Quantum Inf Process (2013) 12:1077–1088
DOI 10.1007/s11128-012-0454-z

Multi-user private comparison protocol using GHZ class states

Yao-Jen Chang · Chia-Wei Tsai · Tzonelih Hwang

Received: 29 March 2012 / Accepted: 9 July 2012 / Published online: 26 July 2012

Abstract This paper proposes a pioneering quantum private comparison (QPC) protocol for n users. State-of-the-art QPC protocols have been designed for two users who wish to compare their private information. However, if n users want to perform the equality comparison, these two-user QPC protocols have to be executed repeatedly at least $n - 1$ times. The proposed protocol allows n users' private information to be compared within one protocol execution. The proposed QPC protocol takes the Greenberger–Horne–Zeilinger (GHZ) class as a quantum resource and uses a special property in the GHZ-class state to perform the equality comparison. Moreover, due to the one-step quantum transmission, the protocol is free from Trojan horse attacks and it is also shown to be secure against other well-known attacks.

Keywords Greenberger–Horne–Zeilinger class state · Quantum private comparison · Trojan horse attack

1 Introduction

Since the first quantum cryptographic protocol, i.e., the quantum key distribution protocol (called BB84 protocol), was presented by Bennett and Brassard [1] in 1984, many quantum cryptographic protocols have been proposed to provide various security properties, such as teleportation [2–7], quantum secret sharing (QSS) [8–16], quantum secure direct communication (QSDC) [17–21], and quantum private comparison (QPC) [22,23]. Recently, QPC protocols have gained further prominence [22,23].

Y.-J. Chang · T. Hwang (✉)
Department of Computer Science and Information Engineering (CSIE),
National Cheng Kung University, Tainan City, Taiwan, ROC
e-mail: hwangtl@ismail.csie.ncku.edu.tw

C.-W. Tsai
Institute for Information Industry, Tainan City, Taiwan, ROC

The main goal of QPCs is to compare the equality of two parties' private information in public without revealing their information. Based on the properties of quantum mechanics, the equality comparison can be easily achieved without any complex computation.

The idea of private comparison has already been discussed in classical cryptography. Yao [24] proposed a protocol for the millionaires' problem to determine the richer candidate without the participating candidates knowing about the actual property owned by any other candidate. Based on Yao's millionaires' problem, Boudot [26] subsequently proposed a protocol to decide whether two millionaires are equally rich. However, Lo [25] pointed out that the equality function cannot be securely evaluated in a two-user scenario. Therefore, some additional assumptions [e.g., a semi-honest third party (TP)] need to considered to reach the goal of private comparison.

Previously, pioneering works such as quantum voting [27,28] and quantum auction [29–31] have shown how quantum private comparison can be used for applications. In these works, using the quantum mechanism, some evaluation functions are designed to calculate the summation of votes or to determine the winner of an auction. Upon summarizing the concepts described in [22,23] for designing a secure QPC protocol, the following requirements can be arrived at:

1. A TP, which is at least semi-honest, is required to help users complete the comparison. A semi-honest TP is a party who always follows the procedure of the protocol. This party will record all intermediate computations, and will not be corrupted by an outside eavesdropper. However, the TP may be curious about the users' information and might try to steal the information from the record.
2. The TP may know the positions of different bits in the compared information, but will not be able to know the actual bit value of the information.
3. All outsiders and users should only know the result of the comparison (i.e., identical or different), and not the different positions of the bits storing the information.
4. To guarantee the security of private information, several bits should be compared simultaneously instead of one bit at a time.

The first QPC protocol was proposed by Yang et al. [22] using Einstein–Podolsky–Rosen (EPR) pairs. In their protocol, a TP is required to generate photons and announce the comparison result. The security in Yang et al.'s scheme is based on the one-way hash function performed by the involved two users using local unitary operations. Since round trip transmissions (transmitting photons back and forth) are required in Yang et al.'s protocol, special optical filters have to be used to prevent Trojan horse attack [32–34]. However, these additional devices further decrease the protocol's efficiency. Therefore, Chen et al. [23] recently proposed a more efficient QPC protocol via a triplet Greenberger–Horne–Zeilinger (GHZ) state [35]. In their protocol, after TP delivers two qubits of each GHZ state to the two involved parties, the comparison can be completed by classical information exchange. Furthermore, TP needs to perform one of the following two unitary operations $I\,(=|0\rangle\langle 0|1\rangle\langle 1|)$ and $\sigma_z\,(=|0\rangle\langle 0|-|1\rangle\langle 1|)$ depending on his/her remaining qubits to correctly obtain the comparison result.

State-of-the-art QPC protocols mainly address the comparison between two users' information. If n users' information is compared and a two-user QPC protocol is used, then the same QPC protocol has to be executed $(n-1) \sim n\,(n-1)/2$ times (i.e.,

if n users' information is the same, the same protocol must be executed $n\,(n-1)/2$ times; if n users' information is different, the same protocol must be executed times) for achieving equality comparisons. It is obvious that the intuitive manner of comparing n parties' information using a two-user QPC is inefficient. Therefore, this study attempts to propose a method to perform a multi-user equality comparison within one protocol execution. In our protocol, TP uses the GHZ-class state (e.g., GHZ state $|\phi\rangle_{12\ldots n} = \frac{1}{\sqrt{2}}(|q_1, q_2, \ldots, q_n\rangle + |\bar{q}_1, \bar{q}_2, \ldots, \bar{q}_n\rangle)$ and GHZ-like state $|\psi\rangle_{12\ldots n} = \frac{1}{\sqrt{2}}(|g_1, g_2, \ldots, g_n\rangle + |\bar{g}_1, \bar{g}_2, \ldots, \bar{g}_n\rangle)$, where $q_i \in \{0, 1\}$, $g_i \in \{+, -\}$) to distribute a secret random key for each user. Then, each user employs the secret key to encrypt his/her information into a ciphertext, which is then sent to the TP. After executing the proposed protocol once, based on a special property in the GHZ-class state, the TP can compare any two users' information for equality by using the ciphertexts. That is, TP can complete the entire equality comparison in one execution of the new QPC protocol.

The rest of this paper is organized as follows. Section 2 introduces the special property of the GHZ-class state and provides details of the proposed QPC protocol. Section 3 analyzes the security of the proposed QPC and compares our protocol with other QPC protocols. Finally, a short conclusion is given in Sect. 4.

2 The proposed QPC protocol using GHZ class state

Section 2.1 introduces a property of GHZ class state, which discloses that the GHZ class state generator is able to know the xoring value of arbitrary two qubit measurement results without knowing the individual qubit's measurement result. Section 2.2 gives a detail description of multi-user QPC protocol.

2.1 A property in GHZ class state

Let $|\psi\rangle_{1\ldots n}\frac{1}{\sqrt{2}}(|q_1, q_2, \ldots, q_n\rangle \pm |\bar{q}_1, \bar{q}_2, \ldots, \bar{q}_n\rangle)$ be a GHZ state, where $q_i \in \{0, 1\}$ According to Heisenberg uncertainty principle, the ith particle could be $|q_i\rangle$ or $|\bar{q}_i\rangle$ (e.g., $|0\rangle$ or $|1\rangle$) with a probability of 50 %. In other words, no one can predetermine the ith particle's measurement result K_i in Z basis $\{|0\rangle, |1\rangle\}$.

However, if arbitrary two particles, say the ith and the jth particles, are considered at a time, one finds that the xoring value of the two measurement results $K_i \oplus K_j$ is fixed. Moreover, one can infer this fixed xoring value if he/she knows the initial state of GHZ state.

In order to clearly explain the property of GHZ state, let us take the four-particle GHZ state as an example. The four-particle GHZ state is shown as follows:

$$|\Psi_1\rangle = \frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle)\,|\Psi_2\rangle = \frac{1}{\sqrt{2}}(|0000\rangle - |1111\rangle)$$
$$|\Psi_3\rangle = \frac{1}{\sqrt{2}}(|0001\rangle + |1110\rangle)\,|\Psi_4\rangle = \frac{1}{\sqrt{2}}(|0001\rangle - |1110\rangle)$$

$$|\Psi_5\rangle = \frac{1}{\sqrt{2}}(|0010\rangle + |1101\rangle)\ |\Psi_6\rangle = \frac{1}{\sqrt{2}}(|0010\rangle - |1101\rangle)$$
$$|\Psi_7\rangle = \frac{1}{\sqrt{2}}(|0011\rangle + |1100\rangle)\ |\Psi_8\rangle = \frac{1}{\sqrt{2}}(|0011\rangle - |1100\rangle)$$
$$|\Psi_9\rangle = \frac{1}{\sqrt{2}}(|0100\rangle + |1011\rangle)\ |\Psi_{10}\rangle = \frac{1}{\sqrt{2}}(|0100\rangle - |1011\rangle)$$
$$|\Psi_{11}\rangle = \frac{1}{\sqrt{2}}(|0101\rangle + |1010\rangle)\ |\Psi_{12}\rangle = \frac{1}{\sqrt{2}}(|0101\rangle - |1010\rangle)$$
$$|\Psi_{13}\rangle = \frac{1}{\sqrt{2}}(|0110\rangle + |1001\rangle)\ |\Psi_{14}\rangle = \frac{1}{\sqrt{2}}(|0110\rangle - |1001\rangle)$$
$$|\Psi_{15}\rangle = \frac{1}{\sqrt{2}}(|0111\rangle + |1000\rangle)\ |\Psi_{16}\rangle = \frac{1}{\sqrt{2}}(|0111\rangle - |1000\rangle)$$

Obviously, if the initial state of $|\Psi_7\rangle$, state is, one immediately knows these values, $K_1 \oplus K_2 = 0$, $K_1 \oplus K_3 = 1$, $K_1 \oplus K_4 = 1$, $K_2 \oplus K_3 = 1$, $K_2 \oplus K_4 = 1$ and $K_3 \oplus K_4 = 0$ without knowing any individual measurement result K_i. If the state is $|\Psi_{15}\rangle$, one knows these values, $K_1 \oplus K_2 = 1$, $K_1 \oplus K_3 = 1$, $K_1 \oplus K_4 = 1$, $K_2 \oplus K_3 = 0$, $K_2 \oplus K_4 = 0$ and $K_3 \oplus K_4 = 0$.

Similarly, the GHZ-like state $|\psi\rangle_{12\ldots n} = \frac{1}{\sqrt{2}}(|g_1, g_2, \ldots, g_n\rangle + |\bar{g}_1, \bar{g}_2, \ldots, \bar{q}_n\rangle)$ has the same property if the qubit is measured in the X basis $\{|+\rangle, |-\rangle\}$, where $g_i \in \{+, -\}$.

With this property in the GHZ class state, a multi-user QPC protocol can be designed as follows.

2.2 The proposed QPC protocol

In this section, a multi-user QPC protocol is proposed. Firstly, a four-user QPC protocol is introduced to conveniently explain the idea and then the n-user QPC protocol is presented. To prevent malicious users from eavesdropping, TP will use both GHZ state and GHZ-like state as the quantum carrier. Here, we assume that the quantum channel is an ideal channel (i.e. there is no noise in this channel and the particle is not lost), the classical channel is an authenticated channel (the transmitted message is public but cannot be modified), and there is a semi-honest party, TP, who will honestly follow the procedure of the protocol to help users to do the equality comparison, but at the same time TP is also curious to know users' private information.

2.2.1 Four-user QPC protocol

Suppose four users, Alice, Bob, Charlie, and David, want to compare their information (m-bit classical messages) for equality. Then, they can proceed as follows (See also Fig. 1):

Step 1:

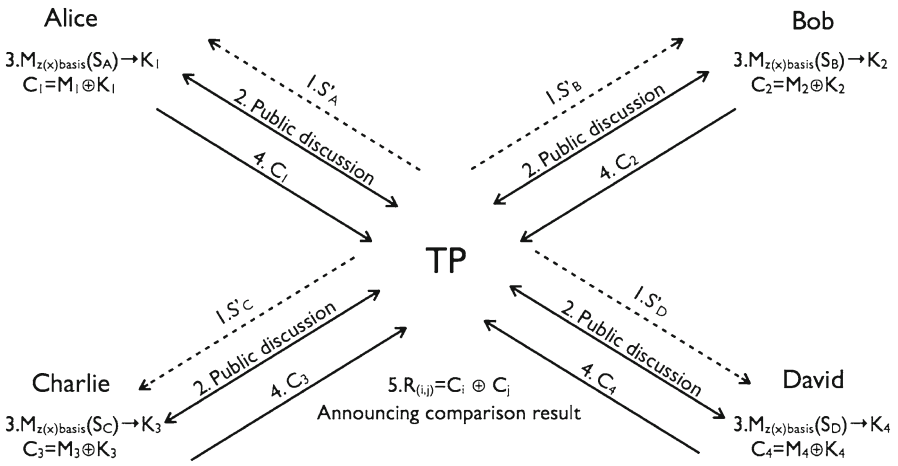

Fig. 1 Four-user QPC protocol

Firstly, TP prepares m GHZ class states randomly chosen from the GHZ state $|\Psi_i\rangle_{1234}$ or the GHZ-like states $|\psi_i\rangle_{1234}$, where $i = 1$ to 16. Then, TP divides these m states into four quantum sequences, S_A, S_B, S_C and S_D, which are formed by all the first, the second, the third and the forth particles of these GHZ class states, respectively. In order to check the presence of eavesdroppers, TP also generates enough decoy photons from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ to form the check sequences (i.e., D_A, D_B, D_C and D_D) and randomly mixes the check sequences respectively with the four quantum sequences S_A, S_B, S_C and S_D to get four new quantum sequences S'_A, S'_B, S'_C and S'_D, where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Finally, TP sends the quantum sequences S'_A, S'_B, S'_C and S'_D to Alice, Bob, Charlie, and David, respectively.

Step 2:

After Alice, Bob, Charlie and David receive the quantum sequences, they preserve the quantum sequences in short-time quantum registers [36–39] and send the acknowledgements to TP. Then, TP and the four users use the decoy photons to check the security of their quantum channels. In the procedure of checking eavesdropping, TP announces the positions and bases of the check sequences. According to the announced information, Alice, Bob, Charlie and David can extract D_A, D_B, D_C and D_D from S'_A, S'_B, S'_C and S'_D, respectively. Then, they perform the corresponding measurement and return the measurement results to TP. TP verifies these measurement results and checks whether eavesdroppers exist in the quantum channels. If the detected error rate exceeds a predetermined threshold [$\tau \doteq 2 \sim 8.9\,\%$ depending on the channel situation (e.g. the distance, etc.) [40–42]], TP will abort this communication and restart the protocol. Otherwise, TP moves to the next step.

Step 3:

After the procedure of eavesdropping check, TP announces which states are in the GHZ state and which are in the GHZ-like state. According to the type of initial states announced by TP, Alice, Bob, Charlie and David can measure each particle of S_A,

S_B, S_C and S_D in the corresponding basis, respectively. That is, if the i-th particle belongs to GHZ state, the users will measure it in Z basis ($|0\rangle$, $|1\rangle$); otherwise, they will measure it in X basis ($|+\rangle$, $|-\rangle$). Then, they decode each measurement result as a classical bit ("0" or "1"). Here, TP and all users pre-agree that the measurement results $|0\rangle$ and $|+\rangle$ are decoded as "0", and $|1\rangle$ and $|-\rangle$ are decoded as "1". Therefore, after measuring the quantum sequences, Alice (Bob, Charlie, and David) can obtain an m-bit classical sequence, which is denoted as K_1 (K_2, K_3 and K_4, respectively)

Step 4:

Alice, Bob, Charlie and David compute $C_1 = M_1 \bigoplus K_1$, $C_2 = M_2 \bigoplus K_2$, $C_3 = M_3 \bigoplus K_3$ and $C_4 = M_4 \bigoplus K_4$, where $\bigoplus$ is a bitwise exclusive-OR operation, and denote Alice's, Bob's, Charlie's and David's private information, respectively. Then, Alice, Bob, Charlie and David send C_1, C_2, C_3 and C_4 to TP via the authenticated classical channels, respectively.

Step 5:

TP computes $C_i \oplus C_j$, and obtains $R_{(i,j)}$ as shown in the following, where $i =$ 1 to 3, $j = 2$ to 4 and $i \neq j$.

$$\begin{array}{ll} R_{(1,2)} = C_1 \oplus C_2 & R_{(1,3)} = C_1 \oplus C_3 \\ R_{(1,4)} = C_1 \oplus C_4 & R_{(2,3)} = C_2 \oplus C_3 \\ R_{(2,4)} = C_2 \oplus C_4 & R_{(3,4)} = C_3 \oplus C_4 \end{array} \tag{1.1}$$

And we have:

$$\begin{aligned} R_{(i,j)} &= C_i \oplus C_j \\ &= M_i \oplus K_i \oplus M_j \oplus K_j \\ &= M_i \oplus M_j \oplus K_i \oplus K_j \end{aligned} \tag{1.2}$$

According to the property of GHZ class state described in Sect. 2.1, TP can infer the value $K_{(i,j)} = K_i \oplus K_j$ from the initial state of GHZ class state without knowing the individual values K_i and K_j. TP then obtains $M_i \oplus M_j$:

$$\begin{aligned} K_{(i,j)} \oplus R_{(i,j)} &= \left(K_i \oplus K_j\right) \oplus \left(M_i \oplus M_j \oplus K_i \oplus K_j\right) \\ &= \left(M_i \oplus M_j\right) \oplus \left(K_i \oplus K_j \oplus K_i \oplus K_j\right) \\ &= M_i \oplus M_j \end{aligned} \tag{1.3}$$

Hence, if all bits in $K_{(i,j)} \oplus R_{(i,j)}$ are 0, then M_i and M_j are the same. Otherwise, M_i and M_j are different. In this way, TP can do the equality comparison between an arbitrary pair of users and hence the private comparison among four users can be completed within one execution of the new QPC protocol.

2.2.2 Multiple-user QPC protocol

Here, we extend the four-user QPC protocol to the n-user situation as follows:

Step 1:

TP prepares mn-particle GHZ class states randomly chosen from either the GHZ state $|\Psi_j\rangle_{1\ldots n} = \frac{1}{\sqrt{2}}(|q_1, q_2, \ldots, q_n\rangle \pm |\bar{q}_1, \bar{q}_2, \ldots, \bar{q}_n\rangle)$ or GHZ-like state $|\Psi_j\rangle_{1\ldots n} = \frac{1}{\sqrt{2}}(|g_1, g_2, \ldots, g_n\rangle \pm |\bar{g}_1, \bar{g}_2, \ldots, \bar{g}_n\rangle)$, where, $j = 1$ to 2^n, $q_i \in \{|0\rangle, |1\rangle\}$ and $g_i \in \{|+\rangle, |-\rangle\}$. TP forms n quantum sequences S_i's from these GHZ class state as described earlier in the four-user QPC and mixes each S_i with enough decoy photons to obtain $S_i^{'}$. Each of which is then sent to the corresponding user.

Step 2:

Similar to the four-user QPC protocol, TP and each user employ the decoy photons to check the presence of eavesdroppers. If the quantum channel is secure, TP will continue the protocol; otherwise, TP will abort this communication and restart the protocol.

Step 3:

User$_i$ measures the remaining particles using the corresponding basis according to the type of initial GHZ class state announced by TP and then User$_i$ decodes the measurement results into an m-bit key K_i, where $i = 1$ to n.

Step 4:

User$_i$ computes $C_i = M_i \bigoplus K_i$ and sends C_i to TP through the authenticated classical channel.

Step 5:

According to the property of the GHZ class state descripted in Sect. 2.1, TP computes $R_{(i,j)} \oplus K_{(i,j)} = M_i \oplus M_j$ and he/she can complete the equality comparison among n users, where $i = 1$ to $n-1$, $j = 2$ to n, and $i \neq j$ Finally, TP announces the results of the equality comparison.

Obviously, all users' information can be compared within one execution of the proposed protocol. The proposed protocol provides better efficiency than the existing QPC protocols under the n-user situation.

3 Security analysis and comparison

This section contains two parts, the security analysis (Sects. 3.1, 3.2, 3.3) and the efficiency comparison (Sect. 3.4). Sections 3.1 and 3.2 focus on discussing the outsider attack and the insider attack, respectively. Then, in Sect. 3.3, the noisy and lossy quantum channel situation is discussed. Finally, a comparison is given to compare the efficiency among our protocol and two QPC protocols in Sect. 3.4.

3.1 Outsider attack

Similar to [23], after TP delivers particles to each user, all parties will start their first public discussion to check for the presence of an eavesdropper. TP announces the positions and the measurement bases of all decoy photons. Later, each user publishes the measurement results. TP can verify the measurement results to determine whether an eavesdropper exists on the quantum channel or not. Since the eavesdropper, Eve, does not know the positions, and the measurement bases of all decoy photons, some well-known attacks such as intercept-resend attack, measurement-resend

attack, and entanglement-measure attack can be detected via the checking mechanism [14,16,18,22,43–49]. For example, if Eve measures an *X basis* decoy photon $\{|+\rangle, |-\rangle\}$ with Z basis $\{|0\rangle, |1\rangle\}$, she will have a probability of 50 % to be detected. Obviously, Eve has a probability of 50 % to choose the wrong basis for measurement. Therefore, the detection rate for each decoy photons is 25 % $(1/2 \times 1/2)$. For l decoy photons, the detection rate is $1 - (3/4)^l$ which is close to 1 if l is large enough. Furthermore, since quanta are transmitted in one step in the proposed protocol, the Trojan horse attack can be automatically prevented. Therefore, the proposed protocol is free from outsider attacks.

3.2 Insider attack

In this sub-section, two cases of insider attacks are considered. The first case discusses the possibility for a user to obtain the other user's private information. The second case discusses the possibility for TP to steal each user's information.

Case 1. Insider user attack

Suppose a user, Alice, is a dishonest user who attempts to obtain the other user's (Bob) private information and TP is a semi-honest party who will not act in collusion with any user. If Alice tries to intercept the transmitted photons from TP to Bob, she will be caught as an outside attacker as described in Sect. 3.1 Thus, the only possible way for Alice to do is to use her particles to extract Bob's measurement result or infer $K_{Alice} \oplus K_{Bob}$. However, without knowing the initial GHZ class state, it is impossible for her to do so.

Case 2. The semi-honest party attack

In the protocol, we assume that TP is a semi-honest party. That is, he/she will follow the process of the protocol honestly, but TP is curious to know user's private information. Hence, TP will not prepare other types of particles (e.g., EPR state, single photon, and etc.) to steal the user's information. TP will not try to extract the information about users' information from the received ciphertext $C_i = M_i \bigoplus K_i$. Because TP has no information about K_i (i.e., C_i is an one-time pad ciphertext), he/she cannot obtain M_i. Thus, the proposed protocol is secure against the semi-honest party attack.

3.3 Security analyses over lossy and noisy channel

In the above analysis, the quantum channel is assumed to be ideal (i.e., no particle will lose and there is not noise). In practice, however, the quantum channel tends to be lossy and noisy. This subsection shows that our proposed protocol is still secure in a lossy and noisy channel. Moreover, we also assume that the eavesdropper, Eve, is powerful enough to be able to establish an ideal channel with any user. The lossy and the noisy situations are each discussed in case as follows.

Case 1. Lossy quantum channel

Eve intercepts the particles transmitted from TP to each user, retains some particles (e.g., 4 photons) to herself, and sends the other photons ($m + l - 4$ photons) to the user through an ideal channel. If the embezzled particles are not decoy photons, then Eve can measure the photons in the Z basis. The measurement result will correspond to

the user's key bits. Fortunately, our protocol can be secure against this kind of attack if it is modified slightly as follows. In Step 2 of our protocol, each user has to inform TP which particles have been received and which particles are lost in the transmission process. TP and each user only use the received photons to do the public discussion and the equality comparison. Because the intercepted particles become useless photons, Eve cannot extract any information about each user's secret from these photons.

Case 2. Noisy quantum channel

Eve intercepts the particles transmitted from TP to each user, performs intercept-and-resend attack or entangle-and-measure attack, and then forwards theses tampered particles to the user through an ideal channel established by herself. In this case, Eve attempts to cover up the tampering of particles as the noise existed on the quantum channel between TP and the user. It is clear that the attack will not be detected if the eavesdropper detection rate of our protocols is smaller than the quantum error rate (QBER) of noise, which, according to [40–42], is approximately between 2 and 8.9 % depending on the channel situation (e.g., distance, etc.). Fortunately, the eavesdropping detection rate of our protocol for a decoy photon is 25 %, which is obviously greater than the error rate of the quantum channel. Hence, our protocol is also secure under the noisy quantum channel.

3.4 Efficiency comparison

Suppose that n users want to do the equality comparisons with m-bit classical messages, and TP uses l decoy photons to check the presence of eavesdropping for a communication between TP and each user. In order to compare the efficiency of the proposed protocol with Yang et al.'s [22] and Chen et al.'s [23] protocols, the qubit efficiency is defined as $\eta_E = \frac{c}{t}$, where c denotes the classical bits that can be compared, and t denotes the total particles for each comparison phase. The comparison is shown in the following (see also Table 1).

Table 1 The comparison of the proposed protocol to the other QPC protocols

	Yang et al.'s [22]	Chen et al.'s [23]	Our protocol
Quantum state	Bell state	Triplet GHZ state	m-particle GHZ class state
Devices for Trojan horse attack	Yes	No	No
Operators for users	Unitary operator	Single photon measurement	Single photon measurement
Quantum measurement for TP	Yes	Yes	No
Quantum memory for TP	No	Yes	No
Qubit efficiency	$\frac{nm}{4(m+l)(n-1)} \sim \frac{nm}{4n(m+l)(n-1)}$	$\frac{nm}{(3m+2l)(n-1)} \sim \frac{n}{n(3m+2l)(n-1)}$	$\frac{nm}{n(m+1)}$
Number of times of protocol execution	$n-1 \sim \frac{n(n-1)}{2}$	$n-1 \sim \frac{n(n-1)}{2}$	1

Yang et al. use Bell states to compare the information between two parties. Therefore, in order to complete the equality comparison with n users, TP has to execute the same protocol x times, where $x = (n-1)$ to $\frac{n(n-1)}{2}$. In the optimal case (i.e., all users' information is the same), TP can complete the whole equality comparisons within the $n-1$-time executions; otherwise, in the worst case (i.e., each user's information is different from the others), TP has to execute the protocol $\frac{n(n-1)}{2}$ times. Since the round-trip strategy (the same photons are sent back and forth) for photon transmission has been adopted in their scheme, extra filters such as single photon detectors and the photon number splitter (PNS) have to be used to avoid the Trojan horse attacks. If we assume that at least 50 % of the transmitted photons are used to detect the delayed photons caused by Trojan horse attack, then the qubit efficiency of Yang et al.'s protocol is $\frac{nm}{4(m+l)(n-1)} \sim \frac{nm}{4(m+l)(n-1)}$.

In Chen et al.'s scheme, the triplet GHZ states are used to construct the QPC, in which TP only can compare two users' information within one execution. TP has also to execute the protocol x times. Similar to Yang et al.'s, x is from $(n-1)$ to $\frac{n(n-1)}{2}$. Because the particle transmission in the protocol is one-step, the Trojan horse attack is unsuccessful. The qubit efficiency of Chen et al.'s is $\frac{nm}{(3m+2l)(n-1)} \sim \frac{n}{n(3m+2l)(n-1)}$.

Our protocol employs the GHZ class state to complete n-user equality comparison within one execution, that is, TP only prepares n GHZ class states with m particles and $n \times l$ decoy photons. Moreover, the one-step particle transmission is adopted. Thus, the qubit efficiency of our protocol is $\frac{nm}{n(m+1)}$, which is more efficient than Yang et al.'s and Chen et al.'s protocols even in the optimal case.

In addition, Yang et al.'s and Chen et al.'s schemes require extra quantum devices such as the unitary operation and the quantum memory to perform the comparison. For Yang et al.'s scheme, the users have to perform unitary operations to encode the hash code of their information on the photons distributed from TP. For Chen et al.'s scheme, TP has to use quantum memory to store the third particles of the prepared GHZ states, and later perform unitary operation I or σ^z on those photons depending on the exclusive-OR result provided by the two players. In the proposed scheme, the TP is not required to perform any local unitary operation, store particles, or do any quantum measurement. The users only need to perform the single photon measurement to retrieve their own key. Thus, the proposed scheme is more efficient in multi-user information equality comparison.

4 Conclusion

This paper proposes an n-user QPC protocol using the GHZ class state. Users' information can be compared within one execution of the proposed protocol. The proposed protocol provides higher efficiency than existing QPC protocols under the n-user situation. Moreover, according to the technology of decoy photons and the Heisenberg Uncertainty Principle, the proposed protocol is secure against both outsider and insider attacks under ideal and noisy quantum channel environments. Furthermore, because one-step quantum transmission is adopted, the proposed protocol is free from Trojan

horse attacks. However, maximal entanglement states with n-particle must be used. Designing an n-user QPC protocol using the entanglement state, which is easier to maintain, is a promising concept for future research.

Acknowledgments The authors would like to thank the National Science Council of the Republic of China and the Research Center of Quantum Communication and Security, National Cheng Kung University, Taiwan, R.O.C. for financially supporting this research under Contract Nos. NSC 100-2221-E-006-152-MY3 and D100-36002, respectively.

References

1. Bennett, C.H., Brassard, G.: Quantum cryptography: public-key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, New York, Bangalore, India, pp. 175–179 (1984)
2. Bennett, CH., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., Wootters, WK.: Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels. Phys. Rev. Lett. **70**(13), 1895–1899 (1993)
3. Furusawa, A., Sørensen, J.L., Braunstein, S.L., Fuchs, C.A., Kimble, H.J., Polzik, E.S.: Unconditional quantum teleportation. Science **282**(5389), 706–709 (1998)
4. Zhang, Z.J., Man, Z.X.: Many-agent controlled teleportation of multi-qubit quantum information. Phys. Lett. A **341**(1–4), 55–59 (2005)
5. Zhang, W., Liu, Y.M., Liu, J., Zhang, Z.J.: Teleportation of arbitrary unknown two atom state with cluster state via thermal cavity. Chin. Phys. B **17**(9), 3203–3208 (2008)
6. Zhang, Z.Y., Liu, Y.M., Zuo, X.Q., Zhang, W., Zhang, Z.J.: Transformation operator and criterion for perfectly teleporting arbitrary three-qubit state with six-qubit channel and Bell-state measurement. Chin. Phys. Lett. **26**(12), 120303 (2009)
7. Tsai, C.W., Hwang, T.: Teleportation of a pure EPR state via GHZ-like state. Int. J. Theor. Phys. **49**(8), 1969–1975 (2010)
8. Hillery, M., Buzek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A **59**(3), 1829–1834 (1999)
9. Xiao, L., Long, G.L., Deng, F.G., Pan, J.W.: Efficient multiparty quantum secret sharing schemes. Phys. Rev. A **69**(5), 052307 (2004)
10. Zhang, Z.J., Man, Z.X.: Multiparty quantum secret sharing of classical messages based on entanglement swapping. Phys. Rev. A **72**(2), 022303 (2005)
11. Deng, F.G., Long, G.L., Zhou, H.Y.: An efficient quantum secret sharing scheme with Einstein–Podolsky–Rosen pairs. Phys. Lett. A **340**(1–4), 43–50 (2005)
12. Deng, F.G., Zhou, H.Y., Long, G.L.: Circular quantum secret sharing. J. Phys. A Math. Gen. **39**(45), 14089–14099 (2006)
13. Han, L.F., Liu, Y.M., Liu, J., Zhang, Z.J.: Multiparty quantum secret sharing of secure direct communication using single photons. Opt. Commun. **281**(9), 2690–2694 (2008)
14. Deng, F.G., Li, X.H., Zhou, H.Y.: Efficient high-capacity quantum secret sharing with two-photon entanglement. Phys. Lett. A **372**(12), 1957–1962 (2008)
15. Sun, Y., Wen, Q.Y., Gao, F., Chen, X.B., Zhu, F.C.: Multiparty quantum secret sharing based on Bell measurement. Opt. Commun. **282**(17), 3647–3651 (2009)
16. Shi, R.H., Huang, L.S., Yang, W., Zhong, H.: Multiparty quantum secret sharing with Bell states and Bell measurements. Opt. Commun. **283**(11), 2476–2480 (2010)
17. Bostroem, K., Felbinger, T.: Deterministic secure direct communication using entanglement. Phys. Rev. Lett. **89**(18), 187902 (2002)
18. 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**(4), 042317 (2003)
19. Man, Z.X., Zhang, Z.J., Li, Y.: Deterministic secure direct communication by using swapping quantum entanglement and local unitary operations. Chin. Phys. Lett. **22**(1), 18–21 (2005)
20. Zhan, Y.B., Zhang, L.L., Zhang, Q.Y.: Quantum secure direct communication by entangled qutrits and entanglement swapping. Opt. Commun. **282**(23), 4633–4636 (2009)
21. Yang, C.W., Tsai, C.W., Hwang, T.: Fault tolerant two-step quantum secure direct communication protocol against collective noises. Sci. China Ser. G: Phys. Mech. Astron. **54**(3), 496–501 (2011)

22. 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**(5), 055305 (2009)
23. Chen, X.B., Xu, G., Niu, X.X., Wen, QY., 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**(7), 1561–1565 (2010)
24. Yao, A.C.: Protocols for secure computations. In: Proceedings of 23rd IEEE Symposium on Foundations of Computer Science (FOCS' 82), Washington, DC, USA, p. 160 (1982)
25. Lo, H.K.: Insecurity of quantum secure computations. Phys. Rev. A **56**(2), 1154–1162 (1997)
26. Boudot, F., Schoenmakers, B., Traor'e, J.: A fair and efficient solution to the socialist millionaires' problem. Discret. Appl. Math. (Special Issue on Coding and Cryptology) **111**(1–2), 23–36 (2001)
27. Hillery, M., Ziman, M., Bužek, V., Bieliková, M.: Towards quantum-based privacy and voting. Phys. Lett. A **349**(1–4), 5–81 (2006)
28. Vaccaro, J.A., Spring, J., Chefles, A.: Quantum protocols for anonymous voting and surveying. Phys. Rev. A **75**(1), 012333 (2007)
29. Hogg, T., Harsha, P., Chen, K.Y.: Quantum auctions. Int. J. Quantum Inf. **5**, 751–780 (2007)
30. Yang, Y.G., Naseri, M., Wen, Q.Y.: Improved secure quantum sealed-bid auction. Opt. Commun. **282**(20), 4167–4170 (2009)
31. Zhao, Z., Naseri, M., Zheng, Y.: Secure quantum sealed-bid auction with post confirmation. Opt. Commun. **283**(16), 3194–3197 (2010)
32. Deng, F.G., Li, X.H., Zhou, H.Y., Zhang, Z.J.: Improving the security of multiparty quantum secret sharing against Trojan horse attack. Phys. Rev. A **72**(4), 044302 (2005)
33. Cai, Q.Y.: Eavesdropping on the two-way quantum communication protocols with invisible photons. Phys. Lett. A **351**(1–2), 23–25 (2006)
34. Li, X.H., Deng, F.G., Zhou, H.Y.: Improving the security of secure direct communication based on the secret transmitting order of particles. Phys. Rev. A **74**(5), 054302 (2006)
35. Greenberger, D.M., Horne, M.A., Zeilinger, A.: Going beyond Bell's theorem. Arxiv preprint arXiv:0712.0921 (2007)
36. Nielsen, M.A.: Quantum computation by measurement and quantum memory. Phys. Lett. A **308** (2–3), 96–100 (2003)
37. Jeffrey, E., Brenner, M., Kwiat, P.: Delayed-choice quantum cryptography. Proc. SPIE **5161**, 269–279 (2004)
38. Jeffrey, E., Altepeter, J., Kwiat, P.: Relativistic quantum cryptography. In: Frontiers in Optics, OSA Technical Digest (CD), Optical Society of America, paper FWB1 (2006)
39. Jeffrey, E., Altepeter, J., Kwiat, P.: Relativistic quantum cryptography with optical storage. In: International Conference on Quantum Information, OSA Technical Digest (CD), Optical Society of America, paper IFE1 (2007)
40. Jennewein, T., Simon, C., Weihs, G., Weinfurter, H., Zeilinger, A.: Quantum cryptography with entangled photons. Phys. Rev. Lett. **84**(20), 4729–4732 (2000)
41. Hughes, R.J., Nordholt, J.E., Derkacs, D., Peterson, C.G.: Practical free-space quantum key distribution over 10 km in daylight and at night. New. J. Phys. **4**, 43.1–43.14 (2002)
42. Gobby, C., Yuan, Z.L., Shields, A.J.: Quantum key distribution over 122 km of standard telecom fiber. Appl. Phys. Lett. **84**(19), 3762–3764 (2004)
43. Chong, S.K., Hwang, T.: The enhancement of three-party simultaneous quantum secure direct communication scheme with EPR pairs. Opt. Commun. **284**(1), 515–518 (2011)
44. Lin, J., Hwang, T.: An enhancement on Shi et al.'s multiparty quantum secret sharing protocol. Opt. Commun. **284**(5), 1468–1471 (2011)
45. Tsai, C.-W., Hwang, T.: New deterministic quantum communication via symmetric W state. Opt. Commun. **283**(21), 4397–4400 (2010)
46. Hsieh, C.R., Tsai, C.W., Hwang, T.: Quantum secret sharing using GHZ-like state. Commun. Theor. Phys. **54**(6), 1019–1022 (2010)
47. Tsai, C.W., Hsieh, C.R., Hwang, T.: Dense coding using cluster states and it's application on deterministic secure quantum communication. Eur. Phys. J. D **61**(3), 779–783 (2011)
48. Hwang, C.C., Hwang, T., Tsai, C.W.: Quantum key distribution protocol using dense coding of three-qubit W state. Eur. Phys. J. D **61**(3), 785–790 (2011)
49. Tsai, C.W., Hwang, T.: Multiparty quantum secret sharing based on two special entangled states. Sci. China Phys. Mech. Astron. **55**(3), 460–464 (2012)