Quantum Inf Process (2014) 13:2375–2389
DOI 10.1007/s11128-014-0774-2

Multi-party quantum private comparison protocol with *n*-level entangled states

Qing-Le Wang · Hong-Xiang Sun · Wei Huang

Received: 29 July 2013 / Accepted: 7 June 2014 / Published online: 19 June 2014

Abstract In this paper, two multi-party quantum private comparison (MQPC) protocols are proposed in distributed mode and traveling mode, respectively. Compared with the first MQPC protocol, which pays attention to compare between arbitrary two participants, our protocols focus on the comparison of equality for n participants with a more reasonable assumption of the third party. Through executing our protocols once, it is easy to get if n participants' secrets are same or not. In addition, our protocols are proved to be secure against the attacks from both outside attackers and dishonest participants.

Keywords Quantum secure multi-party computation · Quantum private comparison · Security

1 Introduction

Quantum cryptography has attracted widespread attention since Bennett and Brassard [1] presented the first quantum cryptographic protocol in 1984. Until now, kinds of quantum cryptographic protocols have been proposed, such as quantum key distribution (QKD) [1,2,35–38], quantum secure direct communication (QSDC) [3–6], quantum teleportation (QT) [7,8], and so on.

Secure multi-party computing (SMC, also called secure function evaluation.), which plays an important role in classical cryptography, is existing in the field of quantum cryptography. Considering from a macro point of view, SMC can be described

Q.-L. Wang (✉) · W. Huang
State Key Laboratory of Networking and Switching Technology,
Beijing University of Posts and Telecommunications, Beijing 100876, China
e-mail: wqle519@gmail.com

Q.-L. Wang · H.-X. Sun
School of Science, Beijing University of Posts and Telecommunications, Beijing 100876, China

as follows. Based on the private input x_i of each participant P_i ($i \in \{1, 2, \ldots, n\}$), the n mutually distrustful participants could compute the value y of a given function $f(x_1, x_2, \ldots, x_n)$. More specially, P_i cannot gain more information about other inputs than y. Recently, greater attention has been paid to the applications of quantum mechanics to solve SMC problems. And some SMC protocols for particular problems have been proposed, for instance, quantum voting and surveying [9,10], quantum auction [11,12], quantum multi-party summation [13], and so on.

As the origin of SMC, the famous millionaires' problem [14] was proposed by Yao in 1982. The problem is how to accurately determine who is the richer between two millionaires without unduly disclosing to others about their fortunes. Private comparison protocol comes to solve this problem. Soon afterward, Boudot [15] proposed another private comparison protocol to determine whether two millionaires are equally rich. Till now, private comparison protocols, especially private comparison of equality protocols, have been deeply studied not only in the field of classical cryptography but also in quantum cryptography. As opposed to classical private comparison (CPC) protocols, the security of quantum private comparison (QPC) protocols does not rely on the assumption of computational complexity, which may be susceptible to the strong ability of quantum computation, but simply on the principles of quantum mechanics, such as quantum no-cloning theorem and Heisenberg uncertainty principle. Hence, QPC protocols draw more worldwide attention. In 2009, Yang et al. [16] presented the first QPC protocol. Since then, many researchers are committed to design secure QPC protocols with different states and methods. Consequently, various QPC protocols [17–26] have been proposed. Until now, it is worth concerning that there is only one MQPC protocol [22]. It can achieve arbitrary pair's comparison of equality among n participants with one execution. Comparing with the previous QPC protocols, if n participants want to perform this comparison of equality, the times for executing protocols is at least $n - 1$. So the first MQPC protocol provides higher efficiency than existing QPC protocols. In the past period of time, we devote ourselves to researching MQPC protocols and put forward comparison of equality for n participants. Concretely, suppose there are n legal participants and each of them has a secret, respectively, and they want to determine whether all of them own the same secrets without disclosing their own secrets. Then, we propose two MQPC protocols, which can judge whether all n participants' secrets are same or not with one execution. Since there is no information about comparison results of arbitrary pairs leaked, our protocols are much better than the pioneering MQPC protocol to achieve comparison for n participants. In addition, comparing with the pioneering MQPC protocol, our protocols are proposed with a more reasonable assumption of TP.

The rest of paper is organized as follows. Section 2 discusses the properties of MQPC protocols and quantum resources used in our protocols. Section 3 makes a detailed description on our MQPC protocols in two modes, and then, the security is analyzed in Sect. 4 and 5. Finally, a short conclusion is given in Sect. 6.

2 Fundamental of quantum private comparison protocols

In light of the foregoing QPC protocols, we desire the MQPC protocols to satisfy the following general theoretical rules.

(R1) The secret of each participant should be kept from others, even after the end of protocol.
(R2) All participants can get the comparison result at the same time.
(R3) The comparison result should be correct, and all malicious behaviors during the process can be discovered.

Now, a detailed discussing of TP is presented here. The unconditional security of QKD protocols greatly encourage researchers to solve other problems with quantum methods. However, the theoretical and practical achievements of QPC protocols are not as significant as QKD protocols. In 1990s Mayers [27] and Lo [28] pointed out independently that it is impossible to construct a secure two-party scheme with equality function because of the unreliable quantum bit commitment schemes. Subsequently, some additional assumptions (e.g., bounded quantum storage [29]) or conditions (e.g., a TP [16]) are introduced to solve this problem. MQPC protocols are proposed in the environment of participants are mutual distrustful. Considering an extreme situation that $n-1$ dishonest participants collude together to get the secret of the rest participant, which the MQPC protocols can be regarded as a QPC protocols. Hence, secure MQPC protocols are impossible. Based on the solutions of the secure QPC protocols, here we adopt the method of adding a TP to design secure MQPC protocols.

According to the reliability of TP, there are three kinds of TP in MQPC protocols.

(k1) TP is completely honest, which is the most ideal situation. Every participant only need to send his (her) encrypted secret to TP, and then, TP compares and announces the result. However, it is so difficult to find this kind of honest TP in actuality.
(k2) TP is dishonest, which is distrusted by every participant. It also can make MQPC protocol equivalent to a QPC protocol sometimes. So this kind of assumption is irrational.
(k3) TP is semi-honest, which has two kinds of assumptions. The first one is that TP executes the protocol loyally, records all the results of its intermediate computations, and cannot conspire with other participants. Since TP might want to steal participants' secrets, this kind of TP is shown to be unreasonable in the actual situation [21,23]. In fact, the first MQPC protocol is proposed with this assumption. The second one is that TP is allowed to misbehave on its own and also cannot conspire with others. Without difficulty, this assumption of TP is more reasonable in MQPC protocols. As we know, it is the best assumption of TP until now.

Next we introduce the quantum resources used in our protocol. For the n-level quantum states $|k\rangle$ ($k \in \{0, 1, \ldots, n-1\}$), the nth order discrete fourier transform is defined to be

$$F\,|k\rangle = \frac{1}{\sqrt{n}} \sum_{r=0}^{n-1} \exp\left(\frac{2\pi i k r}{n}\right) |r\rangle\,.$$

$V_1 = \{|k\rangle\}_{k=0}^{n-1}$, $V_2 = \{|l_k\rangle\}_{k=0}^{n-1} = \{F|k\rangle\}_{k=0}^{n-1} = \left\{\frac{1}{\sqrt{n}} \sum_{r=0}^{n-1} \exp(i\theta r k)\,|r\rangle\right\}_{k=0}^{n-1}$ ($\theta = \frac{2\pi}{n}$) are two common non-orthogonal bases.

The carrier states are

$$|\phi\rangle = \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} |k\rangle^{\otimes n} \tag{1}$$

$$|\varphi\rangle = \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} |k\rangle|k\rangle. \tag{2}$$

After performing $F \otimes F \otimes \cdots \otimes F$ on $|\phi\rangle$ and $F \otimes F$ on $|\varphi\rangle$, the states turn to be

$$\begin{aligned}
\left|\phi'\right\rangle &= F \otimes F \otimes \cdots \otimes F|\phi\rangle \\
&= \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} F|k\rangle \otimes F|k\rangle \otimes \cdots \otimes F|k\rangle \\
&= \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} \left(\frac{1}{\sqrt{n}} \sum_{r_1=0}^{n-1} \exp(i\theta k r_1)\, |r_1\rangle \right) \\
&\quad \otimes \left(\frac{1}{\sqrt{n}} \sum_{r_2=0}^{n-1} \exp(i\theta k r_2)\, |r_2\rangle \right) \\
&\quad \otimes \cdots \otimes \left(\frac{1}{\sqrt{n}} \sum_{r_n=0}^{n-1} \exp(i\theta k r_n)\, |r_n\rangle \right) \\
&= \frac{1}{n^{\frac{n+1}{2}}} \sum_{r_1+r_2+\cdots+r_n=0(\mathrm{mod}\, n)} |r_1\rangle \otimes |r_2\rangle \otimes \cdots \otimes |r_n\rangle
\end{aligned} \tag{3}$$

$$\begin{aligned}
\left|\varphi'\right\rangle &= F \otimes F|\varphi\rangle \\
&= \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} F|k\rangle \otimes F|k\rangle \\
&= \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} \left(\frac{1}{\sqrt{n}} \sum_{r_1=0}^{n-1} \exp(i\theta k r_1)\, |r_1\rangle \right) \otimes \left(\frac{1}{\sqrt{n}} \sum_{r_2=0}^{n-1} \exp(i\theta k r_2)\, |r_2\rangle \right) \\
&= \frac{1}{n^{\frac{3}{2}}} \sum_{r_1+r_2=0(\mathrm{mod}\, n)} |r_1\rangle \otimes |r_2\rangle.
\end{aligned} \tag{4}$$

The phase shifting operation U_x is

$$U_x = \sum_{k=0}^{n-1} \exp(i\theta k \cdot x)\, |k\rangle\, \langle k|,$$

where x is an integer.

By applying U_x on $|\varphi\rangle$, the state becomes

$$\left|\varphi^{''}\right\rangle = \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} \exp(i\theta kx) \, |k\rangle \, |k\rangle.$$

And with the following operator $\hat{T} = \sum_{t=0}^{n-1} t \, |T_t\rangle \langle T_t|$, where $|T_t\rangle = \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} \exp(i\theta k \cdot t) \, |k\rangle \, |k\rangle$ and $\langle T_s| \, T_t\rangle = \delta_{st}$, we can get $\left\langle \varphi^{''} \left| \hat{T} \right| \varphi^{''} \right\rangle = x \, (\mathrm{mod}\, n)$.

3 The MQPC protocols

Inspired by the works of [9,10], we propose two MQPC protocols in distributed mode and traveling mode, respectively. Here we consider the scenario within a TP, which adopts the second kind assumption of semi-honest. And n legal participants P_i $(1 \leq i \leq n)$, who has a secret x_i. The binary representation of x_i is $\left(x_i^1, x_i^2, \ldots, x_i^m\right)$.

3.1 The proposed MQPC scheme in distributed mode

(1) TP prepares an ordered sequence of $m + n\delta$ states $|\phi^{'}\rangle_1, |\phi^{'}\rangle_2, \ldots, |\phi^{'}\rangle_{m+n\delta}$, and nm states $|\varphi^{'}\rangle_1, |\varphi^{'}\rangle_2, \ldots, |\varphi^{'}\rangle_{nm}$. TP takes the ith $(1 \leq i \leq n)$ particle from each $|\phi^{'}\rangle$ to construct the sequence S_i. For each S_i, TP picks out m states $\left|\varphi^{'}\right\rangle$ and inserts the second particles of them randomly into it. To make sure quantum channel is secure between TP and P_i, TP inserts decoy states into S_i at random positions, and each decoy state is one of the states randomly chosen in the set V_1 or V_2. Then, S_i turns to $S_i^{'}$, and TP sends $S_i^{'}$ to P_i.

(2) After receiving $S_i^{'}$, P_i checks whether the quantum channel is secure. Concretely, TP announces the positions and measurement bases of the decoy states in $S_i^{'}$. Then, P_i uses the bases as TP announced to measure the corresponding decoy states and publishes their measurement results. As TP knows the states before measured, he (she) can find whether an eavesdropper exists in communication. If there is no error, TP confirms that the channel is secure and proceeds to the next step. Otherwise, they abort these sequences and restart a protocol.

(3) For resisting TP's malicious behavior, all participants cooperate together to execute the second eavesdropping check process. TP publicly announces the positions of the states $|\varphi^{'}\rangle$ in each sequence. Then, P_i randomly selects δ states $|\phi^{'}\rangle$ from $S_i^{'}$ as detection states and publishes their positions. For each of the chosen states, P_i randomly selects a measurement basis and announces it. All n participants use the announced bases to measure the corresponding particles and publish their measurement results at the order specified by P_i. According to Eq. (3), if the selected measurement bases are V_1, the addition of their measurement results is zero when dividing by n; If the selected measurement bases are V_2, their measurement results are same. Once there is any error, they discard these states and restart a protocol. Otherwise, they assure TP is honest and continue to the next step.

(4) P_i randomly selects the measurement bases of $|\varphi^{'}\rangle$ in $S_i^{'}$ and informs them to TP through the authenticated classical channel. Then, TP and P_i can share a key sequence y_i of length m through their measurement results t_{Ti} and t_i. If the chosen measurement bases are V_1, then $y_i^j = (n - t_{Ti}^j) \bmod n$, $y_i^j = t_i^j$ $(1 \le j \le m)$; if the chosen measurement bases are V_2, then $y_i^j = t_{Ti}^j = t_i^j$.

(5) P_i measures the rest particles of $|\phi^{'}\rangle$ in $S_i^{'}$ with V_1-basis. Then, P_i constructs a m length sequence with the measurement results r_i^j $(1 \le j \le m)$.

(6) For private comparing, P_i needs to encode his (her) secret $x_i = \left(x_i^1, x_i^2, \ldots, x_i^m\right)$. P_i first calculates

$$c_i^j = \left(x_i^j + y_i^j + r_i^j\right) \bmod n.$$

And then, he (she) sends c_i^j to TP through the authenticated classical channel.

(6) After receiving all c_i^j $(1 \le i \le n, 1 \le j \le m)$, TP computes

$$D_j = \left\{\sum_{i=1}^{n} c_i^j + \sum_{i=1}^{n} (n - y_i^j)\right\} \bmod n.$$

If there exists $D_j \neq 0$, TP can declare that the secrets of all participants are not same and publicly announces "1"; otherwise, the secrets of all participants are same and TP publicly announces "0".

3.2 The proposed MQPC scheme in traveling mode

(1) TP and P_i $(1 \le i \le n)$ share a key sequence k_i of length m, $k_i = \left(k_i^1, k_i^2, \ldots, k_i^m\right)$ $(k_i^j \in \{0, 1, \ldots, n-1\}, j \in \{1, \ldots, m\})$ through a secure QKD protocol.

(2) TP prepares an ordered sequence of $m + \delta$ states $|\varphi\rangle_1, |\varphi\rangle_2, \ldots, |\varphi\rangle_{m+\delta}$. And he (she) picks out the first particle from each $|\varphi\rangle$ to form the home sequence S_1, while the second particle to form the traveling sequence S_2. In order to send S_2 to P_1 securely, TP inserts decoy states into S_2 at random positions, and each decoy state is randomly selected in the set V_1 or V_2. Then, S_2 becomes S_2^1, and TP sends S_2^1 to P_1.

(3) After P_1 receives S_2^1, TP publishes the positions and measurement bases of the decoy states in it. P_1 measures the decoy states with the corresponding bases and informs the measurement results to TP. As TP knows the states before measured, he (she) can find whether an eavesdropper exists in communication. If there is any error, they abort these states and restart a protocol from step (2). Otherwise, TP confirms that the transmission of S_2^1 is secure, and they continue to the following steps.

(4) P_1 randomly chooses δ state $|\varphi\rangle$ as detection state to check the integrity of TP. For each of the chosen states, P_1 randomly chooses a basis between V_1 and V_2. After that, P_1 announces the positions and measurement bases of them. Then, TP and P_1 use these measurement bases to measure the corresponding states. TP first

announces his (her) measurement results and P_1 follows. According to Eq. (2), if the measurement bases is V_1,then their measurement results are same. According to Eq. (4), if their measurement bases is V_2, then their measurement results are opposite (The relationship between the measurement results of two particles in $|\varphi\rangle$ measured with fourier basis (V_2) is equivalent to measure them with computing basis (V_1) after performing discrete fourier transforms.). If there is any error, they discard these states and restart a protocol from step (2). Otherwise, they assure that TP is honest and continue the protocol.

(5) For private comparing, P_i needs to encode his (her) secret on the corresponding states. The particular progress is described as follows.

(5.1) P_1 first calculates $c_1^j = \left(x_1^j + k_1^j\right) \bmod n$ and applies the following operation $U_{c_1^j} = \sum_{k=0}^{n-1} \exp\left(\mathrm{i}\theta k \cdot c_1^j\right) |k\rangle \langle k|$ on the jth particle in his (her) hands. After P_1 finishes his (her) encoding operation, the jth state turns to

$$\left|\varphi_j^1\right\rangle = \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} \exp\left(\mathrm{i}\theta k \cdot c_1^j\right) |k\rangle\, |k\rangle$$

In order to guarantee the security of transmission between P_1 and P_2, P_1 disrupts the order of encoding particles and inserts decoy states randomly in them, which is randomly chosen in the set V_1 or V_2. The new sequence is denoted as S_2^2. Then, P_1 sends S_2^2 to P_2.

(5.2) After P_2 receives S_2^2, P_1 declares the positions and measurement bases of the decoy states. Then, P_2 measures them with the corresponding bases and publishes these measurement results. As P_1 knows the states before measured, he (she) can find whether an eavesdropper exists in transmission. If there is any error, they abort these states and restart a protocol. Otherwise, P_1 confirms that the quantum channel is secure and continues the following steps.

(5.3) P_1 announces the right order of the disrupted encoding particles and P_2 restores the right order of them. Then P_2 executes the encoding and transmitting procedure as P_1 does in step (5.1). That is, P_2 calculates $c_2^j = \left(x_2^j + k_2^j\right) \bmod n$ and applies the operation $U_{c_2^j} = \sum_{k=0}^{n-1} \exp\left(\mathrm{i}\theta k \cdot c_2^j\right) |k\rangle \langle k|$ on the jth particle in his (her) hands. Afterward, P_2 disrupts the order of these encoding particles and sends them with some decoy states to P_3.

(6) The rest of participants utilize the same method to encode secrets and transmit particles one by one until TP receives the sequence. TP and P_n first use the decoy states to check the security of quantum channel. If the quantum channel is secure, then P_n announces the right order of the disrupted encoding particles and TP restores the right order of them. The jth state turns to

$$\left|\varphi_j^n\right\rangle = \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} \exp\left(i\theta k \left(c_1^j + \cdots + c_n^j\right)\right) |k\rangle\, |k\rangle.$$

Otherwise, if the quantum channel is unsafe, they abort the protocol and restart a protocol.

(7) For the sake of getting comparison result, TP takes the collective measurement on $\left|\varphi_j^n\right\rangle$ with the operator

$$\hat{T} = \sum_{t=0}^{n-1} t \left|T_t\right\rangle \left\langle T_t\right|.$$

And the measurement yields the result

$$D_j = \left\langle \varphi_j^n \right| \hat{T} \left| \varphi_j^n \right\rangle = \left(c_1^j + \cdots + c_n^j\right) \bmod n.$$

Then, TP calculates

$$D_j^{'} = \left\{ D_j + \sum_{i=1}^{n} (n - k_i^j) \right\} \bmod n.$$

If all $D_j^{'} = 0$, then TP can declare that the secrets of all participants are same and publicly announces "0"; otherwise, the secrets of all participants are not same and TP publicly announces "1".

4 Security analysis of the proposed protocols

Now, we discuss the security and correctness of the above proposed protocols in this section. We first analyze the security, when $P_1, P_2, \ldots, P_n$ are honest or honest, but curious. Then, we present the correctness.

In distributed model, the reduced density matrix of each particle in all participants' ($P_1, P_2, \ldots, P_n$, TP) hands is $\rho = \left(\frac{1}{n}\right) I$, where I is the identity matrix. It indicates that it is impossible for P_i to get other secrets and TP to get any secret by examining particles in his (her) own hands. Even if they get the correct comparison result after the execution of protocol, they still have no idea.

In addition,

$$\begin{aligned} D_j &= \left\{ \sum_{i=1}^{n} c_i^j + \sum_{i=1}^{n} (n - y_i^j) \right\} \bmod n \\ &= \left\{ \sum_{i=1}^{n} (x_i^j + y_i^j + r_i^j) + \sum_{i=1}^{n} (n - y_i^j) \right\} \bmod n \\ &= \sum_{i=1}^{n} \left(x_i^j + r_i^j + y_i^j + n - y_i^j \right) \bmod n \\ &= \left(r_1^j + \cdots + r_n^j + \sum_{i=1}^{n} x_i^j \right) \bmod n. \end{aligned}$$

Since $(r_1^j + \cdots + r_n^j) \bmod n = 0$, then $D_j = (\sum_{i=1}^n x_i^j) \bmod n$. If and only if $x_1^j = \cdots = x_n^j$, then $D_j = 0$; Otherwise, $D_j \neq 0$. So if $D_1 = \cdots = D_m = 0$, then $x_1 = \cdots = x_n$; Otherwise, there is any $D_j \neq 0$, then the secrets of n participants are not same.

In traveling model, during the entire time of the second particle of each $|\varphi\rangle$ traveling among participants, the reduced density matrix of each second particle in participants' hands and the corresponding first particle in TP's hands are always $\rho = \left(\frac{1}{n}\right) I$. It indicates that, during the protocol process, P_i cannot get other secrets, and TP cannot get any secret.

In addition,

$$\begin{aligned} D_j^{'} &= \left\{ D_j + \sum_{i=1}^{n} (n - k_i^j) \right\} \bmod n \\ &= \left\{ \sum_{i=1}^{n} c_i^j + \sum_{i=1}^{n} \left(n - k_i^j \right) \right\} \bmod n \\ &= \left\{ \sum_{i=1}^{n} \left(x_i^j + k_i^j \right) + \sum_{i=1}^{n} \left(n - k_i^j \right) \right\} \bmod n \\ &= \left(\sum_{i=1}^{n} x_i \right) \bmod n. \end{aligned}$$

If and only if $x_1^j = \cdots = x_n^j$, then $D_j^{'} = 0$; Otherwise, $D_j^{'} \neq 0$. So if $D_1^{'} = \cdots = D_m^{'} = 0$, then $x_1 = \cdots = x_n$. Otherwise, there is any $D_j^{'} \neq 0$, the secrets of n participants are not same.

From the above discussing, we show our protocols are secure for honest or honest, but curious participants. And the correctness of our protocols is also presented. However, driven by curiosity or interest, there might be dishonest participants or eavesdroppers to threaten the security of our protocols in reality. In the following, we will focus on analyzing that our protocols are still secure in this situation.

4.1 Outside attacks

In distributed model, the only opportunity for an outside eavesdropper to steal secrets is in the stage of distributing states (step (1)). Since each particle is in the maximally mixed state $\rho = \left(\frac{1}{n}\right) I$, an outside eavesdropper cannot distinguish between decoy particles and carrier particles. Therefore, several kinds of eavesdroppers' attacks, such as the intercept-resend attack, the measurement-resend attack, and the denial-of-service attack will be discovered with nonzero probability in the eavesdropping detection stage. For example, in the intercept-resend attack, the eavesdropping on each decoy particle by an outside eavesdropper will introduce a probability of $\frac{n-1}{2n}$ to be detected. For the length of d decoy particles, the detection rate is $1 - \left(\frac{n+1}{2n}\right)^d$, which reach to 1 when d is large enough. Actually, any effective eavesdropping will leave a mark

on the decoy particles, so an outside eavesdropper cannot steal secrets without being detected.

In traveling model, the chances for an outside eavesdropper to steal secrets are in the stages of sharing keys [step (1)] and distributing states [step (2)]. However, the security of the key sharing stage follows directly from the unconditional security of QKD protocol. As the protocol is proposed based on the use of non-orthogonal decoy particles and the "block" technique transmission, which is similar to the stage of distributing states in distributed model. Once quantum channel is ensured secure, an outside eavesdropper cannot extract any participants' secrets.

4.2 Participant attacks

Since Gao et al. [30] firstly proposed the concept of legitimate participant attacks, much more attention has been paid to it [31–34]. Herein, we will generally consider two possible cases in the following.

4.2.1 Case 1: Participant attacks

In distributed model, suppose the dishonest participant P_t $(1 \leq t \leq n)$ wants to steal the secret of P_s $(1 \leq s \leq n, s \neq t)$. One possible method for P_t is to intercept the transmitted particles from TP to P_s, but he (she) will be detected as an outside attacker in such case. The other possible way is to utilize his (her) particles and the announced information (e.g., c_i^j $(1 \leq i \leq n, 1 \leq j \leq m)$ and the result of comparison) to exact secret x_s. Considering the extreme and perfect situation for P_t, which the other $n-2$ participants cooperate together with him (her), he (she) can get r_s easily on this occasion. Since TP will not act in collusion with any participant, it is impossible to get y_s or $(y_s + r_s) \bmod n$. Therefore, there is no way for P_t to get the secret of P_s.

In traveling model, since particles will be sent from P_t to P_{t+1}, the best chance for P_t is to steal the secret of P_{t+1}. The most general attack for P_t is as follows. P_t prepares $m + \delta$ fake states $|\varphi\rangle = \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} |k\rangle|k\rangle$, and creates S_2^{t+1} with the second particles of $|\varphi\rangle$ and decoy particles. Then, P_t sends S_2^{t+1} to P_{t+1}. There is no doubt that P_{t+1} cannot detect the eavesdropping of P_t during the stage of checking eavesdropper between P_t and P_{t+1}. Afterward, P_t intercepts the transmitted particles from P_{t+1} to P_{t+2}. But it can be detected in the stage of checking eavesdropper between P_{t+1} and P_{t+2}. The luckiest opportunity for P_t is to cooperate with P_{t+2}, and they can easily get c_{i+1} without detection by P_{t+1}. However, they still have no idea of k_{i+1}. Thence, P_t cannot get the secret of P_{t+1} as before.

4.2.2 Case 2: The semi-honest party (TP) attack

In distributed model, since the particle is in the maximally mixed state from being transmitted to be measured by P_i $(1 \leq i \leq n)$, the only opportunity for TP is to send fake states instead of $|\phi'\rangle$. For example, TP creates $m + n\delta$ states $\left|\phi''\right\rangle = |0\rangle^{\otimes n}$ and then applies the operation $F' |k\rangle = \frac{1}{\sqrt{n}} \sum_{r=0}^{n-1} \exp\left(\frac{-2\pi ikr}{n}\right) |r\rangle$ on each particle. Other

progress is same to the counterpart of above distributed model. The probability on each state of TP escaping to be detected successfully by $P_1, P_2, \ldots, P_n$ in the stage of checking integrity [step (3)] is $\frac{1}{2} + \frac{1}{2n}$. And the detection rate is $1 - \left(\frac{1}{2} - \frac{1}{2n}\right)^d$ with d checking states, which approximates to 1 if d is big enough. As above analyzed, if the states are not the required ones in our protocol, it will be discovered with nonzero probability. Therefore, TP cannot steal any secret without being detected.

In traveling model, the reduced density matrix of the second particle is $\rho = \left(\frac{1}{n}\right) I$ and independent of the phase operations. In fact, the secrets stored in phase are leant only when the first and the second particles are measured by a collective measurement. So the easiest to be stolen for TP is P_1's secret, and the most general attack is as follows. TP intercepts S_2^2 when it is traveling from P_1 to P_2. Since every particle in S_2^2 is in the maximally mixed state, TP cannot distinguish between decoy particles and carrier particles. Hence, TP will be detected as an outside attacker by P_1 and P_2. As TP cannot get the right order of the disrupted second particles, he (she) is impossible to get P_1's secret. Therefore, it is inevitable that TP cannot get any secrets.

Actually, there are some special attacks, such as the photon-number-splitting (PNS) attack, the decoy-photon Trojan horse attack and the invisible-photon Trojan horse attack. In order to defeat these attacks, some additional steps can be applied. For example, each participant can use some beam splitters to split the sampling signals before his (her) operation for checking eavesdropping process and insert filters in front of his (her) devices to filter out the photon signal with an illegitimate wavelength. So far, we have showed that the our proposed protocols in this paper are secure against both outside and inside attackers.

5 Security in real-word situation

We have discussed the security of our protocols in ideal channels. However, the real-world communication channels are generally suffered by losses or noise. And such imperfections will affect our protocols. In order to make our protocols satisfy the real situation, we make corresponding changes for our protocol.

Concretely, for losses channels, our protocols can be improved as follows. In distributed model protocol, TP prepares some extra τ states $|\phi^{'}\rangle$ and $n\mu$ states $|\varphi^{'}\rangle$ in step (1). That is, TP prepares $m + n\delta + \tau$ states $|\phi^{'}\rangle_1, |\phi^{'}\rangle_2, \ldots, |\phi^{'}\rangle_{m+n\delta+\tau}$ and $nm + n\mu$ states $|\varphi^{'}\rangle_1, |\varphi^{'}\rangle_2, \ldots, |\varphi^{'}\rangle_{nm+n\mu}$. Similar to the above constructing S_i, S_i is constructed by the ith particles of all $|\phi^{'}\rangle$, and the second particles of $m + \mu$ states $|\varphi^{'}\rangle$. In step (2), after P_i ($i \in \{1, 2, \ldots, n\}$) receives $S_i^{'}$ from TP, P_i should inform TP which particles have been received and which particles are lost in the transmission. Two maximal tolerable numbers of the embezzled states $|\phi^{'}\rangle$ and $|\varphi^{'}\rangle$ are τ and μ. That is to say, if the number of embezzled states $|\phi^{'}\rangle$ in all sequences $S_1^{'}, S_2^{'}, \ldots, S_n^{'}$ is no more than τ and the number of embezzled states $|\varphi^{'}\rangle$ in every sequence $S_i^{'}$ is no more than μ, the protocol continues. Then, they use the remaining decoy particles and pick out enough states $|\phi^{'}\rangle$ and $|\varphi^{'}\rangle$ to execute eavesdropping detection process and encoding secrets process. Otherwise, they abort the protocol and restart a protocol.

In traveling model protocol, TP prepares some extra τ states $|\varphi\rangle$ in step (2). In step (3), after P_1 receives S_2^1 from TP, P_1 also informs TP which particles have been

received and which particles are lost. A maximal tolerable number of the embezzled particles $|\varphi\rangle$ is τ in this transmission. However, in the following steps, if there is any encoding particle is lost in the transmission from P_{i-1} (P_n) to P_i (TP), they abort the protocol and restart a protocol. Otherwise if there is no state lost or the embezzled states are decoy states, the protocol continues.

Since noise is another unavoidable problem in the applications of our protocols, it will threaten the comparison result. However, even if we make many tries, there is as yet no effective method to improve our protocols, not to mention a maximal tolerable threshold. For example, in BB84 protocol, the maximal tolerable is $\omega = 11\,\%$. This is a disadvantage of our protocols.

Enlightened by Ref. [26,35–38], we have made an attempt for our protocol in distributed mode. Although it is not as significant as QKD protocols, it might be useful for further research in MQPC protocols. The detailed process is given as follows.

As we know, in distributed mode, our protocol is secure if y_i and r_i are got securely. In fact, the process of getting y_i and r_i can be seen as two process of QKD protocols between TP and P_i and among $P_1, P_2, \ldots, P_n$. So two simple classical post-process of error correction and privacy amplification can be adopted after step (4) and (5).

Since the security of QKD protocols for two participants based on d-level quantum systems has been detailedly described in Refs. [35–38], we do not give specific process of the first error correction and privacy amplification after step (4) here. By adopting the method in Ref. [26], simple process of the second error correction and privacy amplification for sharing r_i among n participants after step (5) is given below.

(i) All participants choose a permutation γ randomly in the set $\{1, 2, \ldots, m\}$.

(ii) $P_1, P_2, \ldots, P_n$ broadcast $\bar{k}_1 = \left\{\bar{k}_1^1, \ldots, \bar{k}_1^{\frac{m}{2}}\right\}$, $\bar{k}_2 = \left\{\bar{k}_2^1, \ldots, \bar{k}_2^{\frac{m}{2}}\right\}, \ldots, \bar{k}_n = \left\{\bar{k}_n^1, \ldots, \bar{k}_n^{\frac{m}{2}}\right\}$, where $\bar{k}_i^j = (\bar{k}_i^{\gamma(2j-1)} + \bar{k}_i^{\gamma(2j)}) \bmod n$ ($i \in \{1, 2, \ldots, n\}$, $j \in \{1, 2, \ldots, \frac{m}{2}\}$).

All participants verify whether

$$(\bar{k}_1 + \bar{k}_2 + \cdots + \bar{k}_n) \bmod n = 0. \tag{5}$$

If it holds they randomly keep one of the two sets $\{\bar{k}_1^{\gamma(2j-1)}, \bar{k}_2^{\gamma(2j-1)}, \ldots, \bar{k}_n^{\gamma(2j-1)}\}$ and $\{\bar{k}_1^{\gamma(2j)}, \bar{k}_2^{\gamma(2j)}, \ldots, \bar{k}_n^{\gamma(2j)}\}$. Otherwise, they discard both of the two sets. Suppose the accuracy of Eq. (6) is ε (i.e. the error rate is $1 - \varepsilon$), where

$$(k_1 + k_2 + \cdots + k_n) \bmod n = 0. \tag{6}$$

However, after the error correction, the accuracy becomes to

$$\varepsilon' = \frac{\varepsilon^2}{\varepsilon^2 + \frac{(1-\varepsilon)^2}{n-1}} \tag{7}$$

which is larger than ε when $\varepsilon > \frac{1}{n}$. By executing this algorithm many times, the accuracy can reach an expected value. Of course, there may be some more complex and efficient algorithms.

In order to reduce the information that an potential eavesdropper got, the process of privacy amplification need to execute after error correction. Similarly, we also give a simple example. P_i randomly chooses pairs of equations and publicizes their positions. Compared with announcing the summation values in error correction, P_i just needs to calculate them. Then, $P_1, P_2, \ldots, P_n$ replace every pair of chosen equations with their summation values. They will shorten their keys in this way, but an potential eavesdropper will get even less information. Suppose the probability for an eavesdropper to guess a Eq. (6) correctly is ϵ, then the probability that he (she) can guess the summation value of two equations is

$$\epsilon^{'} = \epsilon^2 + \frac{(1-\epsilon)^2}{n-1} \tag{8}$$

which is less than ϵ when $\epsilon > \frac{1}{n}$. Similarly, in order to reduce the information of an eavesdropper got, this process could be repeated many times. Note that steps (1)–(5) can be repeated several times or prepare more states $|\phi^{'}\rangle$ and $|\varphi^{'}\rangle$ in step (1), until TP and P_i and $P_1, P_2, \ldots, P_n$ share enough secure y_i and r_i before step (6).

Since the maximal tolerable threshold ω for QKD protocols based on d-level quantum system have been give out, we have reasons to believe that a error rate ω_1 for our protocol in the first eavesdropping detection is no more than ω. For simplicity, suppose the channels from TP to P_i are same. According to the Eq. (6), another error rate ω_2 for the second eavesdropping detection is

$$\omega_2 = 1 - (1-\omega_1)^n - \sum_{i=2}^{n} \frac{C_n^i \omega_1^i (1-\omega_1)^{n-i}}{n}.$$

For example, when $n = 3$, we can set $\omega_1 = 15.95\,\%$ [35–38], then $\omega_2 = 27.08\,\%$.

Unfortunately, in traveling mode, we still have not find the solution for noise channel. Maybe quantum error correction code [39,40] is a good choice, but we have not found the specific process.

6 Conclusion

In this paper, we further discuss the MQPC protocols for n participants. The comparison of equality for n participants' secrets can be achieved with one execution of our protocols, which is much better than the previous QPC protocols in efficiency. Compared to the pioneering MQPC protocol, we adopt a more reasonable assumption of semi-honest TP. With assistance of TP, n participants can get the comparison result at the same time. Hence, our protocols have the performance of fairness, privacy and security. From an experimental viewpoint, it appears that the traveling mode is easier since it does not require beyond bipartite entanglement. But the entanglement will weaken after a long distance traveling. Furthermore, since these protocols are based on the n level quantum systems, the realization of them may be difficult in actual situation. So we just describe the MQPC protocol in two modes in theory. The specific implement in experiment still need much effort in the future.

Acknowledgments This work is supported by NSFC (Grant Nos. 61272057, 61202434, 61170270, 61100203, 61003286, 61121061), NCET (Grant No. NCET-10-0260), Beijing Natural Science Foundation (Grant Nos. 4112040, 4122054), the Fundamental Research Funds for the Central Universities (Grant Nos. 2012RC0612, 2011YB01).

References

1. Bennett, C.H., Brassard, G.: Quantum cryptography: public-key distribution and coin tossing. In: Proceeding of the IEEE International Conference on Computers, Systems and Signal, pp. 175–179. Bangalore, India (1984)
2. Ekert, A.K.: Quantum cryptography based on Bell theorem. Phys. Rev. Lett. **67**, 661–663 (1991)
3. Boström, K., Felbinger, T.: Deterministic secure direct communication using entanglement. Phys. Rev. Lett. **89**, 187902 (2002)
4. Deng, F.G., Long, G.L., Liu, X.S.: Two-step quantum direct communication protocol using the Einstein–Podolsky–Rosen pair block. Phys. Rev. A **68**, 042317 (2003)
5. Cai, Q.Y., Li, B.W.: Improving the capacity of the Boström–Felbinger protocol. Phys. Rev. A **69**, 054301 (2004)
6. Wang, C., Deng, F.G., Li, Y.S., Liu, X.S., Long, G.L.: Quantum secure direct communication with high-dimension quantum superdense coding. Phys. Rev. A **71**, 044305 (2005)
7. 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. Phys. Rev. Lett. **70**, 1895 (1993)
8. Bouwmeester, D., Pan, J.W., Mattle, K., Eibl, M., Weinfurter, H., Zeilinger, A.: Experimental quantum teleportation. Nature (London) **390**, 575 (1997)
9. Hillery, M.: Quantum voting and privacy protection: first steps. Int. Soc. Opt. Eng. (2006). doi:10.1117/2.1200610.0419
10. Bonanome, M., Bužek, V., Hillery, M., Ziman, M.: Toward protocols for quantum-ensured privacy and secure voting. Phys. Rev. A **84**, 022331 (2011)
11. Naseri, M.: Secure quantum sealed-bid auction. Opt. Commun. **282**, 1939 (2009)
12. Wang, Q.L., Zhang, W.W., Su, Q.: Revisiting "The loophole of the improved secure quantum sealed-bid auction with post-confirmation and solution". Int. J. Theor. Phys. (2014). doi:10.1007/s10773-014-2112-y
13. Du, J.Z., Chen, X.B., Wen, Q.Y., Zhu, F.C.: Secure multiparty quantum summation. Acta Phys. Sin. **56**, 6214 (2007)
14. Yao, A.C.: Protocols for secure computations. In: Proceedings of 23rd I EEE Symposium on Foundations of Computer Science (FOCS 82), p. 160, Washington, DC, USA (1982)
15. Boudot, F., Schoenmakers, B., Traore, J.: A fair and efficient solution to the socialist millionaires problem. Discr. Appl. Math. (Special Issue Coding Cryptol.) **111**(1–2), 23–36 (2001)
16. Yang, Y.G., Wen, Q.Y.: An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement. J. Phys. A Math. Theor. **42**, 055305 (2009)
17. Chen, X.B., Xu, G., Niu, X.X., Wen, Q.Y., Yang, Y.X.: An efficient protocol for the private comparison of equal information based on the triplet entangled state and single-particle measurement. Opt. Commun. **283**, 1161–1165 (2009)
18. Jia, H.Y., Wen, Q.Y., Song, T.T., Gao, F.: Quantum protocol for millionaire problem. Opt. Commun. **284**, 545–549 (2011)
19. Liu, B., Gao, F., Jia, H.Y., Huang, W., Zhang, W.W., Wen, Q.Y.: Efficient quantum private comparison employing single photons and collective detection. Quantum Inf. Process. **12**, 887–897 (2012)
20. Tseng, H.Y., Lin, J., Hwang, T.: New quantum private comparison protocol using EPR pairs. Quantum Inf. Process. **11**, 373–384 (2012)
21. Yang, Y.G., Xia, J., Jia, X., Zhang, H.: Comment on "Quantum private comparison protocols with a semi-honest third party". Quantum Inf. Process. **12**, 877–885 (2013)
22. Chang, Y.J., Tsai, ChW: Multi-user private comparison protocol using GHZ class states. Quantum Inf. Process. **12**, 1077–1088 (2013)
23. Zhang, W.W., Zhang, K.J.: Cryptanalysis and improvement of the quantum private comparison protocol with semi-honest third party. Quantum Inf. Process. **12**, 1987–1990 (2013)

24. Zhang, W.W., Li, D., Zhang, K.J., Zuo, H.J.: A quantum protocol for millionaire problem with Bell states. Quantum Inf. Process. **12**, 2241–2249 (2013)
25. Huang, W., Wen, Q.Y., Liu, B., Gao, F., Sun, Y.: Robust and efficient quantum private comparison of equality with collective detection over collective-noise channels. Sci. Chin. Phys. Mech. Astron. **56**, 1670–1678 (2013)
26. Yu, C.H., Guo, G.D., Lin, S.: Quantum private comparison with d-level single-particle states. Phys. Scr. **88**, 065013 (2013)
27. Mayers, D.: Unconditionally secure quantum bit commitment is impossible. Phys. Rev. Lett. **78**, 3414 (1997)
28. Lo, H.K.: Insecurity of quantum secure computations. Phys. Rev. A **56**, 1154–1162 (1997)
29. Damgard, I., Fehr, S., Salvail, L., Schaffner, C.: Secure Identification and QKD in the bounded-quantum-storage model. Proc. Adv. Cryptol. **4622**, 342–359 (2007)
30. Gao, F., Qin, S.J., Wen, Q.Y., Zhu, F.C.: A simple participant attack on the Bradler C-Dusek protocol. Quantum Inf. Comput. **7**, 329 (2007)
31. Qin, S.J., Gao, F., Wen, Q.Y., Zhu, F.C.: Cryptanalysis of the Hillery–Bužek–Berthiaume quantum secret sharing protocol. Phys. Rev. A **76**, 062324 (2007)
32. Lin, S., Gao, F., Guo, F.Z., Wen, Q.Y., Zhu, F.C.: Comment on "Multiparty quantum secret sharing of classical messages based on entanglement swapping". Phys. Rev. A **76**, 036301 (2007)
33. Gao, F., Guo, F.Z., Wen, Q.Y., Zhu, F.C.: Comment on "Experimental demonstration of a quantum protocol for byzantine agreement and liar detection". Phys. Rev. Lett. **101**, 208901 (2008)
34. Song, T.T., Zhang, J., Gao, F.: Participant attack on quantum secret sharing based on entanglement swapping. Chin. Phys. B **18**, 1333 (2009)
35. Cerf, N.J., Bourennane, M., Karlsson, A., Gisin, N.: Security of quantum key distribution using d-level systems. Phys. Rev. Lett. **88**, 127902 (2002)
36. Karimipour, V., Bahraminasab, A.: Quantum key distribution for d-level systems with generalized Bell states. Phys. Rev. A **65**, 052331 (2002)
37. Durt, T., Kaszlikowski, D., Chen, J.L., Kwek, L.C.: Security of quantum key distributions with entangled qudits. Phys. Rev. A **69**, 032313 (2004)
38. Sheridan, L., Scarani, V.: Security proof for quantum key distribution using qudit systems. Phys. Rev. A **82**, 030301 (2010)
39. Raymond, L., Cesar, M., Juan, P.P., Wojciech, H.Z.: Perfect quantum error correcting code. Phys. Rev. Lett. **77**, 198–201 (1996)
40. Emanuel, K., Raymond, L.: Theory of quantum error-correcting codes. Phys. Rev. A **55**, 900–911 (1997)