 1829
[24] Wang T Y and Wen Q Y 2011 *Quant. Inf. Comput.* **11** 434
[25] Yang Y G, Wang Y A, Chai H P, Teng Y W and Zhang H 2013 *Opt. Commun.* **284** 3479
[26] Zhou N R, Song H C and Gong L H 2013 *Int. J. Theor. Phys.* **52** 4174
[27] Chen X B, Xu G, Su Y and Yang Y X 2014 *Quant. Inf. Comput.* **14** 589
[28] Zhang Z J 2006 *Phys. A* **361** 233
[29] Wang T Y, Cai X Q and Zhang R L 2014 *Quantum Inf. Process.* **13** 1677
[30] Yang Y G and Wen Q Y 2009 *J. Phys. A: Math. Theor.* **42** 055305
[31] Zeng G H, Lee M H, Guo Y and He G Q 2007 *Int. J. Quantum Inf.* **5** 553
[32] Zeng G H, Keitel C H 2002 *Phys. Rev. A* **65** 042312
[33] Wen X J 2010 *Phys. Scr.* **82** 065403
[34] Shih H, Lee K and Hwang T 2009 *IEEE J. Sel. Top. Quant. Electron.* **15** 1602
[35] Gao F, Qin S J, Guo F Z and Wen Q Y 2011 *IEEE J. Quant. Electron.* **47** 630
[36] Liu B, Gao F and Wen Q Y 2011 *IEEE J. Quant. Electron.* **47** 1383
[37] Liu B, Gao F, Jia H Y and Huang W 2013 *Quantum Inf. Process.* **12** 887
[38] Lin S, Wen Q Y, Qin S J and Zhu F C 2009 *Opt. Commun.* **282** 4455
[39] Gao G 2010 *Opt. Commun.* **283** 2997
[40] Liu B, Gao F and Wen Q Y 2011 *Int. J. Theor. Phys.* **51** 1211
[41] Huang W, Wen Q Y, Liu B, Gao F and Chen H 2012 *Int. J. Theor. Phys.* **51** 2787
[42] Li X H, Deng F G and Zhou H Y 2008 *Phys. Rev. A* **78** 022321
[43] Zanardi P and Rasetti M 1997 *Phys. Rev. Lett.* **79** 3306
[44] Lin S 2014 *Quantum Inf. Comput.* **14** 845
[45] Yang Y G, Teng Y W, Chai H P and Wen Q Y 2011 *Phys. Scr.* **83** 025003
[46] Yang C W, Tsai C W amd Hwang T 2013 *Quantum Inf. Process.* **12** 3043
[47] Wu G T, Zhou N R, Gong L H and Liu S Q 2014 *Acta Phys. Sin.* **63** 060302 (in Chinese)
[48] Chang Y, Zhang S B, Li J and Yan L L 2014 *Sci. China-Phys. Mech. Astron.* **57** 1907
[49] Huang W, Wen Q Y, Jia H Y, Qin S J and Gao F 2012 *Chin. Phys. B* **21** 100308
[50] Cabello A 2007 *Phys. Rev. A* **75** 020301
[51] Sun Y, Wen Q Y, Gao F and Zhu F C 2009 *Phys. Rev. A* **80** 032321
[52] Gu B, Zhang C Y, Cheng G S and Huang Y G 2011 *Sci. China-Phys. Mech. Astron.* **54** 942

[53] Walton Z D, Abouraddy A F and Sergienko A V 2003 *Phys. Rev. Lett.* **91** 087901
[54] Kwiat P G, Berglund A J, Altepeter J B and White A G 2000 *Science* **290** 498
[55] Qin S J, Gao F, Wen Q Y and Zhu F C 2006 *Phys. Lett. A* **357** 101
[56] Zhang Z J, Li Y and Man Z X 2005 *Phys. Rev. A* **71** 044301
[57] Deng F G, Li X H, Chen P and Zhou H Y 2006 *arXiv:* 0604060
[58] Mauro D'Ariano G, Presti P L and Paris M G A 2001 *Phys. Rev. Lett.* **87** 270404
[59] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
[60] Deutsch D, Ekert A, Jozsa R, Macchiavello C, Popescu S and Sanpera A 1996 *Phys. Rev. Lett.* **77** 2818
[61] Cai Q Y 2006 *Phys. Lett. A* **351** 23
[62] Li X H, Deng F G and Zhou H Y 2006 *Phys. Rev. A* **74** 054302
[63] Xie C M, Liu Y M, Li G F and Zhang Z J 2014 *Quantum Inf. Process.* **13** 2713
[64] Gao F, Qin S J, Wen Q Y and Zhu F C 2010 *Opt. Commun.* **283** 192
[65] Wang G M and Ying M S 2006 *Phys. Rev. A* **73** 042301