Commun. Theor. Phys. **66** (2016) 280–290 Vol. 66, No. 3, September 1, 2016

Multi-Party Quantum Private Comparison Protocol Based on Entanglement Swapping of Bell Entangled States*

Tian-Yu Ye (叶天语)†

College of Information and Electronic Engineering, Zhejiang Gongshang University, Hangzhou 310018, China

(Received May 19, 2016; revised manuscript received July 4, 2016)

Abstract *Recently, Liu et al. proposed a two-party quantum private comparison (QPC) protocol using entanglement swapping of Bell entangled state (Commun. Theor. Phys.* **57** *(2012) 583). Subsequently, Liu et al. pointed out that in Liu et al.'s protocol, the TP can extract the two users' secret inputs without being detected by launching the Bell-basis measurement attack, and suggested the corresponding improvement to mend this loophole (Commun. Theor. Phys.* **62** *(2014) 210). In this paper, we first point out the information leakage problem toward TP existing in both of the above two protocols, and then suggest the corresponding improvement by using the one-way hash function to encrypt the two users' secret inputs. We further put forward the three-party QPC protocol also based on entanglement swapping of Bell entangled state, and then validate its output correctness and its security in detail. Finally, we generalize the three-party QPC protocol into the multi-party case, which can accomplish arbitrary pair's comparison of equality among K users within one execution.*

PACS numbers: 03.67.Dd, 03.67.Hk, 03.67.Pp

Key words: multi-party quantum private comparison, Bell entangled state, entanglement swapping, information leakage

1 Introduction

Secure multi-party computation (SMPC), which was first introduced by Yao[1] in the millionaire problem, is a basic and important topic in classical cryptography. In Yao's millionaire problem, two millionaires wish to know who is richer under the condition of not revealing the genuine amount of asset to each other. Afterward, Boudot *et al.*[2] constructed an equality comparison protocol to judge whether two millionaires are equally rich. SMPC can be applied into many scenarios such as private bidding and auctions, secret ballot elections, e-commerce, data mining and so on.

As a particular branch of SMPC, classical private comparison (CPC) aims to determine whether two secret inputs from different users are equal or not without disclosing their genuine values. With the development of quantum technology, CPC has been extensively generalized to its quantum counterpart, i.e., quantum private comparison (QPC), whose security is based on the quantum mechanics principles rather than the computation complexity. However, Lo[3] pointed out that in a two-party scenario, the equality function cannot be securely evaluated. Under this circumstance, some additional assumptions, for example, a third party (TP), are needed.

The first QPC protocol was proposed by Yang *et al.*[4] using Einstein–Podolsky–Rosen (EPR) pairs with the help of one TP. In the same year, Yang *et al.*[5] proposed the QPC protocol with single photons. The security of these two protocols are essentially based on the one-way hash function. In 2010, Chen *et al.*[6] designed the QPC protocol with Greenberger–Horne–Zeilinger (GHZ) states. In 2012, Tseng *et al.*[7] constructed a novel QPC protocol with EPR pairs. In these two protocols, the secret inputs from two users are encrypted with the one-time-pad keys derived from the single-particle measurements. In 2012, Liu *et al.*[8] proposed the QPC protocol based on entanglement swapping of Bell states (hereafter, this protocol is called as LWC-QPC protocol). In this protocol, the secret inputs from two users are encrypted with the one-time-pad keys derived from the Bell-basis measurements after entanglement swapping of the original Bell states. However, Liu *et al.*[9] pointed out that in the protocol of Ref. [8], the TP can extract the two users' secret inputs without being detected by launching the Bell-basis measurement attack, and suggested an improved protocol (hereafter, this improved protocol is called as LLCLL-improved-QPC protocol). Up to now, besides the protocols mentioned above, many other two-party QPC protocols[10−34] have also been designed with different quantum states and quantum technologies.

As to the role of TP, Chen *et al.*[6] first introduced the semi-honest model. That is, TP executes the protocol loyally, records all its intermediate computations but might try to reveal the users' secret inputs from the record under the limit that he cannot conspire with the adversary including the dishonest user. However, Yang *et al.*[12] pointed out that this model of semi-honest TP was unreasonable and thought that the reasonable one should be in the following way: TP is allowed to misbehave on his own and also cannot be corrupted by the adversary in-

*Supported by the National Natural Science Foundation of China under Grant No. 61402407

†E-mail: happyyty@aliyun.com

cluding the dishonest user. In fact, up to now, this kind of assumption for TP is the most reasonable one.

Suppose that there are K users, each of whom has a secret input. They want to know whether their K secret inputs are equal or not without disclosing them. If the two-party QPC protocol is adopted to solve this multi-party equality comparison problem, the same two-party QPC protocol has to be executed with $K-1 \sim K(K-1)/2$ times so that the efficiency is not high enough. In 2013, Chang *et al.*[35] proposed the first multi-party quantum private comparison (MQPC) protocol with n-particle GHZ class states, which can accomplish arbitrary pair's comparison of equality among K users within one execution. Subsequently, the MQPC protocol based on d-dimensional basis states and quantum fourier transform,[36] and the MQPC protocol based on n-level entangled states and quantum fourier transform[37] were constructed. However, there are still few MQPC protocols until now.

In this paper, after carefully investigating the LLCLL-improved-QPC protocol, we find out that it still has an information leakage problem toward TP. Then we suggest an improved strategy for this loophole. We further put forward the three-party QPC protocol also based on entanglement swapping of Bell entangled state and generalize it into the multi-party case accordingly.

2 Review of the LLCLL-Improved-QPC Protocol

For integrity, in this section, a brief review of the LLCLL-improved-QPC protocol is given.

Alice and Bob have two secret integers, X and Y, respectively, where

$$X = \sum_{j=0}^{L-1} x_j 2^j\,, \quad Y = \sum_{j=0}^{L-1} y_j 2^j\,,$$

here, $x_j, y_j \in \{0,1\}$. They want to know whether X and Y are equal or not with the help of a semi-honest TP.

The LLCLL-improved-QPC protocol can be depicted in the following way:

Step 1 Alice/Bob divides her/his binary representation of X/Y into $\lceil L/2\rceil$ groups

$$G_1^A, G_2^A, \ldots, G_{\lceil L/2\rceil}^A / G_1^B, G_2^B, \ldots, G_{\lceil L/2\rceil}^B\,,$$

where each group contains two binary bits. If L mod $2 = 1$, one 0 should be added to $G_{\lceil L/2\rceil}^A / G_{\lceil L/2\rceil}^B$ by Alice/Bob.

Step 2 Alice/Bob/TP prepares $\lceil L/2\rceil$ quantum states all in the state of $|\phi^+\rangle_{A_1A_2}/\ |\phi^+\rangle_{B_1B_2}\ /|\phi^+\rangle_{T_1T_2}$. Afterward, Alice/Bob/TP picks out the first particle from each state to form an ordered sequence $S_1^A/\ S_1^B/\ S_1^T$. The remaining second particle from each state automatically forms the other ordered sequence $S_2^A/\ S_2^B/\ S_2^T$.

Step 3* Alice/TP prepares L' decoy photons randomly in one of the four states $\{\ |0\rangle, |1\rangle, |+\rangle, |-\rangle\ \}$ to form sequence $D_A/\ D_T$. Then, Alice/TP randomly inserts $D_A/\ D_T$ into $S_2^A/\ S_2^T$ to obtain $S_2^{A^*}/\ S_2^{T^*}$. Afterward, Alice and TP exchange $S_2^{A^*}$ and $S_2^{T^*}$ between them. To check the security of the TP-Alice channel, Alice and TP implement the following procedures after Alice receives $S_2^{T^*}$: (i) TP tells Alice the positions and the measurement bases of decoy photons in $S_2^{T^*}$; (ii) Alice uses the measurement bases TP told to measure the decoy photons in $S_2^{T^*}$ and informs TP of her measurement results; (iii) TP computes the error rate by comparing the initial states of the decoy photons in $S_2^{T^*}$ with Alice's measurement results. If the error rate is low enough, they will continue the next step and Alice will drop out the decoy photons in $S_2^{T^*}$; otherwise, they will halt the communication.

Step 4 For $j = 1, 2, \ldots, \lceil L/2\rceil$, Alice performs the Bell-basis measurement on each pair in (S_1^A, S_2^T) and obtains the corresponding measurement result M_j^A. If M_j^A is $|\phi^+\rangle/\ |\phi^-\rangle/\ |\psi^+\rangle/\ |\psi^-\rangle$, then $R_j^A = 00/01/10/11$. Consequently, the corresponding pair in (S_1^T, S_2^A) in TP's hands is collapsed into one of the four Bell states. These $\lceil L/2\rceil$ collapsed Bell states in TP's hands are denoted by $(S_1^{T''}, S_2^{T''})$.

Step 5* Bob prepares L' decoy photons randomly in one of the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ to form sequence D_B and randomly inserts D_B into S_2^B to obtain $S_2^{B^*}$. Then, Bob and TP exchange $S_2^{B^*}$ and $S_2^{A^*}$ between them. After TP receives $S_2^{B^*}$, TP and Bob check the security of the Bob-TP channel with the same method as that in Step 3*. On the other hand, after Bob receives $S_2^{A^*}$, Bob makes one-time eavesdropping check for the Alice-TP channel and the TP-Bob channel with Alice by checking the decoy photons in $S_2^{A^*}$. If all quantum channels are secure, Bob and TP will discard the decoy photons and continue the next step.

Step 6 For $j = 1, 2, \ldots, \lceil L/2\rceil$, Bob performs the Bell-basis measurement on each pair in $(S_1^B, S_2^{T''})$ and obtains the corresponding measurement result M_j^B. If M_j^B is $|\phi^+\rangle/|\phi^-\rangle/|\psi^+\rangle/|\psi^-\rangle$, then $R_j^B = 00/01/10/11$. Consequently, the corresponding pair in $(S_1^{T''}, S_2^B)$ in TP's hands is collapsed into one of the four Bell states. TP also performs the Bell-basis measurement on each pair in $(S_1^{T''}, S_2^B)$ and obtains the corresponding measurement result M_j^T. If M_j^T is $|\phi^+\rangle/|\phi^-\rangle/|\psi^+\rangle/|\psi^-\rangle$, then $R_j^T = (r_j^{T_1} r_j^{T_2}) = 00/01/10/11$.

Step 7 For $j = 1, 2, \ldots, \lceil L/2\rceil$, Alice and Bob calculate $R_j = (R_j^A \oplus G_j^A) \oplus (R_j^B \oplus G_j^B) = (r_j^1 r_j^2)$, and send R_j to TP. Then, TP calculates $R = \sum_{j=1}^{\lceil L/2\rceil} \big((r_j^1 \oplus r_j^{T_1}) + (r_j^2 \oplus r_j^{T_2})\big)$. Without loss of generality, we assume that Alice needs to send the result of $R_j^A \oplus G_j^A$ to Bob for calculating R_j.

Step 8 TP sends R to Alice and Bob. If $R = 0$, Alice and Bob conclude that $X = Y$; otherwise, they know that $X \neq Y$.

Note that the LLCLL-improved-QPC protocol only makes change for Steps 3 and 5 of LWC-QPC protocol. Steps 1, 2, 4, 6, 7, and 8 of LWC-QPC protocol are kept unchanged.

3 Information Leakage Problem and Corresponding Improvement

In this section, we first point out the information leakage problem in the LLCLL-improved-QPC protocol in

Subsec. 3.1, then suggest the corresponding improvement in Subsec. 3.2.

3.1 *Information Leakage Problem*

The protocol involves many different parameters, including Alice's two-bit input G_j^A, Bob's two-bit input G_j^B, Alice's measurement result M_j^A, the coding of Alice's measurement result R_j^A, Bob's measurement result M_j^B, the coding of Bob's measurement result R_j^B, TP's measurement result M_j^T, the coding of TP's measurement result R_j^T, the result of $(R_j^A \oplus G_j^A) \oplus (R_j^B \oplus G_j^B)$ (i.e., R_j) and the result of $(r_j^1 \oplus r_j^{T_1}) + (r_j^2 \oplus r_j^{T_2})$ (i.e., R'_j). The relations among these different parameters when $G_j^A = 00$ are listed in Table 1 (see Appendix). It is easy to find out that R'_j totally has three different kinds of value, i.e., 0, 1 and 2. When $R'_j = 0$, we have $G_j^A = G_j^B$; otherwise, it follows $G_j^A \neq G_j^B$. After deducing all the relations among these different parameters when $G_j^A = 01$, $G_j^A = 10$ and $G_j^A = 11$, respectively, we can further summarize the relations between R'_j and G_j^A, G_j^B, which are shown in Table 2 (see Appendix). From Table 2, it is easy to know that when $R'_j = 0$, (G_j^A, G_j^B) may be (00,00), (01,01), (10,10) or (11,11); when $R'_j = 1$, (G_j^A, G_j^B) may be (00,01), (01,00), (10,11), (11,10), (00,10), (01,11), (10,00) or (11,01); and when $R'_j = 2$, (G_j^A, G_j^B) may be (00,11), (01,10), (10,01) or (11,00). Furthermore, when $G_j^A = G_j^B$, there are totally four kinds of (G_j^A, G_j^B); and when $G_j^A \neq G_j^B$, there are totally twelve kinds of (G_j^A, G_j^B). As a result, when $R'_j = 1$, the eight possible kinds of (G_j^A, G_j^B) include 3 bits for TP, which means that $\log_2 3 - 1$ bit information has been leaked out to TP; and when $R'_j = 2$, the four possible kinds of (G_j^A, G_j^B) include 2 bits for TP, which means that $\log_2 3$ bit information has been leaked out to TP. This protocol has an information leakage problem toward TP indeed.

3.2 *Corresponding Improvement*

In order to avoid the information leakage problem toward TP, we should make TP get nothing about G_j^A and G_j^B when $R'_j \neq 0$. In this Subsection, we give an improvement to mend this loophole. In order to retain the main features of the LWC-QPC protocol, we make as few modifications as possible. The LWC-QPC protocol should be modified as follows:

Step $1^{\#}$ Similar to the QPC protocols of Refs. [4–5], Alice and Bob share a secret one-way hash function H in advance. Here, the one-way hash function is defined as: $H : \{0,1\}^L \to \{0,1\}^N$, where L is the length of the secret inputs and N is the length of the hash values of the secret inputs. The hash values of X and Y are $H(X) = X^{\#} = (x_{N-1}^{\#}, x_{N-2}^{\#}, \ldots, x_0^{\#})$ and $H(Y) = Y^{\#} = (y_{N-1}^{\#}, y_{N-2}^{\#}, \ldots, y_0^{\#})$, respectively. Alice/Bob divides her/his binary representation of $X^{\#}$/ $Y^{\#}$ into $\lceil N/2 \rceil$ group $G_1^{A^{\#}}, G_2^{A^{\#}}, \ldots, G_{\lceil N/2 \rceil}^{A^{\#}}/G_1^{B^{\#}}, G_2^{B^{\#}}, \ldots, G_{\lceil N/2 \rceil}^{B^{\#}}$, where each group contains two binary bits. If N mod2 $= 1$, one 0 should be added to $G_{\lceil N/2 \rceil}^{A^{\#}}/G_{\lceil N/2 \rceil}^{B^{\#}}$ by Alice/Bob.

Step $2^{\#}$ Alice/Bob/TP prepares $\lceil N/2 \rceil$ quantum states all in the state of $|\phi^+\rangle_{A_1A_2}/|\phi^+\rangle_{B_1B_2}/|\phi^+\rangle_{T_1T_2}$. Afterward, Alice, Bob and TP do the same thing as that in Step 2 of the LWC-QPC protocol.

Step $3^{\#}, 4^{\#}, 5^{\#}$ and $6^{\#}$ These Steps here are the same as those of the LWC-QPC protocol.

Step $7^{\#}$ For $j = 1, 2, \ldots, \lceil N/2 \rceil$, Alice and Bob calculate $R_j = (R_j^A \oplus G_j^{A^{\#}}) \oplus (R_j^B \oplus G_j^{B^{\#}}) = (r_j^1 r_j^2)$, and send R_j to TP. Then, TP calculates $R = \sum_{j=1}^{\lceil N/2 \rceil}((r_j^1 \oplus r_j^{T_1}) + (r_j^2 \oplus r_j^{T_2}))$. Without loss of generality, we assume that Alice needs to send the result of $R_j^A \oplus G_j^{A^{\#}}$ to Bob for calculating R_j.

Step $8^{\#}$ This Step here is the same as that of the LWC-QPC protocol.

Compared with the LWC-QPC protocol, in the above improvement, we add the encryption process for Alice and Bob' secret inputs with a one-way hash function to enhance their privacy. Similar to the LWC-QPC protocol, in the above improvement, TP can also obtain the relations between R'_j and $G_j^{A^{\#}}$, $G_j^{B^{\#}}$, which are shown in Table 3 (See appendix). However, the one-way property of the hash function can guarantee that knowing $G_j^{A^{\#}}$ and $G_j^{B^{\#}}$ is still helpless to deduce G_j^A and G_j^B. As a result, TP cannot get the relations between R'_j and G_j^A, G_j^B when $R'_j \neq 0$. Therefore, none of information about Alice and Bob' secret inputs have been leaked out to TP when $R'_j \neq 0$. It can be concluded that using a one-way hash function to encrypt Alice and Bob' secret inputs beforehand helps overcome the information leakage problem toward TP.

It should be further emphasized that in order to retain the main features of the LWC-QPC protocol as many as possible, the above improvement still adopts the same eavesdropping check methods to those used in the LWC-QPC protocol. Because the encryption process for Alice and Bob' secret inputs with a one-way hash function can automatically resist the Bell-basis measurement attack from TP suggested by Liu *et al.*,[9] it is not necessary for the above improvement to employ the decoy photon eavesdropping check methods any more.

4 Three-Party QPC Protocol Based on Entanglement Swapping of Bell Entangled States

In this section, by utilizing the above analysis, we suggest the three-party QPC protocol based on entanglement swapping of Bell entangled states in Subsec. 4.1 first, then analyze its correctness and security in Subsec. 4.2.

4.1 *Three-Party QPC Protocol*

Alice, Bob and Charlie have three secret integers, X, Y and Z, respectively, where $X = \sum_{j=0}^{L-1} x_j 2^j$, $Y = \sum_{j=0}^{L-1} y_j 2^j$, and $Z = \sum_{j=0}^{L-1} z_j 2^j$. Here, $x_j, y_j, z_j \in \{0,1\}$. They want to know whether every two of X, Y, and Z

are equal or not with the help of a semi-honest TP. They achieve the equality comparison of every two secret integers by implementing the following steps.

Step 1 Preparation

(a) Similar to the QPC protocols of Refs. [4–5], Alice, Bob and Charlie share a secret one-way hash function H in advance. The hash values of X, Y and Z are $H(X) = X^{\#} = (x^{\#}_{N-1}, x^{\#}_{N-2}, \ldots, x^{\#}_0)$, $H(Y) = Y^{\#} = (y^{\#}_{N-1}, y^{\#}_{N-2}, \ldots, y^{\#}_0)$, and $H(Z) = Z^{\#} = (z^{\#}_{N-1}, z^{\#}_{N-2}, \ldots, z^{\#}_0)$, respectively. Alice/Bob/Charlie divides her/his/her binary representation of $X^{\#}/Y^{\#}/\ Z^{\#}$ into $\lceil N/2 \rceil$ groups $G^{A^{\#}}_1, G^{A^{\#}}_2, \ldots, G^{A^{\#}}_{\lceil N/2 \rceil}/G^{B^{\#}}_1, G^{B^{\#}}_2, \ldots, G^{B^{\#}}_{\lceil N/2 \rceil}/G^{C^{\#}}_1, G^{C^{\#}}_2, \ldots, G^{C^{\#}}_{\lceil N/2 \rceil}$, where each group contains two binary bits. If $N \bmod 2 = 1$, one 0 should be added to $G^{A^{\#}}_{\lceil N/2 \rceil}/G^{B^{\#}}_{\lceil N/2 \rceil}/G^{C^{\#}}_{\lceil N/2 \rceil}$ by Alice/Bob/ Charlie.

(b) Alice/Bob/Charlie/TP prepares $\lceil N/2 \rceil$ quantum states all in the state of $|\phi^+\rangle_{A_1A_2}/|\phi^+\rangle_{B_1B_2}/|\phi^+\rangle_{C_1C_2}/|\phi^+\rangle_{T_1T_2}$. Afterward, Alice/Bob/Charlie/TP picks out the first particle from each state to form an ordered sequence $S^A_1/S^B_1/S^C_1/S^T_1$. The remaining second particle from each state automatically forms the other ordered sequence $S^A_2/S^B_2/S^C_2/S^T_2$.

(c) For the security check, Alice/TP prepares a sequence of L' quantum states all in the state of $|\phi^+\rangle$ again, which is denoted as $D_{A'}/D_{T'}$. Then Alice/TP inserts the first and the second particles of each Bell state in $D_{A'}/D_{T'}$ into S^A_1/S^T_1 and S^A_2/S^T_2 at the same positions, respectively. Accordingly, Alice/TP obtains $S^{A'}_1/S^{T'}_1$ and $S^{A'}_2/S^{T'}_2$. Then, Alice and TP exchange $S^{A'}_2$ and $S^{T'}_2$ between them. To ensure the transmission security of Alice-TP/TP-Alice quantum channel, the entanglement correlation between two different particles of each Bell state in $D_{A'}/D_{T'}$ is used to check whether there is an eavesdropper or not. If there is no eavesdropper, Alice and TP drop out the sample particles, and implement the next step.

(d) For $j = 1, 2, \ldots, \lceil N/2 \rceil$, Alice performs the Bell-basis measurement on each pair in (S^A_1, S^T_2) and obtains the corresponding measurement result M^A_j. If M^A_j is $|\phi^+\rangle/|\phi^-\rangle/|\psi^+\rangle/|\psi^-\rangle$, then $R^A_j = 00/01/10/11$. Consequently, the corresponding pair in (S^T_1, S^A_2) in TP's hands is collapsed into one of the four Bell states. These $\lceil N/2 \rceil$ collapsed Bell states in TP's hands are denoted by $(S^{T^1}_1, S^{T^1}_2)$.

Step 2 The First Round Comparison

(a) Bob/TP prepares a sequence of L' quantum states all in the state of $|\phi^+\rangle$ to guarantee the security for the exchange of S^B_2 and $S^{T^1}_2$. If there is no eavesdropper, Bob and TP drop out the sample particles, and implement the next step.

(b) For $j = 1, 2, \ldots, \lceil N/2 \rceil$, Bob performs the Bell-basis measurement on each pair in $(S^B_1, S^{T^1}_2)$ and obtains the corresponding measurement result M^B_j. If M^B_j is $|\phi^+\rangle/|\phi^-\rangle/|\psi^+\rangle/|\psi^-\rangle$, then $R^B_j = 00/01/10/11$. Consequently, the corresponding pair in $(S^{T^1}_1, S^B_2)$ in TP's hands is collapsed into one of the four Bell states. TP also performs the Bell-basis measurement on each pair in $(S^{T^1}_1, S^B_2)$ and obtains the corresponding measurement result $M^{T^1}_j$. If $M^{T^1}_j$ is $|\phi^+\rangle/|\phi^-\rangle/|\psi^+\rangle/|\psi^-\rangle$, then $R^{T^1}_j = (r^{T^1_1}_j r^{T^1_2}_j) = 00/01/10/11$. These $\lceil N/2 \rceil$ collapsed Bell states in TP's hands are denoted by $(S^{T^2}_1, S^{T^2}_2)$.

(c) For $j = 1, 2, \ldots, \lceil N/2 \rceil$, Alice and Bob cooperate to calculate

$$R^{AB}_j = (R^A_j \oplus G^{A^{\#}}_j) \oplus (R^B_j \oplus G^{B^{\#}}_j) = (r^{AB_1}_j r^{AB_2}_j),$$

and send R^{AB}_j to TP. Without loss of generality, we assume that Alice needs to send the result of $R^A_j \oplus G^{A^{\#}}_j$ to Bob for calculating R^{AB}_j. Then, TP calculates

$$R^{AB'}_j = (r^{AB_1}_j \oplus r^{T^1_1}_j) + (r^{AB_2}_j \oplus r^{T^1_2}_j),$$

$$R^{AB} = \sum_{j=1}^{\lceil N/2 \rceil} R^{AB'}_j .$$

Afterward, TP publishes R^{AB} to Alice and Bob. If $R^{AB} = 0$, Alice and Bob conclude that $X = Y$; otherwise, they know that $X \neq Y$.

Step 3 The Second Round Comparison

(a) Charlie/TP prepares a sequence of L' quantum states all in the state of $|\phi^+\rangle$ to guarantee the security for the exchange of S^C_2 and $S^{T^2}_2$. If there is no eavesdropper, Charlie and TP drop out the sample particles, and implement the next step.

(b) For $j = 1, 2, \ldots, \lceil N/2 \rceil$, Charlie performs the Bell-basis measurement on each pair in $(S^C_1, S^{T^2}_2)$ and obtains the corresponding measurement result M^C_j. If M^C_j is $|\phi^+\rangle/|\phi^-\rangle/|\psi^+\rangle/|\psi^-\rangle$, then $R^C_j = 00/01/10/11$. Consequently, the corresponding pair in $(S^{T^2}_1, S^C_2)$ in TP's hands is collapsed into one of the four Bell states. TP also performs the Bell-basis measurement on each pair in $(S^{T^2}_1, S^C_2)$ and obtains the corresponding measurement result $M^{T^2}_j$. If $M^{T^2}_j$ is $|\phi^+\rangle/|\phi^-\rangle/|\psi^+\rangle/|\psi^-\rangle$, then $R^{T^2}_j = (r^{T^2_1}_j r^{T^2_2}_j) = 00/01/10/11$.

(c) For $j = 1, 2, \ldots, \lceil N/2 \rceil$, Alice, Bob and Charlie cooperate to calculate

$$R^{BC}_j = R^A_j \oplus (R^B_j \oplus G^{B^{\#}}_j) \oplus (R^C_j \oplus G^{C^{\#}}_j) = (r^{BC_1}_j r^{BC_2}_j),$$

and send R^{BC}_j to TP. Without loss of generality, assume that Alice and Bob send R^A_j and the result of $R^B_j \oplus G^{B^{\#}}_j$ to Charlie for calculating R^{BC}_j, respectively. Then, TP calculates

$$R^{BC'}_j = (r^{BC_1}_j \oplus r^{T^2_1}_j) + (r^{BC_2}_j \oplus r^{T^2_2}_j),$$

$$R^{BC} = \sum_{j=1}^{\lceil N/2 \rceil} R^{BC'}_j .$$

In the meanwhile, for $j = 1, 2, \ldots, \lceil N/2 \rceil$, Alice, Bob, and Charlie cooperate to calculate

$$R^{AC}_j = (R^A_j \oplus G^{A^{\#}}_j) \oplus R^B_j \oplus (R^C_j \oplus G^{C^{\#}}_j) = (r^{AC_1}_j r^{AC_2}_j),$$

and send R^{AC}_j to TP. Without loss of generality, assume that Alice and Bob send the result of $R^A_j \oplus G^{A^{\#}}_j$ and R^B_j

to Charlie for calculating R_j^{AC}, respectively. Then, TP calculates

$$R_j^{AC'} = (r_j^{AC_1} \oplus r_j^{T_1^2}) + (r_j^{AC_2} \oplus r_j^{T_2^2}),$$

$$R^{AC} = \sum_{j=1}^{\lceil N/2 \rceil} R_j^{AC'}.$$

Finally, TP sends R^{BC} to Bob and Charlie. If $R^{BC} = 0$, Bob and Charlie conclude that $Y = Z$; otherwise, they know that $Y \neq Z$. On the other hand, TP sends R^{AC}, to Alice and Charlie. If $R^{AC} = 0$, Alice and Charlie conclude that $X = Z$; otherwise, they know that $X \neq Z$. Until now, the protocol is finished.

For clarity, the entanglement swapping process of Bell states among the four participants of the above three-party QPC protocol is further shown in Fig. 1.

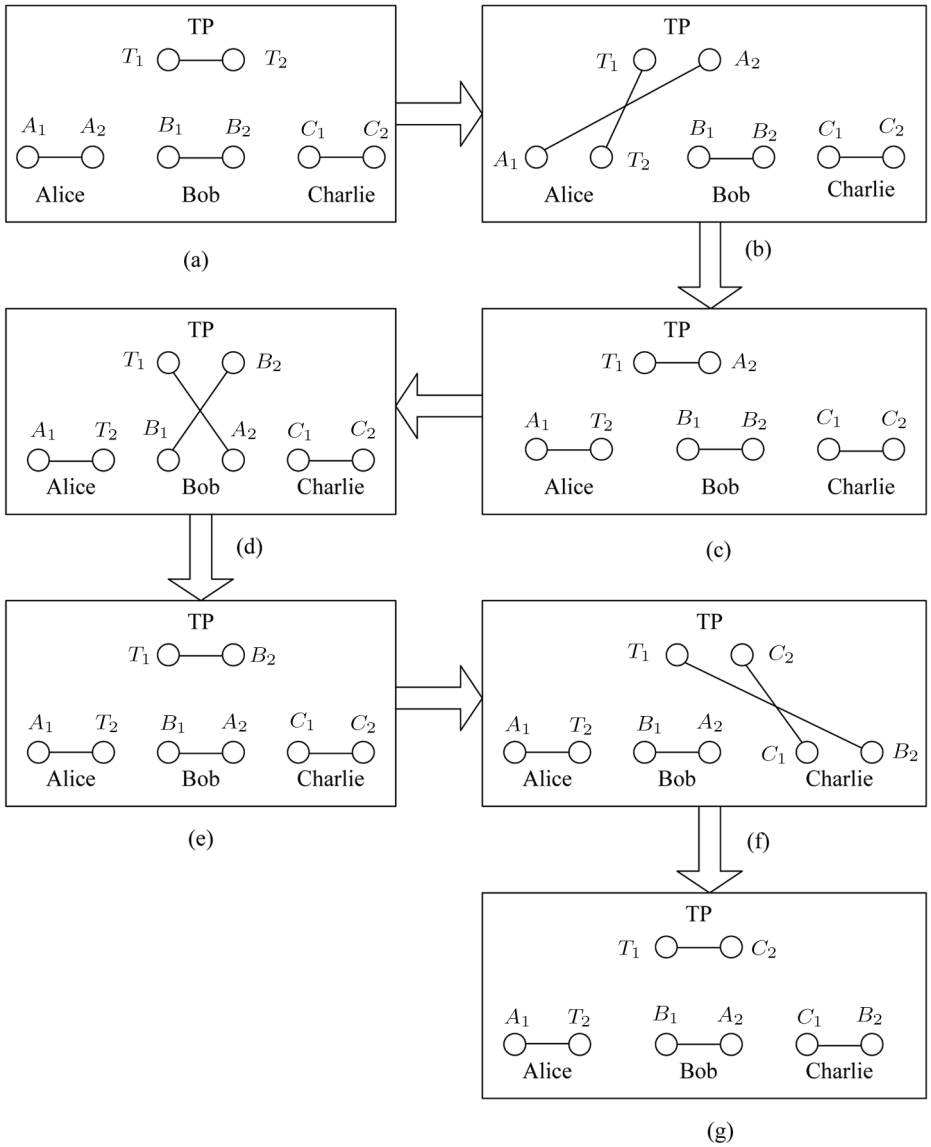

Fig. 1 The entanglement swapping of Bell states among the four participants. (a) Alice/Bob/Charlie/TP prepares quantum states in the state of $|\phi^+\rangle_{A_1A_2}/|\phi^+\rangle_{B_1B_2}/|\phi^+\rangle_{C_1C_2}/|\phi^+\rangle_{T_1T_2}$. (b) Alice and TP exchange the second particles A_2 and T_2 of the Bell states in their respective hands. (c) Particles T_1 and A_2 in TP's hands become entangled together after Alice performs the Bell-basis measurement on particles A_1 and T_2. (d) TP and Bob exchange particles A_2 and B_2. (e) Particles T_1 and B_2 in TP's hands become entangled together after Bob performs the Bell-basis measurement on particles B_1 and A_2. (f) TP and Charlie exchange particles B_2 and C_2. (g) Particles T_1 and C_2 in TP's hands become entangled together after Charlie performs the Bell-basis measurement on particles C_1 and B_2.

4.2 *Analysis*

We analyze the above three-party QPC protocol from the aspects of correctness and security here.

(i) *Correctness*

There are three cases of correctness need to be discussed in total.

Case 1 The Quality Comparison of Alice and Bob's Secret Inputs

As for the quality comparison of X and Y, Alice and Bob need to calculate $R_j^{AB} = (R_j^A \oplus G_j^{A^\#}) \oplus (R_j^B \oplus G_j^{B^\#}) = (r_j^{AB_1} r_j^{AB_2})$. Moreover, TP needs to calculate $R_j^{AB'} = (r_j^{AB_1} \oplus r_j^{T_1^1}) + (r_j^{AB_2} \oplus r_j^{T_2^1})$ and $R^{AB} = \sum_{j=1}^{\lceil N/2 \rceil} R_j^{AB'}$. According to Fig. 1, the following evolution is satisfied:

$$
\begin{aligned}
&\begin{cases} R_{A_1A_2} \oplus R_{T_1T_2} = R_{A_1T_2} \oplus R_{T_1A_2} \\ R_{T_1A_2} \oplus R_{B_1B_2} = R_{T_1B_2} \oplus R_{B_1A_2} \end{cases} \Rightarrow R_{A_1A_2} \oplus R_{T_1T_2} = R_{A_1T_2} \oplus (R_{B_1B_2} \oplus R_{T_1B_2} \oplus R_{B_1A_2}) \\
&\Rightarrow 00 = R_j^A \oplus R_j^B \oplus R_j^{T^1} \\
&\Rightarrow G_j^{A^\#} \oplus G_j^{B^\#} = (R_j^A \oplus G_j^{A^\#}) \oplus (R_j^B \oplus G_j^{B^\#}) \oplus R_j^{T^1} \\
&= R_j^{AB} \oplus R_j^{T^1} \\
&\Rightarrow R_j^{AB'} = \begin{cases} 0\,, & \text{if } G_j^{A^\#} = G_j^{B^\#}\,, \\ 1\,, \ \text{or } 2\,, & \text{if } G_j^{A^\#} \neq G_j^{B^\#}\,, \end{cases} \\
&\Rightarrow R^{AB} = \sum_{j=1}^{\lceil N/2 \rceil} R_j^{AB'} = \begin{cases} 0\,, & \text{if } X = Y\,, \\ \text{others}\,, & \text{if } X \neq Y\,. \end{cases}
\end{aligned} \tag{1}
$$

Therefore, the quality comparison result of X and Y in the above three-party QPC protocol is correct.

Case 2 The Quality Comparison of Bob and Charlie's Secret Inputs

As for the quality comparison of Y and Z , Alice, Bob and Charlie need to calculate $R_j^{BC} = R_j^A \oplus (R_j^B \oplus G_j^{B^\#}) \oplus (R_j^C \oplus G_j^{C^\#}) = (r_j^{BC_1} r_j^{BC_2})$. Moreover, TP needs to calculate $R_j^{BC'} = (r_j^{BC_1} \oplus r_j^{T_1^2}) + (r_j^{BC_2} \oplus r_j^{T_2^2})$ and $R^{BC} = \sum_{j=1}^{\lceil N/2 \rceil} R_j^{BC'}$. According to Fig.1, the following evolution is satisfied:

$$
\begin{aligned}
&\begin{cases} R_{A_1A_2} \oplus R_{T_1T_2} = R_{A_1T_2} \oplus R_{T_1A_2} \\ R_{T_1A_2} \oplus R_{B_1B_2} = R_{T_1B_2} \oplus R_{B_1A_2} \\ R_{T_1B_2} \oplus R_{C_1C_2} = R_{T_1C_2} \oplus R_{C_1B_2} \end{cases} \Rightarrow R_{A_1A_2} \oplus R_{T_1T_2} \\
&= R_{A_1T_2} \oplus (R_{B_1B_2} \oplus (R_{B_1A_2} \oplus (R_{C_1C_2} \oplus R_{T_1C_2} \oplus R_{C_1B_2}))) \\
&\Rightarrow 00 = R_j^A \oplus R_j^B \oplus R_j^C \oplus R_j^{T^2} \\
&\Rightarrow G_j^{B^\#} \oplus G_j^{C^\#} = R_j^A \oplus (R_j^B \oplus G_j^{B^\#}) \oplus (R_j^C \oplus G_j^{C^\#}) \oplus R_j^{T^2} \\
&= R_j^{BC} \oplus R_j^{T^2} \\
&\Rightarrow R_j^{BC'} = \begin{cases} 0\,, & \text{if } G_j^{B^\#} = G_j^{C^\#}\,, \\ 1\,, \ \text{or } 2\,, & \text{if } G_j^{B^\#} \neq G_j^{C^\#}\,, \end{cases} \\
&\Rightarrow R^{BC} = \sum_{j=1}^{\lceil N/2 \rceil} R_j^{BC'} = \begin{cases} 0\,, & \text{if } Y = Z\,, \\ \text{others}\,, & \text{if } Y \neq Z\,. \end{cases}
\end{aligned} \tag{2}
$$

Therefore, the quality comparison result of Y and Z in the above three-party QPC protocol is correct.

Case 3 The Quality Comparison of Alice and Charlie's Secret Inputs

As for the quality comparison of X and Z, Alice, Bob and Charlie need to calculate $R_j^{AC} = (R_j^A \oplus G_j^{A^\#}) \oplus R_j^B \oplus (R_j^C \oplus G_j^{C^\#}) = (r_j^{AC_1} r_j^{AC_2})$. Moreover, TP needs to calculate $R_j^{AC'} = (r_j^{AC_1} \oplus r_j^{T_1^2}) + (r_j^{AC_2} \oplus r_j^{T_2^2})$ and $R^{AC} = \sum_{j=1}^{\lceil N/2 \rceil} R_j^{AC'}$. According to Fig.1, the following evolution is satisfied:

$$
\begin{aligned}
&\begin{cases} R_{A_1A_2} \oplus R_{T_1T_2} = R_{A_1T_2} \oplus R_{T_1A_2} \\ R_{T_1A_2} \oplus R_{B_1B_2} = R_{T_1B_2} \oplus R_{B_1A_2} \\ R_{T_1B_2} \oplus R_{C_1C_2} = R_{T_1C_2} \oplus R_{C_1B_2} \end{cases} \Rightarrow R_{A_1A_2} \oplus R_{T_1T_2} \\
&= R_{A_1T_2} \oplus (R_{B_1B_2} \oplus (R_{B_1A_2} \oplus (R_{C_1C_2} \oplus R_{T_1C_2} \oplus R_{C_1B_2}))) \\
&\Rightarrow 00 = R_j^A \oplus R_j^B \oplus R_j^C \oplus R_j^{T^2} \\
&\Rightarrow G_j^{A^\#} \oplus G_j^{C^\#} = (R_j^A \oplus G_j^{A^\#}) \oplus R_j^B \oplus (R_j^C \oplus G_j^{C^\#}) \oplus R_j^{T^2} \\
&= R_j^{AC} \oplus R_j^{T^2}
\end{aligned}
$$

$$\Rightarrow R_j^{AC'} = \begin{cases} 0\,, & \text{if } G_j^{A^\#} = G_j^{C^\#}\,, \\ 1 \text{ or } 2\,, & \text{if } G_j^{A^\#} \neq G_j^{C^\#}\,, \end{cases}$$

$$\Rightarrow R^{AC} = \sum_{j=1}^{\lceil N/2 \rceil} R_j^{AC'} = \begin{cases} 0\,, & \text{if } X = Z\,, \\ \text{others}\,, & \text{if } X \neq Z\,. \end{cases} \tag{3}$$

Therefore, the quality comparison result of X and Z in the above three-party QPC protocol is correct.

(ii) *Security*

As far as the security is concerned, all of the outside attack, the participant attack and the information leakage problem should be taken into account.

Case 1 Outside Attack

We analyze the possibility for an outside eavesdropper to get information about X, Y, and Z.

In Step 1(c)/2(a)/3(a), TP and Alice/ Bob/ Charlie exchange two quantum state sequences in their respective hands. However, same to the LWC-QPC protocol, the entanglement correlation between two different particles of each Bell state is used to detect the eavesdropping behavior from an outside attacker. It has been widely accepted that several famous attacks, such as the intercept-resend attack, the measure-resend attack and the entangle-measure attack *et al.*, are invalid to this eavesdropping check method.[38−41] Moreover, except Steps 1(c), 2(a) and 3(a), there is no chance for an eavesdropper to steal as no transmission for quantum states occurs.

In addition, in Steps 2(c) and 3(c), there are classical information transmissions. Suppose that the outside attacker is powerful enough to get all the transmitted classical information. In Step 2(c), the outside attacker obtains the result of $R_j^A \oplus G_j^{A^\#}$ when Alice sends it out to Bob and the result of $R_j^B \oplus G_j^{B^\#}$ when Bob sends R_j^{AB} out to TP. However, as she has no knowledge about the one-time-pad keys R_j^A and R_j^B, she cannot deduce out $G_j^{A^\#}$ and $G_j^{B^\#}$ from $R_j^A \oplus G_j^{A^\#}$ and $R_j^B \oplus G_j^{B^\#}$, respectively. Similarly, in Step 3(c), the outside attacker can get other useful classical information including R_j^A, R_j^B and the result of $R_j^C \oplus G_j^{C^\#}$. Until now, the outside attacker can extract $G_j^{A^\#}$ and $G_j^{B^\#}$ from $R_j^A \oplus G_j^{A^\#}$ and $R_j^B \oplus G_j^{B^\#}$, respectively, since she has known R_j^A and R_j^B. However, the one-way property of the hash function can guarantee that knowing $G_j^{A^\#}$ and $G_j^{B^\#}$ is still helpless to deduce G_j^A and G_j^B, respectively. In this way, the outside attacker still has no access to G_j^A and G_j^B. On the other hand, the outside attacker cannot get $G_j^{C^\#}$ either since she does not know R_j^C. Right now, it can be concluded that an outside eavesdropper cannot get X, Y and Z in the three-party QPC protocol.

Case 2 Participant Attack

Gao *et al.*[42] pointed out for the first time that the attack from dishonest participants, i.e., the participant attack, is generally more powerful and should be paid more attention to. It has greatly aroused the interest of researchers in the cryptanalysis of quantum cryptography. There are two cases of participant attack in the three-party QPC protocol. The first one is the attack from an insider user, while the second one is the attack from TP.

(a) *Inside User's Attack*

Suppose that Alice is a powerful dishonest user who tries her best to get the other users' secret inputs with possible strong means. If Alice tries to intercept the transmitted particles from the TP-Bob channel, the Bob-TP channel, the TP-Charlie channel or the Charlie-TP channel, she will be caught as an outside attacker as analyzed in Case 1. Another way for Alice to get Bob and Charlie's secret inputs is to utilize all the possible classical information in her hands. After the protocol is finished, all the possible classical information Alice has is R_j^A, $G_j^{A^\#}$, R_j^{AB}, $R_j^B \oplus G_j^{B^\#}$, R_j^{BC}, R_j^B, and R_j^{AC}. As a result, Alice can only deduce out $G_j^{B^\#}$ and $R_j^C \oplus G_j^{C^\#}$ from these classical information, but she still cannot know $G_j^{C^\#}$ since she has no knowledge about R_j^C. Moreover, the one-way property of the hash function can make Alice not aware of G_j^B from $G_j^{B^\#}$. Therefore, Alice cannot get Y and Z.

Suppose that Bob is a powerful dishonest user who tries his best to get the other users' secret inputs with possible strong means. If Bob tries to intercept the transmitted particles from the TP-Alice channel, the Alice-TP channel, the TP-Charlie channel or the Charlie-TP channel, he will be caught as an outside attacker as analyzed in Case 1. Another way for Bob to get Alice and Charlie's secret inputs is to utilize all the possible classical information in his hands. After the protocol is finished, all the possible classical information Bob has is R_j^B, $G_j^{B^\#}$, $R_j^A \oplus G_j^{A^\#}$, R_j^{AB}, R_j^A, R_j^{BC} and R_j^{AC}. As a result, Bob can only deduce out $G_j^{A^\#}$ and $R_j^C \oplus G_j^{C^\#}$ from these classical information, but he still cannot know $G_j^{C^\#}$ since he has no knowledge about R_j^C. Moreover, the one-way property of the hash function can make Bob not aware of G_j^A from $G_j^{A^\#}$. Therefore, Bob cannot get X and Z.

Suppose that Charlie is a powerful dishonest user who tries her best to get the other users' secret inputs with possible strong means. If Charlie tries to intercept the transmitted particles from the TP-Alice channel, the Alice-TP channel, the TP-Bob channel or the Bob-TP channel, she will be caught as an outside attacker as analyzed in Case 1. Another way for Charlie to get Alice and Bob's secret

inputs is to utilize all the possible classical information in her hands. After the protocol is finished, all the possible classical information Charlie has is R_j^C, $G_j^{C\#}$, $R_j^A \oplus G_j^{A\#}$, R_j^{AB}, R_j^A, $R_j^B \oplus G_j^{B\#}$, R_j^{BC}, R_j^B and R_j^{AC}. As a result, Charlie can deduce out both $G_j^{A\#}$ and $G_j^{B\#}$ from these classical information. However, according to the one-way property of the hash function, knowing $G_j^{A\#}$ and $G_j^{B\#}$ is still helpless for Charlie to deduce G_j^A and G_j^B, respectively. Therefore, Charlie cannot get X and Y.

(b) *TP's Attack*

TP may try to get Alice, Bob and Charlie's secret inputs with all the possible classical information in her hands. After the protocol is finished, all the possible classical information TP has is $R_j^{T^1}$, $R_j^A \oplus G_j^{A\#}$, R_j^{AB}, $R_j^{AB'}$, R^{AB}, $R_j^{T^2}$, R_j^A, $R_j^B \oplus G_j^{B\#}$, R_j^{BC}, $R_j^{BC'}$, R^{BC}, R_j^B, R_j^{AC}, $R_j^{AC'}$ and R^{AC}. Note that TP need not launch the Bell-basis measurement attack to get R_j^A and R_j^B, as she can get them from the public classical channels. As a result, TP can deduce out all of $G_j^{A\#}$, $G_j^{B\#}$ and $G_j^{C\#}$ from these classical information. However, according to the one-way property of the hash function, knowing $G_j^{A\#}$, $G_j^{B\#}$ and $G_j^{C\#}$ is still helpless for TP to deduce G_j^A, G_j^B and G_j^C, respectively. Therefore, TP cannot get X, Y, and Z accurately.

To sum up, in the three-party QPC protocol, TP can know the comparison result of each two users' secret inputs but cannot know the genuine value of each input. Each user cannot know the genuine values of the other two users' secret inputs.

Case 3 The Information Leakage Problem

According to formulas (1)–(3), the relations between $R_j^{AB'}$ and $G_j^{A\#}$, $G_j^{B\#}$, the relations between $R_j^{BC'}$ and $G_j^{B\#}$, $G_j^{C\#}$, and the relations between $R_j^{AC'}$ and $G_j^{A\#}$, $G_j^{C\#}$, can also be depicted as Table 3, respectively. As analyzed in Subsec. 3.2, the usage of one-way hash function can automatically avoid the information leakage problem pointed out in Subsec. 3.1.

It can be concluded now that the three-party QPC protocol is highly secure.

5 MQPC Protocol Based on Entanglement Swapping of Bell Entangled States

There are K users, P_1, $P_2, \ldots, P_K$, where P_i has a secret integer X^i, $i = 1, 2, \ldots, K$. The binary representation of X^i in F_{2^L} is $(x_{L-1}^i, x_{L-2}^i, \ldots, x_0^i)$. Here, $x_j^i \in \{0, 1\}$, $j = 0, 1, \ldots, L-1$. They want to know whether each two different X^i are equal or not with the help of a semi-honest TP.

They achieve the equality comparison of each two different X^i by implementing the following steps. Same to the above three-party QPC protocol, each transmission of quantum state sequence here is checked with the entanglement correlation between two different particles of a sample Bell state $|\phi^+\rangle$. For simplicity, we omit the description of eavesdropping check processes in the following.

Step 1 Preparation

(a) Similar to the QPC protocols of Refs. [4–5], K users, $P_1, P_2, \ldots, P_K$, share a secret one-way hash function H in advance. The hash value of X^i is $H(X^i) = X^{i\#} = (x_{N-1}^{i\#}, x_{N-2}^{i\#}, \ldots, x_0^{i\#})$, $i = 1, 2, \ldots, K$. P_i divides her binary representation of $X^{i\#}$ into $\lceil N/2 \rceil$ groups $G_1^{P_i^\#}, G_1^{P_i^\#}, \ldots, G_{\lceil L/2 \rceil}^{P_i^\#}$, where each group contains two binary bits. If $N \bmod 2 = 1$, one 0 should be added to $G_{\lceil N/2 \rceil}^{P_i^\#}$ by P_i.

(b) P_i/TP prepares $\lceil N/2 \rceil$ quantum states all in the state of $|\phi^+\rangle_{P_{i_1}P_{i_2}}/|\phi^+\rangle_{T_1T_2}$. Afterward, P_i/TP picks out the first particle from each state to form an ordered sequence $S_1^{P_i}/S_1^T$. The remaining second particle from each state automatically forms the other ordered sequence $S_2^{P_i}/S_2^T$.

(c) P_1 and TP exchange $S_2^{P_1}$ and S_2^T.

(d) For $j = 1, 2, \ldots, \lceil N/2 \rceil$, P_1 performs the Bell-basis measurement on each pair in $(S_1^{P_1}, S_2^T)$ and obtains the corresponding measurement result $M_j^{P_1}$. If $M_j^{P_1}$ is $|\phi^+\rangle/|\phi^-\rangle/|\psi^+\rangle/|\psi^-\rangle$, then $R_j^{P_1} = 00/01/10/11$. Consequently, the corresponding pair in $(S_1^T, S_2^{P_1})$ in TP's hands is collapsed into one of the four Bell states. These $\lceil N/2 \rceil$ collapsed Bell states in TP's hands are denoted by $(S_1^{T^1}, S_2^{T^1})$.

Step k The $k-1^{\text{th}}$ Round Comparison ($k = 2, 3, 4, \ldots, K$)

(a) P_k and TP exchange $S_2^{P_k}$ and $S_2^{T^{k-1}}$.

(b) For $j = 1, 2, \ldots, \lceil N/2 \rceil$, P_k performs the Bell-basis measurement on each pair in $(S_1^{P_k}, S_2^{T^{k-1}})$ and obtains the corresponding measurement result $M_j^{P_k}$. If $M_j^{P_k}$ is $|\phi^+\rangle/|\phi^-\rangle/|\psi^+\rangle/|\psi^-\rangle$, then $R_j^{P_k} = 00/01/10/11$. Consequently, the corresponding pair in $(S_1^{T^{k-1}}, S_2^{P_k})$ in TP's hands is collapsed into one of the four Bell states. TP also performs the Bell-basis measurement on each pair in $(S_1^{T^{k-1}}, S_2^{P_k})$ and obtains the corresponding measurement result $M_j^{T^{k-1}}$. If $M_j^{T^{k-1}}$ is $|\phi^+\rangle/|\phi^-\rangle/|\psi^+\rangle/|\psi^-\rangle$, then $R_j^{T^{k-1}} = (r_j^{T_1^{k-1}} r_j^{T_2^{k-1}}) = 00/01/10/11$.

(c) For $j = 1, 2, \ldots, \lceil N/2 \rceil$, k users cooperate to calculate

$$\begin{aligned} R_j^{P_m P_k} = {} & R_j^{P_1} \oplus R_j^{P_2} \oplus \cdots \oplus R_j^{P_{m-1}} \oplus (R_j^{P_m} \oplus G_j^{P_m^\#}) \\ & \oplus R_j^{P_{m+1}} \oplus R_j^{P_{m+2}} \oplus \cdots \\ & \oplus R_j^{P_{k-1}} \oplus (R_j^{P_k} \oplus G_j^{P_k^\#}) = (r_j^{P_m P_{k_1}} r_j^{P_m P_{k_2}}), \end{aligned}$$

and send $R_j^{P_m P_k}$ to TP. Here, $m = 1, 2, \ldots, k-1$. Without loss of generality, assume that P_i $(i = 1, 2, \ldots, m-1, m+1, \ldots, k-2, k-1)$ and P_m send $R_j^{P_i}$ and the result of $R_j^{P_m} \oplus G_j^{P_m^\#}$ to P_k for calculating $R_j^{P_m P_k}$, respectively.

Then, TP calculates

$$R_j^{P_mP'_k} = \left(r_j^{P_mP_{k_1}} \oplus r_j^{T_1^{k-1}}\right) + \left(r_j^{P_mP_{k_2}} \oplus r_j^{T_2^{k-1}}\right)$$

and $R^{P_mP_k} = \sum_{j=1}^{\lceil N/2\rceil} R_j^{P_mP'_k}$.

TP sends $R^{P_mP_k}$ to P_m and P_k. If $R^{P_mP_k} = 0$, P_m and P_k conclude that $X^m = X^k$; otherwise, they know that $X^m \neq X^k$.

Correctness We continue to demonstrate the output correctness. As for the quality comparison of X^m and X^k ($m = 1, 2, \ldots, k-1$ and $k = 2, 3, 4, \ldots, K$), k users need to calculate $R_j^{P_mP_k} = R_j^{P_1} \oplus R_j^{P_2} \oplus \cdots \oplus R_j^{P_{m-1}} \oplus \left(R_j^{P_m} \oplus G_j^{P_m^{\#}}\right) \oplus R_j^{P_{m+1}} \oplus R_j^{P_{m+2}} \oplus \cdots \oplus R_j^{P_{k-1}} \oplus \left(R_j^{P_k} \oplus G_j^{P_k^{\#}}\right) = \left(r_j^{P_mP_{k_1}} r_j^{P_mP_{k_2}}\right)$. Moreover, TP needs to calculate

$$R_j^{P_mP'_k} = \left(r_j^{P_mP_{k_1}} \oplus r_j^{T_1^{k-1}}\right) + \left(r_j^{P_mP_{k_2}} \oplus r_j^{T_2^{k-1}}\right)$$

and $R^{P_mP_k} = \sum_{j=1}^{\lceil N/2\rceil} R_j^{P_mP'_k}$. According to the entanglement swapping processes of the multi-party QPC protocol, we can obtain

$$\begin{cases} R_{P_{1_1}P_{1_2}} \oplus R_{T_1T_2} = R_{P_{1_1}T_2} \oplus R_{T_1P_{1_2}} \\ R_{T_1P_{1_2}} \oplus R_{P_{2_1}P_{2_2}} = R_{T_1P_{2_2}} \oplus R_{P_{2_1}P_{1_2}} \\ R_{T_1P_{2_2}} \oplus R_{P_{3_1}P_{3_2}} = R_{T_1P_{3_2}} \oplus R_{P_{3_1}P_{2_2}} \\ R_{T_1P_{3_2}} \oplus R_{P_{4_1}P_{4_2}} = R_{T_1P_{4_2}} \oplus R_{P_{4_1}P_{3_2}} \\ \vdots \\ R_{T_1P_{k-1_2}} \oplus R_{P_{k_1}P_{k_2}} = R_{T_1P_{k_2}} \oplus R_{P_{k_1}P_{k-1_2}} \end{cases} \Rightarrow R_{P_{1_1}P_{1_2}} \oplus R_{T_1T_2}$$

$$= R_{P_{1_1}T_2} \oplus (R_{P_{2_1}P_{2_2}} \oplus (R_{P_{2_1}P_{1_2}} \oplus (R_{P_{3_1}P_{3_2}} \oplus (R_{P_{3_1}P_{2_2}} \oplus \cdots \oplus (R_{P_{k_1}P_{k_2}} \oplus R_{P_{k_1}P_{k-1_2}} \oplus R_{T_1P_{k_2}})))))$$

$$\Rightarrow 00 = R_j^{P_1} \oplus R_j^{P_2} \oplus \cdots \oplus R_j^{P_{m-1}} \oplus R_j^{P_m} \oplus R_j^{P_{m+1}} \oplus R_j^{P_{m+2}} \oplus \cdots \oplus R_j^{P_{k-1}} \oplus R_j^{P_k} \oplus R_j^{T^{k-1}}$$

$$\Rightarrow G_j^{P_m^{\#}} \oplus G_j^{P_k^{\#}} = R_j^{P_1} \oplus R_j^{P_2} \oplus \cdots \oplus R_j^{P_{m-1}} \oplus (R_j^{P_m} \oplus G_j^{P_m^{\#}}) \oplus R_j^{P_{m+1}} \oplus R_j^{P_{m+2}}$$

$$\oplus \cdots \oplus R_j^{P_{k-1}} \oplus (R_j^{P_k} \oplus G_j^{P_k^{\#}}) \oplus R_j^{T^{k-1}} = R_j^{P_mP_k} \oplus R_j^{T^{k-1}}$$

$$\Rightarrow R_j^{P_mP'_k} = \begin{cases} 0, & \text{if } G_j^{P_m^{\#}} = G_j^{P_k^{\#}}, \\ 1 \text{ or } 2, & \text{if } G_j^{P_m^{\#}} \neq G_j^{P_k^{\#}}, \end{cases} \Rightarrow R^{P_mP_k} = \sum_{j=1}^{\lceil N/2\rceil} R_j^{P_mP'_k} = \begin{cases} 0, & \text{if } X^m = X^k, \\ \text{others}, & \text{if } X^m \neq X^k. \end{cases} \quad (4)$$

Therefore, the quality comparison result of X^m and X^k in the above K-party QPC protocol is correct.

Security As far as the security of the MQPC protocol is concerned, we can analyze it in a way similar to that of the three-party QPC protocol. It is easy to find out that the MQPC protocol is also immune to all of the outside attack, the participant attack and the information leakage problem.

Comparison with Previous QPC Protocols The comparison of our MQPC protocol with some previous representative QPC protocols, such as Yang *et al.*'s protocol,[4] Chen *et al.*'s protocol,[6] Tseng *et al.*'s protocol,[7] Liu *et al.*'s protocol,[8] Yang *et al.*'s protocol[17] and Chang *et al.*'s protocol,[35] is described in Table 4. According to Table 4, it is easy to know that each of the protocols in Refs. [4, 6–8, 17, 35] has advantages and disadvantages more or less. For example, our protocol adopts Bell state as quantum resource. As for quantum state used, our protocol takes advantage over the protocols of Refs. [6, 35] but is defeated by the protocol of Ref. [17], since the preparation of Bell state is easier than that of GHZ state and is more difficult than that of single photon product state. However, it can be concluded that our protocol exceeds the protocols of Refs. [4, 6–8, 17] in number of times of protocol execution when they are used to achieve the equality comparison among K users, because in our protocol, arbitrary pair's comparison of equality among K users can be accomplished within one execution.

It should be further emphasized that different quantum methods have been used to achieve the equality comparison in present MQPC protocols[35–37] and our MQPC protocol. Concretely speaking, Chang *et al.*'s protocol[35] uses the entanglement correlation between two different particles of one n-particle GHZ class state; both Liu *et al.*'s protocol[36] and Wang *et al.*'s protocol[37] use quantum fourier transform. However, our protocol uses quantum entanglement swapping.

6 Conclusion

In this paper, we first point out the information leakage problem toward TP in the LLCLL-improved-QPC protocol, and then mend this loophole by utilizing the one-way hash function to encrypt the two users' secret inputs. Afterward, the three-party QPC protocol also based on entanglement swapping of Bell entangled state is constructed. Its output correctness and its security against the outside attack, the inside participant attack and the information leakage problem are validated in detail. Finally, the MQPC protocol also based on entanglement swapping of Bell entangled state is designed, where arbitrary pair's comparison of equality among K users can be accomplished within one execution.

Appendix

Table 1 The relations among different parameters when $G_j^A = 00$.

G_j^A	G_j^B	M_j^A	M_j^B	R_j^A	R_j^B	$R_j(r_j^1 r_j^2)$	M_j^T	$R_j^T(r_j^{T_1} r_j^{T_2})$	R'_j
		$\|\phi^+\rangle$	$\|\phi^+\rangle$	00	00	00/01/10/11	$\|\phi^+\rangle$	00	0/1/1/2
		$\|\phi^+\rangle$	$\|\phi^-\rangle$	00	01	01/00/11/10	$\|\phi^-\rangle$	01	0/1/1/2
		$\|\phi^+\rangle$	$\|\psi^+\rangle$	00	10	10/11/00/01	$\|\psi^+\rangle$	10	0/1/1/2
		$\|\phi^+\rangle$	$\|\psi^-\rangle$	00	11	11/10/01/00	$\|\psi^-\rangle$	11	0/1/1/2
		$\|\phi^-\rangle$	$\|\phi^-\rangle$	01	01	00/01/10/11	$\|\phi^+\rangle$	00	0/1/1/2
		$\|\phi^-\rangle$	$\|\phi^+\rangle$	01	00	01/00/11/10	$\|\phi^-\rangle$	01	0/1/1/2
00	00/01/10/11	$\|\phi^-\rangle$	$\|\psi^-\rangle$	01	11	10/11/00/01	$\|\psi^+\rangle$	10	0/1/1/2
		$\|\phi^-\rangle$	$\|\psi^+\rangle$	01	10	11/10/01/00	$\|\psi^-\rangle$	11	0/1/1/2
		$\|\psi^+\rangle$	$\|\psi^+\rangle$	10	10	00/01/10/11	$\|\phi^+\rangle$	00	0/1/1/2
		$\|\psi^+\rangle$	$\|\psi^-\rangle$	10	11	01/00/11/10	$\|\phi^-\rangle$	01	0/1/1/2
		$\|\psi^+\rangle$	$\|\phi^+\rangle$	10	00	10/11/00/01	$\|\psi^+\rangle$	10	0/1/1/2
		$\|\psi^+\rangle$	$\|\phi^-\rangle$	10	01	11/10/01/00	$\|\psi^-\rangle$	11	0/1/1/2
		$\|\psi^-\rangle$	$\|\phi^+\rangle$	11	00	11/10/01/00	$\|\psi^-\rangle$	11	0/1/1/2
		$\|\psi^-\rangle$	$\|\psi^+\rangle$	11	10	01/00/11/10	$\|\phi^-\rangle$	01	0/1/1/2
		$\|\psi^-\rangle$	$\|\phi^-\rangle$	11	01	10/11/00/01	$\|\psi^+\rangle$	10	0/1/1/2
		$\|\psi^-\rangle$	$\|\psi^-\rangle$	11	11	00/01/10/11	$\|\phi^+\rangle$	00	0/1/1/2

Table 2 The relations between R'_j and G_j^A, G_j^B.

R'_j	G_j^A	G_j^B
0	00/01/10/11	00/01/10/11
1	00/01/10/11	01/00/11/10 10/11/00/01
2	00/01/10/11	11/10/01/00

Table 3 The relations between R'_j and $G_j^{A^\#}$, $G_j^{B^\#}$.

R'_j	$G_j^{A^\#}$	$G_j^{B^\#}$
0	00/01/10/11	00/01/10/11
1	00/01/10/11	01/00/11/10 10/11/00/01
2	00/01/10/11	11/10/01/00

Table 4 The comparison of our MQPC protocol with previous QPC protocols.

	Yang *et al.*'s protocol[4]	Chen *et al.*'s protocol[6]	Tseng *et al.*'s protocol[7]	Liu *et al.*'s protocol[8]	Yang *et al.*'s protocol[17]	Chang *et al.*'s protocol[35]	Our protocol
Quantum state	Bell state	Triple GHZ state	Bell state	Bell state	Single-photon product state	n-particle GHZ class state	Bell state
Quantum measurement for TP	Bell-basis measurement	Single-photon measurement	No	Bell-basis measurement	No	No	Bell-basis measurement
Quantum measurement for users	No	Single-photon measurement	Single-photon measurement	Bell-basis measurement	Single-photon measurement	Single-photon measurement	Bell-basis measurement
Unitary operation for TP	No	Yes	No	No	No	No	No

Table 4 (continued)

	Yang *et al.*'s protocol[4]	Chen *et al.*'s protocol[6]	Tseng *et al.*'s protocol[7]	Liu *et al.*'s protocol[8]	Yang *et al.*'s protocol[17]	Chang *et al.*'s protocol[35]	Our protocol
Unitary operation for users	Yes	No	No	No	No	No	No
Quantum memory for TP	No	Yes	No	Yes	No	No	Yes
Number of times of protocol execution	$(K-1) \sim K(K-1)/2$	$(K-1) \sim K(K-1)/2$	$(K-1) \sim K(K-1)/2$	$(K-1) \sim K(K-1)/2$	$(K-1) \sim K(K-1)/2$	1	1

Acknowledgments

The author would like to thank the anonymous reviewer for his valuable suggestion that helps enhancing the quality of this paper.

References

[1] A.C. Yao, In *Proceedings of the 23rd Annual IEEE Symposium on Foundations of Computer Science, IEEE Computer Society*, Washington (1982) 160.
[2] F. Boudot, B. Schoenmakers, and J. Traore, Discret Appl. Math. **111** (2001) 23.
[3] H.K. Lo, Phys. Rev. A **56** (1997) 1154.
[4] Y.G. Yang and Q.Y. Wen, J. Phys. A: Math. Theor. **42** (2009) 055305; Y.G. Yang and Q.Y. Wen, J. Phys. A: Math. Theor. **43** (2010) 209801.
[5] Y.G. Yang, J.W. Tian, Y. Hong, and H. Zhang, Phys. Scr. **80** (2009) 065002; Y.G. Yang, W.F. Cao, and Q.Y. Wen, Phys. Scr. **80** (2009) 065002.
[6] X.B. Chen, G. Xu, X.X. Niu, Q.Y. Wen, and Y.X. Yang, Opt. Commun. **283** (2010) 1561.
[7] H.Y. Tseng, J. Lin, and T. Hwang, Quantum Inf. Process. **11** (2012) 373.
[8] W. Liu, Y.B. Wang, and W. Cui, Commun. Theor. Phys. **57** (2012) 583.
[9] W.J. Liu, C. Liu, H.W. Chen, Z.Q. Li, and Z.H. Liu, Commun. Theor. Phys. **62** (2014) 210.
[10] J. Lin, H.Y. Tseng, and T. Hwang, Opt. Commun. **284** (2011) 2412.
[11] C. Wang, G. Xu, and Y.X. Yang, Int. J. Quantum Inf. **11** (2013) 1350039.
[12] Y.G. Yang, J. Xia, X. Jia, and H. Zhang, Quantum Inf. Process. **12** (2013) 877.
[13] W.W. Zhang and K.J. Zhang, Quantum Inf. Process. **12** (2013) 1981.
[14] W. Liu, Y.B. Wang, and Z.T. Jiang, Opt. Commun. **284** (2011) 3160.
[15] Y.B. Li, Q.Y. Wen, F. Gao, H.Y. Jia, and Y. Sun, Eur. Phys. J. D **66** (2012) 110.
[16] W. Liu and Y.B. Wang, Int. J. Theor. Phys. **51** (2012) 3596.
[17] Y.G. Yang, J. Xia, X. Jia, L. Shi, and H. Zhang, Int. J. Quantum Inf. **10** (2012) 1250065.
[18] W. Liu, Y.B. Wang, and Z.T. Jiang, Int. J. Theor. Phys. **51** (2012) 69.
[19] W. Liu, Y.B. Wang, Z.T. Jiang, Y.Z. Cao, and W. Cui, Int. J. Theor. Phys. **51** (2012) 1953.
[20] H.Y. Jia, Q.Y. Wen, Y.B. Li, and F. Gao, Int. J. Theor. Phys. **51** (2012) 1187.
[21] G.A. Xu, X.B. Chen, Z.H. Wei, M.J. Li, and Y.X. Yang, Int. J. Quantum Inf. **10** (2012) 1250045.
[22] S. Lin, C.D. Guo, and X.F. Liu, Int. J. Theor. Phys. **52** (2013) 4185.
[23] Z.W. Sun and D.Y. Long, Int. J. Theor. Phys. **52** (2013) 212.
[24] W. Zi, F.Z. Guo, Y. Luo, S.H. Cao, and Q.Y. Wen, Int. J. Theor. Phys. **52** (2013) 3212.
[25] B. Liu, F. Gao, H.Y. Jia, W. Huang, W.W. Zhang, and Q.Y. Wen, Quantum Inf. Process. **12** (2013) 887.
[26] J. Lin, C.W. Yang, and T. Hwang, Quantum Inf. Process. **13** (2014) 239.
[27] Y.T. Chen and T. Hwang, Int. J. Theor. Phys. **53** (2014) 837.
[28] J. Li, H.F. Zhou, L. Jia, and T.T. Zhang, Int. J. Theor. Phys. **53** (2014) 2167.
[29] Y. Li, Y. Ma, S. Xu, W. Huang, and Y. Zhang, Int. J. Theor. Phys. **53** (2014) 3191.
[30] W.J. Liu, C. Liu, H.W. Chen, Z.H. Liu, M.X. Yuan, and J.S. Lu, Int. J. Quantum Inf. **12** (2014) 1450001.
[31] W.J. Liu, C. Liu, H.B. Wang, J.F. Liu, F. Wang, and X.M. Yuan, Int. J. Theor. Phys. **53** (2014) 1804.
[32] W.W. Zhang, D. Li, and Y.B. Li, Int. J. Theor. Phys. **53** (2014) 1723.
[33] Z.W. Sun, J.P. Yu, P. Wang, L.L. Xu, and C.H. Wu, Quantum Inf. Process. **14** (2015) 2125.
[34] G.P. He, Quantum Inf. Process. **14** (2015) 2301.
[35] Y.J. Chang, C.W. Tsai, and T. Hwang, Quantum Inf. Process. **12** (2013) 1077.
[36] W. Liu, Y.B. Wang, and X.M. Wang, Int. J. Theor. Phys. **53** (2014) 1085.
[37] Q.L. Wang, H.X. Sun, and W. Huang, Quantum Inf. Process. **13** (2014) 2375.
[38] G.F. Shi, X.Q. Xi, X.L. Tian, and R.H. Yue, Opt. Commun. **282** (2009) 2460.
[39] G.F. Shi, Opt. Commun. **283** (2010) 5275.
[40] G. Gao, Opt. Commun. **283** (2010) 2288.
[41] T.Y. Ye and L.Z. Jiang, Chin. Phys. Lett. **30** (2013) 040305.
[42] F. Gao, S.J. Qin, Q.Y. Wen, and F.C. Zhu, Quantum Inf. Comput. **7** (2007) 329.