Quantum Inf Process (2016) 15:2101–2111
DOI 10.1007/s11128-016-1253-8

Efficient multiparty quantum key agreement protocol based on commutative encryption

Zhiwei Sun[1,2] · **Jiwu Huang**[1] · **Ping Wang**[2]

Received: 19 November 2015 / Accepted: 19 January 2016 / Published online: 9 February 2016

Abstract A secure multiparty quantum key agreement protocol using single-qubit states is proposed. The agreement key is computed by performing exclusive-OR operation on all the participants' secret keys. Based on the commutative property of the commutative encryption, the exclusive-OR operation can be performed on the plaintext in the encrypted state without decrypting it. Thus, it not only protects the final shared key, but also reduces the complexity of the computation. The efficiency of the proposed protocol, compared with previous multiparty QKA protocols, is also improved. In the presented protocol, entanglement states, joint measurement and even the unitary operations are not needed, and only rotation operations and single-state measurement are required, which are easier to be realized with current technology.

Keywords Quantum key agreement · Superposition states · Commutative encryption

1 Introduction

Quantum key distribution (QKD) allows two authorized participants to establish a shared secret key over a public channel. The shared key can be used for encryption or authentication protocols. A lot of QKD protocols have been proposed [1,2] since the

✉ Ping Wang
wangping@szu.edu.cn

Zhiwei Sun
sunzhiwei1986@gmail.com

1 Shenzhen Key Laboratory of Media Security, Shenzhen University, Shenzhen 518060, People's Republic of China

2 College of Information Engineering, Shenzhen University, Shenzhen 518060, Guangdong, People's Republic of China

pioneering works of Bennett–Brassard (BB84) [3] and Ekert (E91) [4], and they have been theoretically proven unconditionally secure [5]. Key agreement is another way to distribute keys, i.e., it allows two or more parties to establish a secret key freely and securely over insecure channel without the need for a previously established shared secret. However, compared with the key distribution, in which one party distributes a secret key to the other, all involved parties in a key agreement protocol can equally influence the outcome of the protocol, and no one can decide the shared key alone. In other words, in addition to have the same ability of resisting adversaries from the outside world as the key distribution protocol does, a secure key agreement protocol is also required to prevent the participant attacks, i.e., the dishonest party may try to determine the secret key alone. Therefore, it is useful to establish a shared key by the key agreement protocol in the scenario that all participants do not trust each other. The first practical solution to the key agreement problem was proposed in 1976 [6] by Deffie and Hellman (DH). Since their pioneering work, a large number of variant solutions to the key agreement were proposed. However, the security of these protocols is mainly based on the DH problem or discrete logarithm problem. Since Shor introduced a polynomial-time quantum algorithms for prime factorization and discrete logarithm in 1997 [7], the security of classical key agreement protocols become increasingly vulnerable. Fortunately, quantum cryptography, which is based on the principle of quantum mechanical to perform cryptographic tasks, can provide unconditional security. And it attracts many researchers' attention and has been developed quickly, such as quantum secret sharing [8,9], quantum secure direct communication [10,11], quantum private comparison [12–14] and quantum oblivious transfer [15].

Quantum key agreement (QKA) is a new branch of quantum cryptography, which was first proposed by Zhou et al. [16]. In their protocol, the quantum teleportation technique was used to generate a secret key. However, one party can fully determine the shared key alone [17], and it is susceptible to the participant attack [18]. Later, Chong and Hwang [19] proposed a new QKA protocol by using the technique of delayed measurement. Recently, Huang et al. [20] considered the QKA protocol in the collective noise channels. Shen et al. proposed an efficient two-party QKA scheme with four-qubit cluster states [21], which has been extended to multiparty case [22]. However, only two participants were involved in the above QKA protocols. Recently, an enhanced interest on multiparty QKA protocols has been observed. Shi and Zhong [23] first proposed the multiparty QKA protocol based on EPR pairs and entanglement swapping. Liu et al. [24] found that their protocol was not a fair QKA because a dishonest participant can determine the secret key independently, and they presented a secure multiparty QKA protocol with single particles. However, the efficiency of the proposed protocol is not very satisfactory. How to improve the efficiency of the multiparty QKA protocol is an open problem in this field. In order to solve this problem, Sun et al. extended the classical circle-type conference key agreement to the quantum world and proposed a circle-type QKA protocol [25], and the efficiency of Liu et al.'s protocol was improved. Recently, three-party QKA [26] protocol and five-party QKA protocol [27] were also proposed based on Bell state.

In this paper, we propose a multiparty quantum key agreement protocol using quantum superposition states. The presented protocol uses a commutative encryption to protect participants' agreement key. The shared key is influenced by all parties. And no one can determine the shared key alone. The exclusive-OR operations of participants' secret keys is realized by the property of the commutative encryption. And the exclusive-OR operation is performed on the plaintext in the encrypted state without decrypting it. We encode the participant's secret key into particular rotation angles. Rotating the encryption state by 90° changes the plaintext, logic-one to logic-zero or logic-zero to logic-one. The efficiency of the proposed protocol, compared with other multiparty QKA protocols, is also improved. Entanglement states, joint measurement and even the unitary operations are not needed, and only rotation operations and single-state measurement are required. As it is known, rotation operation and single-state measurement are easier to be realized with current technologies. Thus, the proposed protocol is more practical, compared to other previous QKA protocols. The security of the presented protocol is also proved to be secure against both outside and participant attacks.

The rest of this paper is organized as follows. Section 2 introduces the commutative encryption scheme. Then, our multiparty QKA protocol with quantum superposition states is presented. The security analysis is given in Sect. 4. Section 5 gives a short conclusion.

2 A quantum commutative encryption scheme

In this section, we introduce a quantum commutative encryption scheme, which will be used in the proposed multiparty quantum key agreement protocol. In our protocol, the horizontally polarized photon $|0\rangle$ represents zero in a binary representation. The vertically polarized photon $|1\rangle$ represents one. And, all transmitted polarized photons are encrypted before the transmission. The encryption key is defined as a set of angles $K = \{\theta_i : 0 \leq \theta_i < \pi, i = 1, 2, \ldots, n\}$ for an n-bit message, where the subscript indicates the position in the message where the encryption with the angle θ_i is applied. The encryption is defined as the rotation operation. And, $E_K[M]$ is denoted as an encryption of data M with a secret key K. The decryption is defined as the rotation the encrypted photon by the angle θ_i in the opposite direction. $D_K[M]$ is the decryption of data M with the secret key K. We give a simple example to show the mathematical representation of the encryption and decryption processes as follows.

Suppose the message M is a single photon encoded as $M : |\psi_0\rangle = |0\rangle$ for simplicity. By using the Jones matrix representation, the rotation operation can be represented by the following matrix:

$$R(\theta) = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \tag{1}$$

The data qubit $|\psi_0\rangle$ encryption with θ can be represented as follows

$$\begin{aligned} E_K[M] &= R(\theta)|0\rangle \\ &= \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{aligned}$$

$$= \begin{pmatrix} \cos\theta \\ -\sin\theta \end{pmatrix} = \cos\theta|0\rangle - \sin\theta|1\rangle$$
$$= |\psi_0\rangle' \tag{2}$$

In order to read the message M, we need to rotate the photon $|\psi_0\rangle'$ by θ in the opposite direction, i.e., the decryption can be represented as follows:

$$R(-\theta)|\psi_0\rangle' = \begin{pmatrix} \cos(-\theta) & \sin(-\theta) \\ -\sin(-\theta) & \cos(-\theta) \end{pmatrix} \begin{pmatrix} \cos\theta \\ -\sin\theta \end{pmatrix}$$
$$= \begin{pmatrix} \cos^2\theta + \sin^2\theta \\ \sin\theta\cos\theta - \cos\theta\sin\theta \end{pmatrix}$$
$$= \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle \tag{3}$$

The security of this quantum encryption is proven in Ref. [28]. A main advantage of this encryption scheme is that we do not have to decrypt a cipher text in the exact reverse order as encrypted with different secret key. For example, $E_{K_2}E_{K_1}[M] = E_{K_1}E_{K_2}[M]$, where $K_1 \neq K_2$. And we know that rotating the photon by 90° changes the plaintext, logic-one to logic-zero or logic-zero to logic-one, i.e., $E_{\frac{\pi}{2}}|0\rangle = R(\frac{\pi}{2})|0\rangle = -|1\rangle$, $E_{\frac{\pi}{2}}|1\rangle = R(\frac{\pi}{2})|1\rangle = |0\rangle$ since the $-$ has no observable effects, and for that reason we can effectively write $E_{\frac{\pi}{2}}|0\rangle = |1\rangle$, $E_{\frac{\pi}{2}}|1\rangle = |0\rangle$. Therefore, an exclusive-OR operation can be performed on the plaintext in the encrypted state without decrypting it, i.e., he rotates 90° on the encoded state if the input is 1; otherwise, 0° is rotated. For example, suppose the input is 1, we have $K_2 = \frac{\pi}{2}$, then

$$E_{\frac{\pi}{2}}E_{K_1}|0\rangle = E_{K_1}R\left(\frac{\pi}{2}\right)|0\rangle = E_{K_1}|1\rangle = E_{K_1}|1 \oplus 0\rangle, \tag{4}$$
$$E_{\frac{\pi}{2}}E_{K_1}|1\rangle = E_{K_1}R\left(\frac{\pi}{2}\right)|1\rangle = E_{K_1}|0\rangle = E_{K_1}|1 \oplus 1\rangle, \tag{5}$$

where $\oplus$ denotes the addition module 2.

The rotation operation can be realized by current technologies. The photon is linearly polarized by a polarizing apparatus called linear polarizer and the direction can be determined by the orientation of the polarizer. In order to rotate the polarized photon, the photon is passed through a Faraday effect modulator. The rotation angle is controlled by the strength of the magnetic field parallel to the light beam. The output polarization from the Faraday effect modulator can be rotated by the desired angle [28].

3 Multiparty quantum key agreement protocol

Suppose that there are N participants $P_0, \ldots, P_{N-1}$, and they have secret bit strings keys $K_0, \ldots, K_{N-1}$, respectively (Eq.(6)). They want to derive a secret shared key

$K = K_0 \oplus \cdots \oplus K_{N-1}$ (Eq.(7)), wherein no one can determine the shared key alone.

$$\begin{aligned} K_0 &= (k_{0,1} \cdots k_{0,n}), \\ &\cdots \\ K_i &= (k_{i,1} \ldots k_{i,n}), \\ &\cdots \\ K_{N-1} &= (k_{(N-1),1} \ldots, k_{(N-1),n}), \qquad (6) \\ K_0 \oplus \cdots \oplus K_{N-1} &= (k_{0,1} \oplus \cdots \oplus k_{(N-1),1} \ldots k_{0,n} \oplus \cdots \oplus k_{(N-1),n}). \qquad (7) \end{aligned}$$

Here n is the length of secret bit string. In our protocol, we assume that the classic channel is authenticated. Then, the multiparty QKA protocol can be described as follows:

1. The party $P_i (i = 0, \ldots, N-1)$ randomly generates a secret key $\Theta_i = (\theta_1^i, \theta_2^i, \ldots, \theta_n^i)$. Here, $0 \leq \theta_j^i < \pi, j = 1, 2, \ldots, n$. Then, he encodes his secret key K_i into n photons $|\psi_{K_i}\rangle = |\psi_{k_{i,1}}\rangle |\psi_{k_{i,2}}\rangle \ldots |\psi_{k_{i,n}}\rangle$. Here, if $k_{i,j} = 0$, $|\psi_{k_{i,j}}\rangle = |0\rangle$, otherwise $|\psi_{k_{i,j}}\rangle = |1\rangle$. P_i encrypts $|\psi_{K_i}\rangle$ with Θ_i. The resulting state can be written as

$$E_{\Theta_i}[|\psi_{K_i}\rangle] = R(\theta_1^i)|\psi_{k_{i,1}}\rangle \otimes \cdots \otimes R(\theta_n^i)|\psi_{k_{i,n}}\rangle, \qquad (8)$$

   where $R(\theta_j^i)$ is the rotation operation.
2. P_i sends $E_{\Theta_i}[|\psi_{K_i}\rangle]$ to $P_{(i+1)modN}$ using the decoy state method [29–31]. For example, he prepares κn decoy particles which are randomly in four states $|+\rangle$, $|-\rangle$, $|+y\rangle$, $|-y\rangle$, and inserts the κn decoy particles randomly in $E_{\Theta_i}[|\psi_{K_i}\rangle]$. Then he sends the $n+\kappa n$ photons to the next participant $P_{(i+1)modN}$. Here, κ is the detection rate, and $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, $|+y\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$, $|-y\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$. For simplicity, $P_{(i+1)modN}$ is denoted as P_{i+1} in the following parts.
3. After confirming that P_{i+1} has received the photons, P_i and P_{i+1} begin to check eavesdropping. For example, P_i announces the positions and the corresponding bases $\{|+\rangle, |-\rangle\}$ or $\{|+y\rangle, |-y\rangle$ of the decoy particles, and then P_{i+1} measures the decoy particles in the correct bases and randomly announces half of the measurement results. Then P_i announces the initial states of the left half of the decoy particles. If the initial states and the measurement results are consistent, they claim that $E_{\Theta_i}[|\psi_{K_i}\rangle]$ is secure; otherwise, they abandon the protocol.
4. If all the parties announce the received photons are secure, P_{i+1} performs the commutative encryption on the photons $E_{\Theta_i}[|\psi_{K_i}\rangle]$ according to his secret key K_{i+1}, i.e., if $k_{i+1,j} = 0$, the corresponding encryption key is $\theta_{i+1,j} = 0$; otherwise $\theta_{i+1,j} = \frac{\pi}{2}$, where $j = 1, 2, \ldots, n$.
5. After performing the commutative encryption, the photons $E_{\Theta_i}[|\psi_{K_i}\rangle]$ become $E_{\Theta_i}[|K_{i+1} \oplus K_i\rangle]$. Then, P_{i+1} sends the new photons to the next party P_{i+2} using the decoy- states method described in step 2.
6. The parties $P_{i+2}, \ldots, P_{i-1}$ sequentially execute eavesdropping check and the commutative encryption processes in the same way as participants did in steps

3–5, i.e., they, one after another, check eavesdroppers, and if all the photons are secure, they perform commutative encryption on the received photons according to their secret keys and then insert the decoy particles randomly in the photons and send them to the next participant.

7. When P_i has received the photons from P_{i-1}, he first does eavesdropping check with P_{i-1}. Then he obtains $E_{\Theta_i}[|K_{i-1} \oplus \cdots \oplus K_{i+1} \oplus K_i\rangle]$ if there is no eavesdropper. Then, he decrypts it with key Θ_i,

$$D_{\Theta_i}[E_{\Theta_i}[|K_{i-1} \oplus \cdots \oplus K_{i+1} \oplus K_i\rangle]] = |K_{i-1} \oplus \cdots \oplus K_{i+1} \oplus K_i\rangle. \quad (9)$$

The result of P_i's measurement on $|K_{i-1} \oplus \cdots \oplus K_{i+1} \oplus K_i\rangle$ is the final shared key $K = K_0 \oplus K_1 \oplus \cdots \oplus K_{N-1}$.

4 Security analysis of the presented multiparty QKA protocol

In this section, we will prove that the presented protocol is correct and secure.

4.1 Correctness of the presented protocol

Suppose P_i starts the protocol, and after his encryption in step 1, the photon states can be written as

$$E_{\Theta_i}[|\psi_{K_i}\rangle] = R(\theta_1^i)|\psi_{k_{i,1}}\rangle \otimes \cdots \otimes R(\theta_n^i)|\psi_{k_{i,n}}\rangle. \quad (10)$$

When P_{i+1} receives these secure photons, he perform the commutative encryption according to his secret key K_{i+1}, i.e.,

$$\begin{aligned} E_{K_{i+1}}E_{\Theta_i}[|\psi_{K_i}\rangle] &= R(\theta_{i+1,1})R(\theta_1^i)|\psi_{k_{i,1}}\rangle \otimes \cdots \otimes R(\theta_{i+1,n})R(\theta_n^i)|\psi_{k_{i,n}}\rangle \\ &= R(\theta_1^i)R(\theta_{i+1,1})|\psi_{k_{i,1}}\rangle \otimes \cdots \otimes R(\theta_n^i)R(\theta_{i+1,n})|\psi_{k_{i,n}}\rangle \\ &= E_{\Theta_i}[|K_{i+1} \oplus \psi_{K_i}\rangle] \\ &= E_{\Theta_i}[|K_{i+1} \oplus K_i\rangle], \end{aligned} \quad (11)$$

where $\theta_{i+1,j} = 0$ if $k_{i+1,j} = 0$ and $\theta_{i+1,j} = \frac{\pi}{2}$ if $k_{i+1,j} = 1$, $j = 1, 2, \ldots, n$.

Similarly, $P_{i+2}, \ldots, P_{i-1}$ sequentially execute the commutative encryption processes in the same way as participant P_{i+1} did. According to Eq. (11), the final quantum states that P_i receives in the step 7 is $E_{\Theta_i}[|K_{i-1} \oplus \cdots \oplus K_{i+1} \oplus K_i\rangle]$ if there is no eavesdropper. Since P_i has the secret key Θ_i, he can decrypt the received qubits and then measures them in the basis $\{|0\rangle, |1\rangle\}$. Thus, he obtains the shared secret key $K = K_0 \oplus K_1 \oplus \cdots \oplus K_{N-1}$ correctly.

4.2 Security analysis of the presented protocol

Since the decoy-state method is used in our protocol to detect Eve, outside eavesdroppers cannot obtain the shared key without being detected. In decoy-state method, besides target states, several other non-orthogonal states as decoy states are used. Since

Eve cannot distinguish between the target states and the decoy states, she has to apply the same strategy to all of them. As a result, any eavesdropping attempt by Eve will inevitably modify the photon statistic and expose her [29–31]. Without loss of generality, the most general operation U_E Eve employed is to cause the sample photons to interact coherently with an auxiliary quantum system $|E\rangle$ (if U_E is a swapping operation, this attack mode becomes the well-known intercept–resend attack), which can be defined as follows:

$$U_E|0\rangle|E\rangle = a|0\rangle|E_{00}\rangle + b|1\rangle|E_{01}\rangle, \tag{12}$$
$$U_E|1\rangle|E\rangle = c|0\rangle|E_{10}\rangle + d|1\rangle|E_{11}\rangle, \tag{13}$$

where $|a|^2 + |b|^2 = 1$ and $|c|^2 + |d|^2 = 1$. Since the decoy states involved in our protocol are $|+\rangle, |-\rangle, |+y\rangle$ and $|-y\rangle$, if Eve introduces no error in the eavesdropping check by participants, the general operation U_E must satisfy the following conditions:

$$\begin{aligned} U_E|+\rangle|E\rangle &= \frac{1}{\sqrt{2}}(a|0\rangle|E_{00}\rangle + b|1\rangle|E_{01}\rangle + c|0\rangle|E_{10}\rangle + d|1\rangle|E_{11}\rangle) \\ &= \frac{1}{2}(|+\rangle(a|E_{00}\rangle + b|E_{01}\rangle + c|E_{10}\rangle + d|E_{11}\rangle)). \end{aligned} \tag{14}$$

$$\begin{aligned} U_E|-\rangle|E\rangle &= \frac{1}{\sqrt{2}}(a|0\rangle|E_{00}\rangle + b|1\rangle|E_{01}\rangle - c|0\rangle|E_{10}\rangle - d|1\rangle|E_{11}\rangle) \\ &= \frac{1}{2}(|-\rangle(a|E_{00}\rangle - b|E_{01}\rangle - c|E_{10}\rangle + d|E_{11}\rangle)). \end{aligned} \tag{15}$$

$$\begin{aligned} U_E|+y\rangle|E\rangle &= \frac{1}{\sqrt{2}}(a|0\rangle|E_{00}\rangle + b|1\rangle|E_{01}\rangle + ic|0\rangle|E_{10}\rangle + id|1\rangle|E_{11}\rangle) \\ &= \frac{1}{2}(|+y\rangle(a|E_{00}\rangle - ib|E_{01}\rangle + ic|E_{10}\rangle + d|E_{11}\rangle)). \end{aligned} \tag{16}$$

$$\begin{aligned} U_E|-y\rangle|E\rangle &= \frac{1}{\sqrt{2}}(a|0\rangle|E_{00}\rangle + b|1\rangle|E_{01}\rangle - ic|0\rangle|E_{10}\rangle - id|1\rangle|E_{11}\rangle) \\ &= \frac{1}{2}(|-y\rangle(a|E_{00}\rangle + ib|E_{01}\rangle - ic|E_{10}\rangle + d|E_{11}\rangle)). \end{aligned} \tag{17}$$

From the above Eqs. (14), (15), (16) and (17), we can get

$$a|E_{00}\rangle - b|E_{01}\rangle + c|E_{10}\rangle - d|E_{11}\rangle = 0 \tag{18}$$
$$a|E_{00}\rangle + b|E_{01}\rangle - c|E_{10}\rangle - d|E_{11}\rangle = 0 \tag{19}$$
$$a|E_{00}\rangle + ib|E_{01}\rangle + ic|E_{10}\rangle - d|E_{11}\rangle = 0 \tag{20}$$
$$a|E_{00}\rangle - ib|E_{01}\rangle - ic|E_{10}\rangle - d|E_{11}\rangle = 0 \tag{21}$$

Here 0 denote a column zero vector. Further, we can get $a = d = 1$, $b = c = 0$ and $|E_{00}\rangle = |E_{11}\rangle$. Therefore,

$$U_E|0\rangle|E\rangle = |0\rangle|E_{00}\rangle, \tag{22}$$
$$U_E|1\rangle|E\rangle = |1\rangle|E_{00}\rangle, \tag{23}$$

i.e., Eve introduce no error in the eavesdropping only when her ancillary state and the target photon $\{|0\rangle, |1\rangle\}$ are product states. So outside eavesdroppers cannot obtain the shared key without being detected.

On the other hand, the security of commutative encryption relies on the no-cloning theorem. Hence, by transmitting data as a superposition of state, no one can make a copy of the transmitted data without errors. Without the secret key (rotation angles), no one can obtain the secret data (the shared key) according to measuring the superposition states. Therefore, the commutative encryption can also protect the shared key from exposing to Eve.

Therefore, our proposed protocol is secure against outside attacks.

Generally speaking, the participant is the most powerful attacker. The participant attack is a normal attack mode in the multiparty computation protocols that participants are not of mutual trust. If it is possible for one party (suppose P_i) to know the final key before others, she will completely control the shared key by manipulating her secret key K_i as per her wish. For example, suppose P_i has already obtain the shared key K, where K is the bitwise of all parties' keys. Then P_i encodes $K^{'} \oplus K \oplus K_i$, instead of K_i, as his secret key when he executes the protocol, where $K^{'}$ is the key that P_i desired. It can be easily computed that other parties will accept $K^{'}$ as the final shared key. Thus, this protocol is not a fair key agreement in this situation. To circumvent this attack, we require all participants, one after another, to check eavesdroppers, and only when all the transmitted photons are secure, they encode their secret key on these photons. This strategy introduces a delay in message encoding (commutative encryption operation), but this delayed message encoding strategy ensures that malicious participant cannot control the final key by knowing K prior to her message encoding. Thus, no one can get the final key beforehand, and all participants obtain the final key simultaneously. Therefore, the dishonest party has no way to influence the final key as her expected.

4.3 Efficiency analysis

A well-known measure of efficiency of secure quantum communication is known as qubit efficiency was introduced by Cabello [36], which is given as

$$\eta = \frac{c}{q + b}, \tag{24}$$

where c denotes the length of the transmitted message bits, q is the number of the used qubits and b is the number of classical bits exchanged for decoding of the message (classical communication used for checking of eavesdropping is not counted). Since the QKA protocols are not interested in communicating a message, so the meaning of c in η is modified to make it suitable for comparison of protocols of QKA. In the modified notion, c is the length of the shared key generated by the protocol. In the following part, we will take a simple comparison between previous proposed secure multiparty QKA protocols and ours from the following aspects: the quantum resource, the quantum operation and the qubit efficiency (Table 1). In order to generate n bits of shared key, each party has to prepare n single photons and κn decoy particles in our protocol. There is no classical bits exchanged for decoding of the shared key. Hence,

Table 1 Comparison between previously proposed multiparty QKA protocols and ours

Schemes	Entanglement	Joint measurements	Decoy states	Unitary operation	Qubit efficiency
Ref. [24]	No	No	Yes	No	$\frac{1}{(\kappa+1)N(N-1)}$
Ref. [25]	No	No	Yes	Yes	$\frac{1}{(\kappa+1)N}$
Ref. [22]	Yes	Yes	Yes	Yes	$\frac{2}{(\kappa+1)N}$
Ours	No	No	Yes	No	$\frac{1}{(\kappa+1)N}$

the qubit efficiency of our protocol can be computed, $\eta = \frac{n}{(n+\kappa n)N} = \frac{1}{(\kappa+1)N}$, where κ is the detection rate and N is the number of the participants. The Ref. [24] proposed a secure multiparty QKA protocol, and its qubit efficiency is $\frac{1}{(\kappa+1)N(N-1)}$, which is less efficient than ours. Later, an improved multiparty QKA protocol by using unitary operations was proposed by Sun et al. [25], which qubit efficiency is $\frac{1}{(\kappa+1)N}$. Later, an efficient multiparty QKA with cluster states was also proposed [22].Compared with Refs. [25] and [22], the qubit efficiency of our protocol is almost as efficient as their. However, entanglement states, joint measurement and even the unitary operations are not needed in our protocol, only rotation operations and single-state measurement are required. As it is known, rotation operation and single-state measurement are easier to be realized with current technologies. Thus, the proposed protocol is more practical, compared to these previous QKA protocols. Hence, our new protocol is more efficient than previous proposed secure multiparty QKA protocols (see Table 1).

5 Conclusion and discussion

We have proposed a multiparty quantum key agreement protocol based on superposition states. By transmitting data as a superposition of state, no one can make a copy of the transmitted state without errors. And, when the superposition state is measured, no information regarding the secret key is left. Thus, Eve cannot obtain the final shared secret key. The message encoding process is realized by the commutative encryption operation in our protocol. And the exclusive-OR operation is performed by utilizing the commutative property of the commutative encryption. After performing the commutative encryption sequentially according to their secret keys, a final agreement key can be shared by the participants. Furthermore, the superposition states can be realized using current technologies, and it is easier to realize the rotation operations than the unitary operations. Therefore, it may be easier to realize our protocol physically. The commutative encryption has very interesting properties, and it may be also used to construct quantum private comparison protocol [14,37] and quantum summation protocol, which need our further research.

The insufficiency of the presented protocol may be that it can only prevent one participant from determining the final key alone, i.e., it cannot resist collusion attacks. If more participants collaborate with each other, they can change the final key into their expected. Thus, it will be an unfair QKA protocol in this situation. In other words, there has to be a trade-off between efficiency and security if we want to improve the

efficiency of the multiparty QKA. Thus, we first considered the simplest case where no party trusted each other, in the proposed protocol. And, this is indeed reasonable in some real-life situation. We are currently involved in research into how to prevent two or three participants collusion attacks. Finally, we will give the general circle-type QKA protocol that can resist collusion attacks in our following study.

Since our protocol transmits the same photons more than once, it may suffer from the Trojan horse attacks. Such kind of circular quantum transmission has been discussed [32–35]. To prevent this type of attacks, participants can install a special quantum optical device such as the wavelength quantum filter and the photon number splitters (PNS) to detect an attack. According to Refs. [32–35], Eve's invisible photons can be filtered out by using the wavelength quantum filter, and the PNS can split each legitimate photon to discover the delay photons. If there is an irrational high rate of multiphoton signal, then the attack can be detected.

Acknowledgments The authors are grateful to the anonymous referees for their valuable comments and suggestions that help to improve the paper. This work is supported by the National Natural Science Foundation of China (No. 61402293, 61300204), Seed Funding from Scientific and Technical Innovation Council of Shenzhen Government (No. 827-000035), Natural Science Foundation of Guangdong (2015A030313630), Opening Project of Shanghai Key Laboratory of Integrated Administration Technologies for Information Security, the Science and Technology Innovation Projects of Shenzhen (Nos. JCYJ20150324141711665 and JCYJ20150324141711694), Natural Science Foundation of SZU (No. 201435), Shenzhen R&D Program (GJHZ20140418191518323) and Postdoctoral Science Foundation of China (No. 2015M572360).

References

1. Bennett, C.H.: Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. **68**, 3121 (1992)
2. Goldenberg, L., Vaidman, L.: Quantum cryptography based on orthogonal states. Phys. Rev. Lett. **75**, 1239 (1995)
3. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, pp. 175–179 (1984)
4. Ekert, A.K.: Quantum cryptography based on Bell's theorem. Phys. Rev. Lett. **67**, 661 (1991)
5. Shor, Pw, Preskill, J.: Simple proof of security of the BB84 quantum key distribution protocol. Phys. Rev. Lett. **85**, 441 (2000)
6. Diffie, W., Hellman, M.: New directions in cryptography. IEEE Trans. Inf. Theory **22**, 644–654 (1976)
7. Shor P.W.: Algorithms for quantum computation: discrete logrithms and factoring. In: Proceedings of 35th Annual Symposium on the Foundations of Computer Science, pp. 124–134 (1994)
8. Hillery, M., Buzek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A **59**, 1829 (1999)
9. Du, R.G., Sun, Z.W., Wang, B.H., Long, D.Y.: Quantum secret sharing of secure direct communication using one-time pad. Int. J. Theor. Phys. **51**, 2727–2736 (2012)
10. Sun, Z.W., Du, R.G., Long, D.Y.: Quantum secure direct communication with quantum identification. Int. J. Quantum Inf. **10**, 1250008 (2012)
11. Sun, Zw, Du, R.G., Long, D.Y.: Quantum secure direct communication with two-photon four-qubit cluster state. Int. J. Theor. Phys. **51**, 1946–1952 (2012)
12. Chen, X.B., Xu, G., Niu, X.X., Wen, Q.Y., Yang, Y.X.: An efficient protocol for the private comparison of equal information based on the triplet entangled state and single-particle measurement. Opt. Commun. **283**, 1561–1565 (2010)
13. Sun, Zw, Long, D.Y.: Quantum private comparison protocol based on cluster states. Int. J. Theor. Phys. **52**, 212–218 (2013)
14. Sun, Z.W., Yu, J.P., Wang, P., Xu, L.L., Wu, C.H.: Quantum private comparison with a malicious third party. Quantum Inf. Process. **14**(6), 2125–2133 (2015)

15. Sun, Zhiwei, Jianping, Yu., Wang, Ping, Lingling, Xu: Symmetrically private information retrieval based on blind quantum computing. Phys. Rev. A **91**, 052303 (2015)
16. Zhou, N., Zeng, G., Xiong, J.: Quantum key agreement protocol. Electron. Lett. **40**(18), 1149 (2004)
17. Tsai, C., Hwang, T.: On quantum key agreement protocol. R.O.C, Technical Report, C-S-I-E, NCKU, Taiwan (2009)
18. Chong, S.K., Tsai, C.W., Hwang, T.: Improvement on quantum key agreement protocol with maximally entangled states. Int. J. Theor. Phys. **50**(6), 1793–1802 (2011)
19. Chong, S.K., Hwang, T.: Quantum key agreement protocol based on BB84. Opt. Commun. **283**(6), 1192–1195 (2010)
20. Huang, W., Wen, Q.Y., Liu, B., Gao, F., Sun, Y.: Quantum key agreement with EPR pairs and single particle measurements. Quantum Inf. Process. **13**(3), 649–663 (2014)
21. Dongsu, Shen, Wenping, Ma., Lili, Wang: Two-party quantum key agreement with four-qubit cluster states. Quantum Inf. Process. **13**, 2313 (2014)
22. Sun, Zhiwei, Jianping, Yu., Wang, Ping: Efficient multiparty quantum key agreement by cluster states. Quantum Inf. Process. **15**(1), 373–384 (2016)
23. Shi, R.H., Zhong, H.: Multi-party quantum key agreement with bell states and bell measurements. Quantum Inf. Process **12**(2), 921–932 (2013)
24. Liu, B., Gao, F., Huang, W., Wen, Q.Y.: Multiparty quantum key agreement with single particles. Quantum Inf. Process. **12**(4), 1797–1805 (2013)
25. Sun, Z., Wang, B., Li, Q., Long, D.: Improvements on multiparty quantum key agreement with single particles. Quantum Inf. Process. **12**, 3411 (2013)
26. Yin, X.R., Ma, W.P., Liu, W.Y.: Three-party quantum key agreement with two-photon entanglement. Int. J. Theor. Phys. **52**, 3915–3921 (2013)
27. Chitra, S., Nasir, A., Anirban, P.: Protocols of quantum key agreement solely using bell states and bell measurement. Quantum Inf. Process. **13**, 2391–2405 (2014)
28. Kanamori, Yoshito, Yoo, Seong-Moo, Gregory, Don A., Sheldon, Frederick T.: Authentication protocol using quantum superposition states. Int. J. Netw. Secur. **9**(2), 101–108 (2009)
29. Hwang, Won-Young: Quantum key distribution with high loss: toward global secure communication. Phys. Rev. Lett. **91**, 057901 (2003)
30. Lo, Hoi-Kwong, Ma, Xiongfeng, Chen, Kai: Decoy state quantum key distribution. Phys. Rev. Lett. **94**, 230504 (2005)
31. Wang, Xiang-Bin: Beating the photon-number-splitting attack in practical quantum cryptography. Phys. Rev. Lett. **94**, 230503 (2005)
32. Deng, F.G., Li, X.H., Zhou, H.Y., Zhang, Z.J.: Improving the security of multiparty quantum secret sharing against Trojan horse attack. Phys. Rev. A **72**, 044302 (2005)
33. Li, X.H., Deng, F.G., Zhou, H.Y.: Improving the security of secure direct communication based on the secret transmitting order of particles. Phys. Rev. A **74**, 054302 (2006)
34. Cai, Q.Y.: Eavesdropping on the two-way quantum communication protocols with invisible photons. Phys. Lett. A **351**, 23–25 (2006)
35. Lin, J., Hwang, T.: New circular quantum secret sharing for remote agents. Quantum Inf. Process. **12**, 685 (2013)
36. Cabello, A.: Quantum key distribution in the Holevo limit. Phys. Rev. Lett. **85**, 5633–5638 (2000)
37. Liu, W.-J., Liu, C., Chen, H.-W., Liu, Z.-H., Yuan, M.-X., Lu, J.-S.: Improvement on "an efficient protocol for the quantum private comparison of equality with W state". Int. J. Quantum Inf. **12**(01), 1450001 (2014)