International Journal of Theoretical Physics (2019) 58:436–450
https://doi.org/10.1007/s10773-018-3944-7

Multiparty Quantum Key Agreement Protocol with Entanglement Swapping

Xing-Qiang Zhao[1] · Nan-Run Zhou[2] · Hua-Ying Chen[3] · Li-Hua Gong[2]

Received: 29 July 2018 / Accepted: 26 October 2018 / Published online: 20 November 2018

Abstract
Secure and fair multiparty quantum key agreement protocols demand all participants influence and negotiate the shared secret key with equal right and nobody can determine the shared secret key only by himself. To ensure the security and high efficiency, a novel multiparty quantum key agreement protocol based on entanglement swapping between Bell states and G-like states is proposed. This protocol makes full use of Bell states and G-like states as quantum resources and utilizes Bell measurement, Z-basis measurement and unitary operations to generate the shared secret key. It demonstrates that this proposed multiparty quantum key agreement protocol is secure and fair, and simpler with higher efficiency than some other protocols, especially when the number of participants in the protocol is big enough. Furthermore, the proposed protocol can be implemented with existing physical technologies.

Keywords Multiparty quantum key agreement protocol · Entanglement swapping · Bell state · G-like state · Quantum communication

1 Introduction

In the past few decades, quantum information technology has developed rapidly. With the development of quantum informatics, quantum cryptography has attracted more and more attention. Quantum cryptography exploits quantum informatics and other technologies to ensure unconditionally secure communications. Therefore, many kinds of quantum cryptographic protocols have been put forward, including quantum key distribution (QKD) [1–6], quantum oblivious transfer (QOT) [7, 8], quantum signature (QS) [9–12], quantum secret

✉ Nan-Run Zhou
nrzhou@ncu.edu.cn

[1] Department of Computer Science and Technology, Nanchang University, Nanchang 330031, China

[2] Department of Electronic Information Engineering, Nanchang University, Nanchang 330031, China

[3] Department of Physics, Nanchang University, Nanchang 330031, China

sharing (QSS) [13–15], quantum bit commitment (QBC) [16, 17], quantum secure direct communication (QSDC) [18–20], and so on.

Since the first quantum key distribution protocol was proposed by Bennett and Brassard in 1984 [1], quantum cryptography has made great progress. Recently, quantum key agreement (QKA) [21–39] has become a new focus. Quantum key agreement protocol permits some parties to negotiate a classical shared secret key via public quantum channels. Moreover, each participant has a fair influence on the final key and the key can only be generated jointly by all participants.

The first quantum key agreement protocol [21] was proposed by Zhou et al. in 2004 by replacing a classical channel with a quantum one during quantum teleportation [40]. Inspired by this protocol, Hsueh and Chen put forward a QKA protocol with maximally entangled states in the same year [22]. However, Chong et al. believed that it was susceptible to participant attack [23]. In 2013, Yin et al. presented a tri-party QKA protocol with two-photon entanglement [27]. And in the same year, the first multiparty quantum key agreement protocol was proposed based on entanglement swapping without the help of a third party [24]. Liu et al. pointed out that the security of Shi's protocol does not meet the actual requirement and then put forward a new multiparty quantum key agreement protocol with single particles [25]. Then Sun et al. improved Liu's protocol based on unitary operations in 2013 [26]. Hereafter, a number of multiparty and two-party QKA protocols were proposed [29–39]. In 2017, Wang et al. put forward a circle-type multiparty QKA protocol to solve the problems of multiparty security communication and resist most common attacks [37]. In 2018, Cai et al. proposed a multi-party quantum key agreement protocol with five-qubit Brown states and single-qubit measurements, which weakens the hardware requirements of the participant but involving a large amount of calculations [38]. To counteract participants' collusion attacks, Gong et al. proposed a novel multiparty quantum key agreement protocol with G-like states and Bell states in 2018 [39].

A new tri-party quantum key agreement protocol will be put forward based on entanglement swapping with Bell and G-like states. Furthermore, this proposed QKA protocol will be extended to a multiparty QKA protocol with a circle-type method. The proposed secure and fair protocol needs fewer calculations and is simpler than that in [38]. And the efficiency of the proposed protocol is higher than some other protocols when enough participants involve in the protocol. What's more, the proposed protocol is feasible with real physical devices.

The structure of this paper is described as follows. In Section 2, the G-like and Bell states will be introduced. In Section 3, the tri-party QKA protocol with the seven-particle entangled state will be put forward. In Section 4, the multiparty QKA protocol extended by the tri-party QKA protocol will be proposed. In Section 5, the security and efficiency of this protocol will be analyzed. And in Section 6, a brief conclusion is provided.

2 Quantum States and Quantum Correlation Property

2.1 Bell States

Bell states are two-qubit entangled states. An EPR pair is one of the four Bell states and the four states are expressed as follows:

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle\Big), \tag{1}$$

$$|\phi^-\rangle = \frac{1}{\sqrt{2}}\Big(|00\rangle - |11\rangle\Big), \tag{2}$$

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}\Big(|01\rangle + |10\rangle\Big), \tag{3}$$

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}\Big(|01\rangle - |10\rangle\Big). \tag{4}$$

The entanglement swapping utilizing Bell measurements on Bell states was achieved by Shi et al. [24].

Suppose that $|\phi^+\rangle_{12}$ represents the entangled state $|\phi^+\rangle$ of particles 1 and 2 and $|\psi^+\rangle_{34}$ indicates that particles 3 and 4 are in the entangled state $|\psi^+\rangle$. If someone measures two particles 1 and 4 or 2 and 3 with the Bell basis, respectively, their measurement outcomes could be expressed as follows:

$$\begin{aligned} |\phi^+\rangle_{12}\otimes|\psi^+\rangle_{34} &= \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle\Big)_{12}\otimes\frac{1}{\sqrt{2}}\Big(|01\rangle + |10\rangle\Big)_{34} \\ &= \frac{1}{2}\Big(|0001\rangle + |0010\rangle + |1101\rangle + |1110\rangle\Big)_{1234} \\ &= \frac{1}{2}\Big(|0100\rangle + |0001\rangle + |1110\rangle + |1011\rangle\Big)_{1423} \\ = \frac{1}{2}\Big(|\phi^+\rangle_{14}|\psi^+\rangle_{23} &+ |\phi^-\rangle_{14}|\psi^-\rangle_{23} + |\psi^+\rangle_{14}|\phi^+\rangle_{23} + |\psi^-\rangle_{14}|\phi^-\rangle_{23}\Big) \end{aligned} \tag{5}$$

If one encodes the states with the encoding rule such as: $|\phi^+\rangle \to 00$, $|\phi^-\rangle \to 01$, $|\psi^+\rangle \to 10$ and $|\psi^-\rangle \to 11$, then the correlation between the possible measurement results and the original Bell states can refer to [39]. If controlled-not (CONT) gates are utilized on their measurement outcomes, then the results will be

$$\begin{aligned} |\phi^+\rangle_{12}\otimes|\psi^+\rangle_{34} &= \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle\Big)_{12}\otimes\frac{1}{\sqrt{2}}\Big(|01\rangle + |10\rangle\Big)_{34} \\ &= \frac{1}{2}\Big(|0001\rangle + |0010\rangle + |1101\rangle + |1110\rangle\Big)_{1234} \\ = \frac{1}{2}|01\rangle_{14}|00\rangle_{23} &+ \frac{1}{2}|00\rangle_{14}|01\rangle_{23} + \frac{1}{2}|11\rangle_{14}|10\rangle_{23} + \frac{1}{2}|10\rangle_{14}|11\rangle_{23} \end{aligned} \tag{6}$$

This shows that the result of the tensor product form of two Bell states can be separated into three systems. For example, these can be separated into two single particles and one pair of entangled particles.

2.2 GHZ-Like State

Quantum state $|G\rangle = \frac{1}{2}(|001\rangle + |010\rangle + |100\rangle + |111\rangle)$ is called the GHZ-like state. It consists of a single particle and one EPR pair, that's to say, the state $|G\rangle$ is obtained with the two states $|\varphi\rangle_1 = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_1$ and $|\phi^+\rangle_{23} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{23}$. The specific process is

$$|G_0\rangle_{123} = |\varphi\rangle_1|\phi^+\rangle_{23} = \frac{1}{\sqrt{2}}\Big(|0\rangle + |1\rangle\Big)_1 \otimes \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle\Big)_{23}, \\ = \frac{1}{2}\Big(|000\rangle + |011\rangle + |100\rangle + |111\rangle\Big)_{123} \tag{7}$$

where the subscript denotes the particle's sequence number of the state $|G_0\rangle$. By performing controlled-not (CNOT) gate on $|G_0\rangle_{123}$, the result will be

$$|G_0\rangle_{123} = \frac{1}{2}\Big(|000\rangle + |011\rangle + |100\rangle + |111\rangle\Big)_{123} \\ = \frac{1}{\sqrt{2}}\Big(|0\rangle_1|\phi^+\rangle_{23} + |1\rangle_1|\phi^+\rangle_{23}\Big) \tag{8}$$

Similar to the Bell state, the GHZ-like state is divided into two systems, i.e., a single particle and an EPR pair.

3 Tri-Party QKA Protocol

Assume that U_{00}, U_{01}, U_{10}, U_{11} indicate the four local unitary operations.

$$U_{00} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, U_{01} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, U_{10} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, U_{11} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{9}$$

$|0\rangle$ and $|1\rangle$ form Z-basis, while $|+\rangle$ and $|-\rangle$ form X-basis, where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. All the transformations on the Bell states based on the four unitary operations are in Table 1.

According to entanglement swapping and the specific correlation among the measurement results, a novel tri-party QKA protocol with Bell states and G-like states is proposed. The specific states used in this protocol are as follows:

$$|\phi^+\rangle_{12}|G\rangle_{345}|\phi^+\rangle_{67} = \frac{1}{4}\Big(|00\rangle + |11\rangle\Big)_{12} \otimes \Big(|001\rangle + |010\rangle + |101\rangle + |110\rangle\Big)_{345} \otimes \Big(|00\rangle + |11\rangle\Big)_{67} \tag{10}$$

By taking advantage of controlled-not (CNOT) gate on the particles 1, 3 and 6 of Eq. (10) and representing the decimal number with bold, Eq. (10) can be rewritten as:

$$\begin{aligned} |\phi^+\rangle_{12}|G\rangle_{345}|\phi^+\rangle_{67} &= \frac{1}{4}\Big(|\mathbf{4}\rangle + |\mathbf{7}\rangle + |\mathbf{8}\rangle + |\mathbf{11}\rangle + |\mathbf{20}\rangle + |\mathbf{23}\rangle + |\mathbf{24}\rangle + |\mathbf{27}\rangle + |\mathbf{100}\rangle \\ &+ |\mathbf{103}\rangle + |\mathbf{104}\rangle + |\mathbf{107}\rangle + |\mathbf{116}\rangle + |\mathbf{119}\rangle + |\mathbf{120}\rangle + |\mathbf{123}\rangle\Big)_{1234567} \\ &= \frac{1}{4}|\mathbf{0}\rangle_{136}\Big(|\mathbf{2}\rangle + |\mathbf{4}\rangle\Big)_{2457} + \frac{1}{4}|\mathbf{1}\rangle_{136}\Big(|\mathbf{3}\rangle + |\mathbf{5}\rangle\Big)_{2457} \\ &+ \frac{1}{4}|\mathbf{2}\rangle_{136}\Big(|\mathbf{2}\rangle + |\mathbf{4}\rangle\Big)_{2457} + \frac{1}{4}|\mathbf{3}\rangle_{136}\Big(|\mathbf{3}\rangle + |\mathbf{5}\rangle\Big)_{2457} \\ &+ \frac{1}{4}|\mathbf{4}\rangle_{136}\Big(|\mathbf{10}\rangle + |\mathbf{12}\rangle\Big)_{2457} + \frac{1}{4}|\mathbf{5}\rangle_{136}\Big(|\mathbf{11}\rangle + |\mathbf{13}\rangle\Big)_{2457} \\ &+ \frac{1}{4}|\mathbf{6}\rangle_{136}\Big(|\mathbf{10}\rangle + |\mathbf{12}\rangle\Big)_{2457} + \frac{1}{4}|\mathbf{7}\rangle_{136}\Big(|\mathbf{11}\rangle + |\mathbf{13}\rangle\Big)_{2457} \end{aligned} \tag{11}$$

Table 1 Transformations on Bell states

	$I \otimes U_{00}$	$I \otimes U_{01}$	$I \otimes U_{10}$	$I \otimes U_{11}$
$\|\phi^+\rangle$	$\|\phi^+\rangle$	$\|\psi^+\rangle$	$\|\psi^-\rangle$	$\|\phi^-\rangle$
$\|\phi^-\rangle$	$\|\phi^-\rangle$	$\|\psi^-\rangle$	$\|\psi^+\rangle$	$\|\phi^+\rangle$
$\|\psi^+\rangle$	$\|\psi^+\rangle$	$\|\phi^+\rangle$	$\|\phi^-\rangle$	$\|\psi^-\rangle$
$\|\psi^-\rangle$	$\|\psi^-\rangle$	$\|\phi^-\rangle$	$\|\phi^+\rangle$	$\|\psi^+\rangle$

Equation (11) can also be expanded with the Bell bases as follows:

$$
\begin{aligned}
|\phi^+\rangle_{12}|G\rangle_{345}|\phi^+\rangle_{67} = {} & \frac{1}{8}|\mathbf{0}\rangle_{136}\Big(|\phi^+\rangle_{24}|\psi^+\rangle_{57}-|\phi^+\rangle_{24}|\psi^-\rangle_{57}+|\phi^-\rangle_{24}|\psi^+\rangle_{57}-|\phi^-\rangle_{24}|\psi^-\rangle_{57} \\
& +|\psi^+\rangle_{24}|\phi^+\rangle_{57}+|\psi^+\rangle_{24}|\phi^-\rangle_{57}+|\psi^-\rangle_{24}|\phi^+\rangle_{57}+|\psi^-\rangle_{24}|\phi^-\rangle_{57}\Big) \\
& +\frac{1}{8}|\mathbf{1}\rangle_{136}\Big(|\phi^+\rangle_{24}|\phi^+\rangle_{57}-|\phi^+\rangle_{24}|\phi^-\rangle_{57}+|\phi^-\rangle_{24}|\phi^+\rangle_{57}-|\phi^-\rangle_{24}|\phi^-\rangle_{57} \\
& +|\psi^+\rangle_{24}|\psi^+\rangle_{57}+|\psi^+\rangle_{24}|\psi^-\rangle_{57}+|\psi^-\rangle_{24}|\psi^+\rangle_{57}+|\psi^-\rangle_{24}|\psi^-\rangle_{57}\Big) \\
& +\frac{1}{8}|\mathbf{2}\rangle_{136}\Big(|\phi^+\rangle_{24}|\psi^+\rangle_{57}-|\phi^+\rangle_{24}|\psi^-\rangle_{57}+|\phi^-\rangle_{24}|\psi^+\rangle_{57}-|\phi^-\rangle_{24}|\psi^-\rangle_{57} \\
& +|\psi^+\rangle_{24}|\phi^+\rangle_{57}+|\psi^+\rangle_{24}|\phi^-\rangle_{57}+|\psi^-\rangle_{24}|\phi^+\rangle_{57}+|\psi^-\rangle_{24}|\phi^-\rangle_{57}\Big) \\
& +\frac{1}{8}|\mathbf{3}\rangle_{136}\Big(|\phi^+\rangle_{24}|\phi^+\rangle_{57}-|\phi^+\rangle_{24}|\phi^-\rangle_{57}+|\phi^-\rangle_{24}|\phi^+\rangle_{57}-|\phi^-\rangle_{24}|\phi^-\rangle_{57} \\
& +|\psi^+\rangle_{24}|\psi^+\rangle_{57}+|\psi^+\rangle_{24}|\psi^-\rangle_{57}+|\psi^-\rangle_{24}|\psi^+\rangle_{57}+|\psi^-\rangle_{24}|\psi^-\rangle_{57}\Big) \\
& +\frac{1}{8}|\mathbf{4}\rangle_{136}\Big(|\phi^+\rangle_{24}|\phi^+\rangle_{57}-|\phi^-\rangle_{24}|\phi^+\rangle_{57}+|\phi^+\rangle_{24}|\phi^-\rangle_{57}-|\phi^-\rangle_{24}|\phi^-\rangle_{57} \\
& +|\psi^+\rangle_{24}|\psi^+\rangle_{57}-|\psi^+\rangle_{24}|\psi^-\rangle_{57}+|\psi^-\rangle_{24}|\psi^-\rangle_{57}-|\psi^-\rangle_{24}|\psi^+\rangle_{57}\Big) \\
& +\frac{1}{8}|\mathbf{5}\rangle_{136}\Big(|\psi^+\rangle_{24}|\phi^+\rangle_{57}-|\psi^-\rangle_{24}|\phi^+\rangle_{57}+|\psi^+\rangle_{24}|\phi^-\rangle_{57}-|\psi^-\rangle_{24}|\phi^-\rangle_{57} \\
& +|\phi^+\rangle_{24}|\psi^+\rangle_{57}-|\phi^-\rangle_{24}|\psi^+\rangle_{57}+|\phi^+\rangle_{24}|\psi^-\rangle_{57}-|\phi^-\rangle_{24}|\psi^-\rangle_{57}\Big) \\
& +\frac{1}{8}|\mathbf{6}\rangle_{136}\Big(|\phi^+\rangle_{24}|\phi^+\rangle_{57}-|\phi^-\rangle_{24}|\phi^+\rangle_{57}+|\phi^+\rangle_{24}|\phi^-\rangle_{57}-|\phi^-\rangle_{24}|\phi^-\rangle_{57} \\
& +|\psi^+\rangle_{24}|\psi^+\rangle_{57}-|\psi^+\rangle_{24}|\psi^-\rangle_{57}+|\psi^-\rangle_{24}|\psi^-\rangle_{57}-|\psi^-\rangle_{24}|\psi^+\rangle_{57}\Big) \\
& +\frac{1}{8}|\mathbf{7}\rangle_{136}\Big(|\psi^+\rangle_{24}|\phi^+\rangle_{57}-|\psi^-\rangle_{24}|\phi^+\rangle_{57}+|\psi^+\rangle_{24}|\phi^-\rangle_{57}-|\psi^-\rangle_{24}|\phi^-\rangle_{57} \\
& +|\phi^+\rangle_{24}|\psi^+\rangle_{57}-|\phi^-\rangle_{24}|\psi^+\rangle_{57}+|\phi^+\rangle_{24}|\psi^-\rangle_{57}-|\phi^-\rangle_{24}|\psi^-\rangle_{57}\Big)
\end{aligned}
\tag{12}
$$

According to Eq. (12), the state may collapse into any one of the 64 states with equal probability when the state is measured.

Assume that three participants, i.e., Alice, Bob and Charlie have to generate their own secret keys, i.e., K_A, K_B and K_C, respectively, and then they need to establish a shared secret key K.

$$K_P = \{k_{P_i} | k_{P_i} \in \{0,1\}, i = 1,2,\ldots,n.\}, P \in (A,B,C). \tag{13}$$

$$K = K_A \oplus K_B \oplus K_C. \tag{14}$$

Then the tri-party quantum key agreement protocol as shown in Fig. 1 can be described as follows.

Step 1 State preparation. State preparation is shown in Fig. 1a. (a) Alice prepares n entangled states $|\phi^{+}\rangle_{12}$ and divides these entangled states into two ordered states a_1 and a_2. (b) Bob generates n GHZ-like states in $|G\rangle_{345}$ and divides them into three ordered sequences b_1, b_2 and b_3. (c) Charlie produces n entangled Bell states as same as Alice, and also divides them into two ordered sequences c_1 and c_2.

Step 2 Insertion of decoy states. Three participants randomly select enough decoy photons in the four states $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$. (a) Alice inserts some decoy states into a_2 at random and obtains $a_2^{'}$. (b) Bob randomly plugs some decoy states into b_2 and b_3 to produce $b_2^{'}$ and $b_3^{'}$, respectively. (c) Charlie also inserts some decoy states into c_2 at random to generate $c_2^{'}$ (Please refer to Fig. 1b.). (d) Subsequently, Alice (Bob) sends the mixed sequence $a_2^{'}$ ($b_2^{'}$) to Bob (Alice), and Bob (Charlie) transmits the new sequence $b_3^{'}$ ($c_2^{'}$) to Charlie (Bob) (Please refer to Fig. 1c.).

Step 3 Channel security check. (a) After three participants confirm that all the sequences have received, they announce the positions of the decoy states and the corresponding preparation bases. (b) Then all the receivers measure the decoy states with the correct bases and tell the measurement outcomes to the corresponding sender. (c) All the senders and the corresponding receivers check the security of quantum channels by comparing the measurement results. Once the error rate exceeds the preset value, this round of communication should be aborted. Otherwise, they continue.

Step 4 Bell measurement. Three participants pick out the decoy states in their state sequences and then Alice obtains the state sequence b_2, Bob gains the state sequences a_2

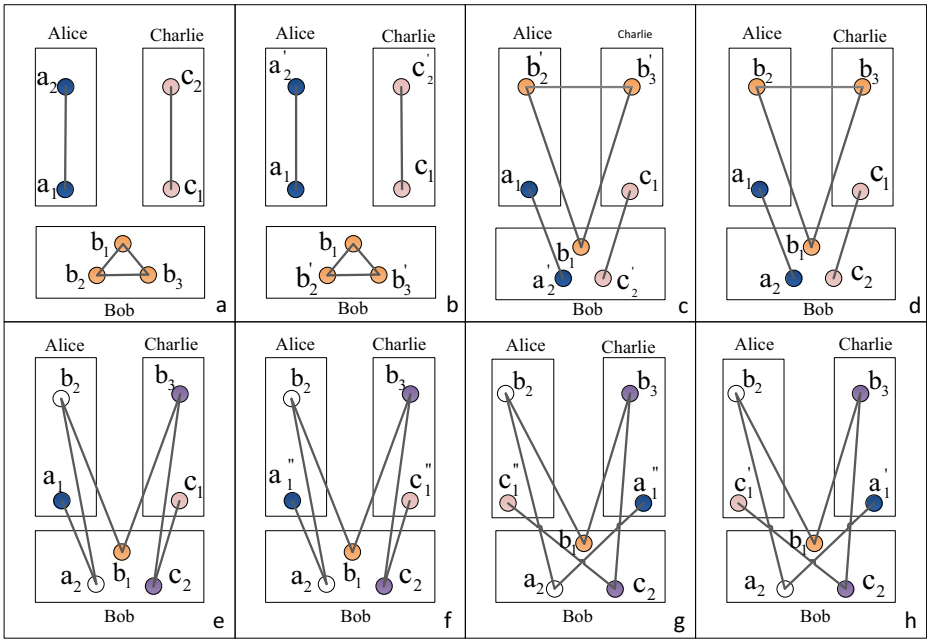

Fig. 1 Entanglement swapping of three parties

and c_2, Charlie obtains the state sequence b_3 (Please refer to Fig. 1d.). Then they perform the Bell measurement on their remaining sequences, respectively (Please refer to Fig. 1e.).

Step 5 Bell measurement and insertion of decoy states. (a) Alice and Charlie perform a series of unitary operations chosen from $\{U_{00}, U_{01}, U_{10}, U_{11}\}$ on each state in state sequences a_1 and c_1 and form new sequences $a_1^{'}$ and $c_1^{'}$. (b) Subsequently, Alice and Charlie insert enough decoy states randomly selected from the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ into $a_1^{'}$ and $c_1^{'}$ to generate two new sequences $a_1^{''}$ and $c_1^{''}$ (Please refer to Fig. 1f.). (c) Alice (Charlie) sends sequence $a_1^{''}$ ($c_1^{''}$) to Charlie (Alice) (Please refer to Fig. 1g.).

Step 6 Channel security check. (a) After Alice (Charlie) acknowledges sequence $c_1^{''}$ ($a_1^{''}$), Charlie (Alice) announces the positions of the decoy states and the corresponding preparation bases. (b) Subsequently, Alice (Charlie) measures the decoy states with the correct bases and tells the measurement results to Charlie (Alice). (c) Then two parties compare the measurement results. If the error rate exceeds the threshold, this round of communication must be abandoned. Otherwise, they continue.

Step 7 Measurement and generation of shared key. (a) After removing the decoy states, Alice obtains sequence $c_1^{'}$ and Charlie gains sequence $a_1^{'}$. Then Alice and Charlie perform the Bell measurement on their sequences. (b) Bob performs the Z-basis measurement on every state in sequence b_1 and tells Alice and Charlie the measurement outcomes. (c) Apparently, Alice (Charlie) holds sequences b_2 and $c_1^{'}$ ($a_1^{'}$ and b_3) and also knows the measurement results of b_1 while Bob possesses sequences b_1, a_2 and c_2 (Please refer to Fig. 1h.). (d) According to the measurement outcomes, each of the three participants can obtain the other two counterparts' secret keys. Therefore, the three participants can compute the shared key as: $K = K_A \oplus K_B \oplus K_C$.

4 Multiparty QKA Protocol

For the multiparty case, circle-type multiparty quantum key agreement protocols are popular. To improve the efficiency significantly, the three participants in the proposed tri-party quantum key agreement protocol are regarded as a group to construct a new circle-type multiparty quantum key agreement protocol. The process of this multiparty QKA protocol is in the following.

Step 1 Subkey generation. Assume that there are $3n$ participants, and all the participants are classified into three groups, i.e., $A = \{a_i | i = 1, 2, \ldots, n\}$, $B = \{b_i | i = 1, 2, \ldots, n\}$ and $C = \{c_i | i = 1, 2, \ldots, n\}$. (a) All the participants in groups A and C prepare Bell states, while all the participants in group B prepare the GHZ-like states. (b) All participants are regrouped into n groups and there are three participants (a_i, b_i, c_i) in each group. (c) Each group performs the tri-party quantum key agreement protocol described in Section 3 once to generate secret subkey, denoted by $\{K_i | i = 1, 2, \ldots, n\}$.

Step 2 Construction of circle-type MQKA protocol. All the participants from group A construct a circle-type multiparty QKA protocol at random, then the participants are randomly re-marked as R_i and $R_i \in A$. Every participant does not know who the two adjacent participants are. The circle-type multiparty QKA protocol is described in Fig. 2.

Step 3 State preparation and insertion of decoy states. (a) Each participant in R_i prepares n Bell states and divides them into two ordered sequences s_i and l_i. Sequence

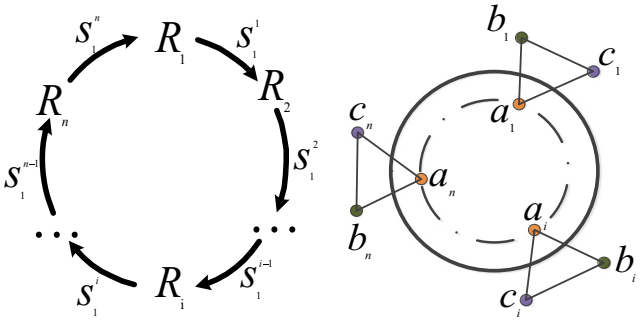

Fig. 2 The circle-type multiparty QKA protocol

s_i includes all the first particles of the EPR pairs, while sequence l_i includes all the second particles of the EPR pairs. (b) R_i randomly inserts enough decoy states in state $|0\rangle$, $|1\rangle$, $|+\rangle$ or $|-\rangle$ into s_i to obtain s_i^1. (c) R_i sends the mixed state sequence s_i^1 to R_{i+1}.

Step 4 Channel security check. (a) After R_{i+1} receives the state sequence s_i^1, R_i announces the positions of the decoy states and the corresponding measurement bases to R_{i+1}. (b) Subsequently, R_{i+1} measures the decoy states with correct bases and tells R_i the measurement outcomes. (c) R_i and R_{i+1} check whether the measurement results are consistent with the initial states of the decoy states or not and calculate the error rate in the measurement outcomes. If the error rate exceeds the threshold, this protocol should be aborted. Otherwise, they continue.

Step 5 Unitary operation and insertion of decoy states. (a) R_{i+1} picks out the decoy states to obtain the state sequence s_i and obtains the secret subkey K_i. (b) Subsequently, R_{i+1} performs a series of unitary operations chosen from $\{U_{00}, U_{01}, U_{10}, U_{11}\}$ on each state in s_i^1. (c) Then R_{i+1} randomly selects and inserts enough decoy states in state $|0\rangle$, $|1\rangle$, $|+\rangle$ or $|-\rangle$ into s_i^1 to obtain s_i^2. (d) R_{i+1} sends the mixed sequence s_i^2 to R_{i+2}.

Step 6 Sequential operation. The participants R_{i+2}, R_{i+3}, …, R_{i-1} execute Step 4 and Step 5 in sequence in the same way as R_i. For security and simplicity, all participants should carry out the eavesdropping check first. Once the quantum channel is insecure, they give up this protocol. Otherwise, they perform specific unitary operations on s_i^j and insert enough decoy photons into $s_i^j (j = 0, 1, \ldots, n)$. After that, they send the mixed sequence to next participant.

Step 7 Generation of secret key. When all the participants execute Steps 2–6, a round of circle communication is finished, and then sequence s_i^n will return to participant R_i. R_i can generate the key $K = K_1 \oplus K_2 \oplus \ldots \oplus K_n$ according to the quantum measurement results and the quantum entanglement property.

Step 8 Intra-group transmission. Every group carries out transfer operation. Then the other two participants can also obtain the shared secret keys.

5 Analysis and Discussion

What a quantum key agreement protocol needs to guarantee firstly is its security. So in this section, the ability of the proposed protocol against all kinds of attacks will be discussed.

5.1 Participant Attack

In order to ensure the security of the proposed tri-party QKA protocol, the delayed measurement technique [41] is adopted. In the multiparty QKA protocol, collusive attack with participants is the biggest security risk, since the dishonest participants may collaborate to predetermine the key without being detected [42]. In this protocol, however, it is impossible for R_i to find the corresponding dishonest participant because no participant knows the positions of other participant groups. Generally, a dishonest participant R_i may adopt three different methods to cheat other legal participants: (1) extracting all the subkeys' information in the sequences and obtaining the final shared secret key before other participants. (2) announcing the wrong decoy positions to others to destroy this protocol. (3) finding the corresponding dishonest participants to obtain the final shared secret key.

For the first method, R_i cannot obtain the final shared secret key in advance. In fact, R_i must gain all the participants' subkeys if he wants to obtain the final shared secret key. However, during the process of the proposed multiparty QKA protocol, each participant sends the state sequence with decoy particles, and all the participants sends their state sequence at the same time, so R_i cannot obtain the final shared secret key before other participants.

For the second method, if R_i announces the wrong positions of the decoy particles to other participants, the protocol must be abandoned. The state sequences that all the participants send to others are mixed state sequences. After each transmission of these state sequences, the receiver and the corresponding sender would check the channel by comparing the positions of decoy particles. If R_i announces the wrong positions of decoy particles, the corresponding sender will definitely find that R_i is dishonest and the protocol must be abandoned by other participants.

For the third method, R_i cannot find corresponding dishonest participants. From Step 2 in Section 4, it is known that every participant does not know who the two adjacent participants are, so even if R_i knows that there are other dishonest participants, he cannot find them since he does not know their positions.

5.2 Outsider Attack

5.2.1 Entangle-Measure Attack

If Eve makes use of entangle-measure attack, she intercepts the sequence transmitted in the quantum channel and entangles it with a pre-prepared intermediate state sequence, and then Eve resends the intercepted sequence to the corresponding participants. When the protocol is finished, Eve measures the intermediate state sequence, and then she will attempt to extract some useful information and obtain the final shared secret key. Assume that Eve intercepts the sequence sent from Alice to Bob, and she intercepts other sequences in the same way. Without loss of generality, Eve's unitary operation U_{e} can be described as follows:

$$U_{\mathrm{e}}|0\rangle|E\rangle = a_e|0\rangle|e_{00}\rangle + b_e|1\rangle|e_{01}\rangle, \tag{15}$$

$$U_{\mathrm{e}}|1\rangle|E\rangle = \mathrm{c}_e|0\rangle|e_{10}\rangle + d_e|1\rangle|e_{11}\rangle, \tag{16}$$

where $|e_{00}\rangle$, $|e_{01}\rangle$, $|e_{10}\rangle$ and $|e_{11}\rangle$ are pure states and $|a_e|^2+|b_e|^2=1$, $|c_e|^2+|d_e|^2=1$. In the proposed protocol, all the decoy states are chosen from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, therefore the states $|+\rangle$ and $|-\rangle$ will become the following entangled states after Eve's entanglement operations.

$$\begin{aligned} U_e|+\rangle|E\rangle &= \frac{1}{\sqrt{2}}\left(a_e|0\rangle|e_{00}\rangle + b_e|1\rangle|e_{01}\rangle + c_e|0\rangle|e_{10}\rangle + d_e|1\rangle|e_{11}\rangle\right) \\ &= \frac{1}{2}\left\{|+\rangle\left(a_e|e_{00}\rangle + b_e|e_{01}\rangle + c_e|e_{10}\rangle + d_e|e_{11}\rangle\right)\right\} \\ &\quad + \frac{1}{2}\left\{|-\rangle\left(a_e|e_{00}\rangle - b_e|e_{01}\rangle + c_e|e_{10}\rangle - d_e|e_{11}\rangle\right)\right\} \end{aligned}, \tag{17}$$

$$\begin{aligned} U_e|-\rangle|E\rangle &= \frac{1}{\sqrt{2}}\left(a_e|0\rangle|e_{00}\rangle + b_e|1\rangle|e_{01}\rangle - c_e|0\rangle|e_{10}\rangle - d_e|1\rangle|e_{11}\rangle\right) \\ &= \frac{1}{2}\left\{|+\rangle\left(a_e|e_{00}\rangle + b_e|e_{01}\rangle - c_e|e_{10}\rangle - d_e|e_{11}\rangle\right)\right\} \\ &\quad + \frac{1}{2}\left\{|-\rangle\left(a_e|e_{00}\rangle - b_e|e_{01}\rangle - c_e|e_{10}\rangle + d_e|e_{11}\rangle\right)\right\} \end{aligned}. \tag{18}$$

If Eve guarantees no errors introduced in the eavesdropping check process, the general operation U_e must satisfy the conditions such as: $a_e=d_e=1$, $b_e=c_e=0$ and $|e_{00}\rangle = |e_{11}\rangle$. So Eqs. (15) and (16) will become

$$U_e|0\rangle|E\rangle = |0\rangle|e_{00}\rangle, \tag{19}$$

$$U_e|1\rangle|E\rangle = |1\rangle|e_{11}\rangle. \tag{20}$$

From Eqs. (17)–(20), it is shown that iff the message qubits and decoy particles are both in the state $|0\rangle$ or $|1\rangle$, Eve may not be found when she attacks the proposed protocol. However, in the protocol, all the decoy particles are in the state $|0\rangle$, $|1\rangle$ $|+\rangle$ or $|-\rangle$ randomly. So it is easy for the participants to detect eavesdropper Eve and it is necessary for Eve to fail to obtain the final shared secret key by the entangle-measure attack strategy.

From Eqs. (15)–(20), it is clear that the error rate introduced by eavesdropper Eve will be: $p_{e,1}=1-|a_e|^2$ or $p_{e,2}=1-|d_e|^2$. Then the mutual information between Alice and Bob will be

$$I_{e,1}(A,B) = 1 + |a_e|^2\log_2|a_e|^2 + \left(1-|a_e|^2\right)\log_2\left(1-|a_e|^2\right), \tag{21}$$

or

$$I_{e,1}(A,B) = 1 + |d_e|^2\log_2|d_e|^2 + \left(1-|d_e|^2\right)\log_2\left(1-|d_e|^2\right). \tag{22}$$

If Eve utilizes the intermediate state sequence, Bob will gain the wrong measurement outcomes with the probability $p_{e,3}=|b_e|^2+|c_e|^2$, and the mutual information between Bob and Eve will be

$$\begin{aligned} I_E(A,B) &= 1 + \left(|a_e|^2+|d_e|^2\right)\log_2\left(|a_e|^2+|d_e|^2\right) \\ &\quad + \left(|b_e|^2+|c_e|^2\right)\log_2\left(|b_e|^2+|c_e|^2\right). \end{aligned} \tag{23}$$

Recalling Eqs. (21)–(23), one can obtain

$$I_E(A,B) < I_{e,1}(A,B). \tag{24}$$

From Eq. (24), it is apparent that the mutual information with eavesdropping will be less than that without eavesdropping. So eavesdropper can be found easily by the participants.

Therefore, if Eve wants to gain the final shared secret key by making use of entangle-measure attack, she will be found by the participants easily, so she must fail and the protocol can effectively resist the entangle-measure attack.

5.2.2 Trojan Horse Attack

The multiparty QKA protocol may be insecure under the Trojan horse attack, since a certain number of particles are transferred more than once. Fortunately, a method to resist the Trojan horse attack was presented by Sun et al. [29] with circular quantum transmission [43, 44]. In the method, every participant should install a wavelength quantum filter to filter the invisible photons and the photon number splitters to discover the delay photons. If there is an irrational high rate of multi-photon signal, the eavesdropper can be detected. Therefore, it is impossible for the eavesdropper to obtain the final secret key by the Trojan horse attack, and the protocol can effectively resist the Trojan horse attack.

5.2.3 Intercept-Resend Attack

In the tri-party QKA protocol, Alice, Bob and Charlie need to send sequences to the other two participants. For instance, we just analyze the case that Alice sends state sequence $a_2^{'}$ to Bob and other state sequence transmissions are similar. When Alice sends the state sequence $a_2^{'}$ to Bob, assume that Eve can intercept state sequence $a_2^{'}$. All the states in sequence $a_2^{'}$ are as follows:

$$\rho_{a_2^{'}} = \mathrm{tr}_{a_1}|\varphi\rangle\langle\varphi| = \frac{1}{2}\Big(|0\rangle\langle 0| + |1\rangle\langle 1|\Big). \tag{25}$$

Obviously, Eve can't gain any information from the intercepted state sequence, for the state sequence $a_2^{'}$ is in the mixed state with decoy particles. For instance, Eve prepares an auxiliary state sequence and it is in the state $|\varphi\rangle_e = \alpha \mid 0\rangle + \beta \mid 1\rangle$ ($|\alpha|^2 + |\beta|^2 = 1$). After intercepting $a_2^{'}$, Eve sends the auxiliary state sequence to Bob. But when Bob receives the state sequence, he will measure it by corresponding measurement bases from Alice. Assume that Alice informs Bob the positions of the decoy particles and Bob measures the decoy particles with computational bases $\{|0\rangle, |1\rangle\}$. After measuring the decoy particles, Bob can gain the measurement outcomes 0 or 1 with probability $|\alpha|^2$ or $|\beta|^2$, which means the error rate with Eve is $|\alpha|^2$ or $|\beta|^2$. Afterwards, Bob's information can be expressed as [6]:

$$H_e(B) = -|\alpha|^2\log_2|\alpha|^2 - |\beta|^2\log_2|\beta|^2 \leq 1 \text{ bit}, \tag{26}$$

where H denotes the Shannon entropy. According to the definition, the Shannon entropy can be expressed by:

$$H(X) = -\sum_x p_x \log_2 p_x, \tag{27}$$

where X is a variable number and p_x is the presence probability of X [45]. From Eq. (26), it can be obtained that $H_e(B) = 1$ only if $|\alpha|^2 = |\beta|^2 = \frac{1}{2}$. If eavesdropper Eve exists, the mutual information between Alice and Bob is

$$I_e(A,B) = H_e(B) - H_e(B|A) < H_e(B) \leq 1 \text{ bit}, \tag{28}$$

where $H_e(B|A)$ denotes conditional entropy, and it is the expected entropy of Bob given the value of Alice and $H_e(B|A) > 0$.

According to the Holevo limit [45], if Eve does not exist, the mutual information is

$$I(A,B) \leq S(\rho) - \sum_x p_x S(\rho_x), \tag{29}$$

where $S(\rho) = -\mathrm{tr}(\rho \log_2 \rho)$ is the von Neumann entropy of state $\rho = \sum_x p_x \rho_x$. In the tri-party QKA protocol, $|\phi^+\rangle_{12} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{12}$ is the maximal entangled state in sequences a_1 and a_2 (a_2'). Each particle in the state sequences a_1 and a_2' is

$$\rho_{a_2'} = \rho_{a_1} = \frac{1}{2}\left(|0\rangle\langle 0| + |1\rangle\langle 1|\right) = \frac{1}{2}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \frac{1}{2} I. \tag{30}$$

So if there is no eavesdropper, the mutual information between Alice and Bob is

$$I(A,B) = S(\rho) = -\sum_x \lambda_x \log_2 \lambda_x = 1 \text{ bit}, \tag{31}$$

where λ_x denotes the eigenvalue of state ρ. Combining Eq. (28) with Eq. (31), one obtains

$$I_e(A,B) < I(A,B). \tag{32}$$

It is clear that the mutual information between Alice and Bob with eavesdropping will be less than that without eavesdropping. Therefore, if Eve wants to gain the shared secret key with the intercept-resend attack, Alice and Bob will easily find Eve's interception attack.

For Eve's interception attack, if Eve initially prepares Bell states instead of a state sequence with single particles, then Eve should send one state sequence of these EPR pairs and reserve the other state sequence. Suppose Alice also informs Bob to measure the decoy particles with computational bases $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. There is no correlation between the state sequence received by Bob and Alice's corresponding state sequence, therefore the probability that Bob's measurement outcomes are same as Alice's is 0.25. Statistically, the probability that the Bell state Eve prepared is $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ is only 0.25. Therefore, the total probability that Eve is successfully found by Alice and Bob is $p_e = 1 - \frac{1}{16^n}$. In the tri-party QKA protocol, the transmission of six sequences is involved, so the total probability during the whole protocol that Eve is successfully found by Alice and Bob is $p_e = 1 - \left(\frac{1}{16^n}\right)^6$ and it is very difficult for Eve to obtain the shared secret key with this attack. Therefore, it is impossible for Eve to obtain the final shared secret key with the interception attack.

5.3 Efficiency Analysis

Cabello's qubit efficiency η is defined as $\frac{c}{q+b}$, where c represents the total number of shared classical bits, q indicates the total amount of used qubits while b denotes the total number of classical bits exchanged for decoding the message. The qubit efficiency of our proposed

Table 2 Comparison with similar QKA protocols

Protocol	Category	Quantum resource	Qubit efficiency
Ref. [24]	Complete-graph-type	Bell states	$\frac{1}{3N(N-1)}$
Ref. [25]	Complete-graph-type	Single photons	$\frac{1}{2N(N-1)}$
Ref. [26]	Circle-type	Single photons	$\frac{1}{N^2}$
Ref. [39]	Circle-type	G-like states and Bell states	$\frac{8}{(10+N)N}$
Ours	Circle-type	G-like states and Bell states	$\frac{18}{(21+N)N}$

multiparty QKA protocol is $\frac{2n}{\left(7n+\frac{N}{3}n\right)\frac{N}{3}}$, i.e., $\frac{18}{(21+N)N}$. The comparison with similar multiparty QKA protocols from the aspects of category, quantum resource and qubit efficiency are compiled in Table 2. From Table 2, it is obvious that the performance of this proposed multiparty QKA protocol is higher especially the number of participants in the protocol is big enough.

6 Conclusion

Based on entanglement swapping between Bell states and G-like states, a novel multiparty quantum key agreement protocol is designed. It is composed of multiple tri-party quantum key agreement protocols and it can resist most of common attacks. The new multiparty quantum key agreement protocol is fair and secure, and it is simpler with few calculations. In addition, the proposed multiparty QKA protocol has better performance than some typical quantum key agreement protocols especially under enough participants in the protocol. The protocol can also be realized with current technology.

Acknowledgements This work is supported by the National Natural Science Foundation of China (Grant Nos. 61871205 and 61561033), the Major Academic Discipline and Technical Leader of Jiangxi Province (Grant No. 20162BCB22011) and the Natural Science Foundation of Jiangxi Province (Grant No. 20171BAB202002).

References

1. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing [C]. In : Proceedings of IEEE international conference on computers, systems, and signal processing, pp. 175–179. Bangalore (1984)
2. Ekert, A.K.: Quantum cryptography based on Bell's theorem [J]. Phys. Rev. Lett. **67**(6), 661–663 (1991)
3. Bennett, C.H., Brassard, G., Mermin, N.D.: Quantum cryptography without Bell's theorem [J]. Phys. Rev. Lett. **68**(5), 557–559 (1992)
4. Dušek, M., Haderka, O., Hendrych, M., Myška, R.: Quantum identification system [J]. Phys. Rev. A. **60**(1), 149–156 (1999)
5. Curty, M., Santos, D.J.: Quantum authentication of classical messages [J]. Phys. Rev. A. **64**(6), 062309 (2001)
6. Zhou, N., Wang, L., Gong, L., Zuo, X., Liu, Y.: Quantum deterministic key distribution protocols based on teleportation and entanglement swapping [J]. Opt. Commun. **284**(19), 4836–4842 (2011)
7. Bennett, C. H., Brassard, G., Crépeau, C., Skubiszewska, M. H.: Practical quantum oblivious transfer [C]. In: Annual international cryptology conference. pp. 351–366. Springer, Berlin Heidelberg (1991)
8. He, G.P., Wang, Z.D.: Oblivious transfer using quantum entanglement [J]. Phys. Rev. A. **73**(1), 012331 (2006)

9. Gottesman D, Chuang I.: Quantum digital signatures [J]. arXiv preprint quant-ph/0105032 (2001)
10. Li, Q., Chan, W.H., Long, D.Y.: Arbitrated quantum signature scheme using Bell states [J]. Phys. Rev. A. **79**(5), 054307 (2009)
11. Wen, X., Tian, Y., Ji, L., Niu, X.: A group signature scheme based on quantum teleportation [J]. Phys. Scr. **81**(5), 055001 (2010)
12. Yin, X.R., Ma, W.P., Liu, W.Y.: A blind quantum signature scheme with χ-type entangled states [J]. Int. J. Theor. Phys. **51**(2), 455–461 (2012)
13. Hillery, M., Bužek, V., Berthiaume, A.: Quantum secret sharing [J]. Phys. Rev. A. **59**(3), 1829–1834 (1999)
14. Xiao, L., Long, G.L., Deng, F.G., Pan, J.W.: Efficient multiparty quantum-secret-sharing schemes [J]. Phys. Rev. A. **69**(5), 052307 (2004)
15. Zhang, Z., Man, Z.: Multiparty quantum secret sharing of classical messages based on entanglement swapping [J]. Phys. Rev. A. **72**(2), 022303 (2005)
16. Mayers, D.: Unconditionally secure quantum bit commitment is impossible [J]. Phys. Rev. Lett. **78**(17), 3414–3417 (1997)
17. Kent, A.: Quantum bit string commitment [J]. Phys. Rev. Lett. **90**(23), 237901 (2003)
18. Boström, K., Felbinger, T.: Deterministic secure direct communication using entanglement [J]. Phys. Rev. Lett. **89**(18), 187902 (2002)
19. Wang, C., Deng, F.G., Long, G.L.: Multi-step quantum secure direct communication using multiparticle Green–Horne–Zeilinger state [J]. Opt. Commun. **253**(1–3), 15–20 (2005)
20. Chang, Y., Xu, C.X., Zhang, S.B., Yan, L.L.: Quantum secure direct communication and authentication protocol with single photons [J]. Chin. Sci. Bull. **58**(36), 4571–4576 (2013)
21. Zhou, N., Zeng, G., Xiong, J.: Quantum key agreement protocol [J]. Electron. Lett. **40**(18), 1149–1150 (2004)
22. Hsueh, C.C., Chen, C.Y.: Quantum key agreement protocol with maximally entangled states [C]. Proceedings of the 14th information security conference, pp. 236–242, Taipei (2004)
23. Chong, S.K., Tsai, C.W., Hwang, T.: Improvement on "quantum key agreement protocol with maximally entangled states" [J]. Int. J. Theor. Phys. **50**(6), 1793–1802 (2011)
24. Shi, R.H., Zhong, H.: Multi-party quantum key agreement with Bell states and Bell measurements [J]. Quantum Inf. Process. **12**(2), 921–932 (2013)
25. Liu, B., Gao, F., Huang, W., Wen, Q.Y.: Multiparty quantum key agreement with single particles [J]. Quantum Inf. Process. **12**(4), 1797–1805 (2013)
26. Sun, Z., Zhang, C., Wang, B., Li, Q., Long, D.: Improvements on multiparty quantum key agreement with single particles [J]. Quantum Inf. Process. **12**(11), 3411–3420 (2013)
27. Yin, X.R., Ma, W.P., Liu, W.Y.: Three-party quantum key agreement with two-photon entanglement [J]. Int. J. Theor. Phys. **52**(11), 3915–3921 (2013)
28. Huang, W., Wen, Q.Y., Liu, B., Gao, F., Sun, Y.: Quantum key agreement with EPR pairs and single-particle measurements [J]. Quantum Inf. Process. **13**(3), 649–663 (2014)
29. Sun, Z.W., Yu, J.P., Wang, P.: Efficient multi-party quantum key agreement by cluster states [J]. Quantum Inf. Process. **15**(1), 373–384 (2016)
30. He, Y.F., Ma, W.P.: Two-party quantum key agreement against collective noise [J]. Quantum Inf. Process. **15**(12), 5023–5035 (2016)
31. Cai, B.B., Guo, G.D., Lin, S.: Multi-party quantum key agreement without entanglement [J]. Int. J. Theor. Phys. **56**(4), 1039–1051 (2017)
32. He, Y.F., Ma, W.P.: Two-party quantum key agreement based on four-particle GHZ states [J]. Int. J. Theor. Phys. **14**(01), 1650007 (2016)
33. Sun, Z.W., Zhang, C., Wang, P., Yu, J.P., Zhang, Y., Long, D.Y.: Multi-party quantum key agreement by an entangled six-qubit state [J]. Int. J. Theor. Phys. **55**(3), 1920–1929 (2016)
34. Gu, J., Hwang, T.: Improvement of "novel multiparty quantum key agreement protocol with GHZ states" [J]. Int. J. Theor. Phys. **56**(10), 3108–3116 (2017)
35. He, Y.F., Ma, W.P.: Two-party quantum key agreement with five-particle entangled states [J]. Int. J. Quantum Inf. **15**(03), 1750018 (2017)
36. Cai, B.B., Guo, G.D., Lin, S.: Multi-party quantum key agreement with teleportation [J]. Mod. Phys. Lett. B. **31**(10), 1750102 (2017)
37. Wang, P., Sun, Z.W., Sun, X.Q.: Multi-party quantum key agreement protocol secure against collusion attacks [J]. Quantum Inf. Process. **16**(7), 170 (2017)
38. Cai, T., Jiang, M., Cao, G.: Multi-party quantum key agreement with five-qubit brown states [J]. Quantum Inf. Process. **17**(5), 103 (2018)
39. Min, S.Q., Chen, H.Y., Gong, L.H.: Novel multi-party quantum key agreement protocol with G-like states and Bell states [J]. Int. J. Theor. Phys. **57**(6), 1811–1822 (2018)

40. Bennett, C.H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., Wootters, W.K.: Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels [J]. Phys. Rev. Lett. **70**(13), 1895 (1993)
41. Deng, F.G., Long, G.L., Wang, Y., Xiao, L.: Increasing the efficiencies of random-choice-based quantum communication protocols with delayed measurement [J]. Chin. Phys. Lett. **21**(11), 2097 (2004)
42. Liu, B., Xiao, D., Jia, H.Y., Liu, R.Z.: Collusive attacks to "circle-type" multi-party quantum key agreement protocols [J]. Quantum Inf. Process. **15**(5), 2113–2124 (2016)
43. Deng, F.G., Li, X.H., Zhou, H.Y., Zhang, Z.: Improving the security of multiparty quantum secret sharing against Trojan horse attack [J]. Phys. Rev. A. **72**(4), 044302 (2005)
44. Li, X.H., Deng, F.G., Zhou, H.Y.: Improving the security of secure direct communication based on the secret transmitting order of particles [J]. Phys. Rev. A. **74**(5), 054302 (2006)
45. Cabello, A.: Quantum key distribution in the Holevo limit [J]. Phys. Rev. A. **85**(26), 5635 (2000)