CHIN. PHYS. LETT. Vol. 33, No. 1 (2016) 010301

Cryptanalysis and Improvement of the Multi-User QPCE Protocol with Semi-Honest Third Party *

Yan Chang(昌燕)[1,2**], Chun-Xiang Xu(许春香)[1], Shi-Bin Zhang(张仕斌)[2], Hai-Chun Wang(王海春)[2], Li-Li Yan(闫丽丽)[2], Gui-Hua Han(韩贵华)[2], Yuan-Yuan Huang(黄源源)[2], Zhi-Wei Sheng(盛志伟)[2]

[1]*Department of Computer Science and Technology, University of Electronic Science and Technology of China, Chengdu 611731*

[2]*College of Information Engineering, Chengdu University of Information Technology, Chengdu 610225*

(Received 7 September 2015)

In a recent work [Quantum Inf. Process 12 (2013) 1077], a multi-user protocol of quantum private comparison of equality (QPCE) is presented. Here we point out that if we relax the constraint of a semi-honest third party, the private information of the users will be totally leaked out to the third party. A special attack is demonstrated in detail. Furthermore, a possible improvement is proposed, which makes the protocol secure against this kind of attack.

PACS: 03.67.Dd, 03.67.Hk, 03.67.Pp DOI: 10.1088/0256-307X/33/1/010301

As we all know, both classical cryptographic algorithms and quantum cryptography can solve the problems of security. However, most classical cryptographic algorithms are based on some unproven intractability hypotheses. For instance, the security of the famous RSA public key cryptographic algorithm depends on the difficulty of the integer factorization problem.[1] Thus they only have computation security. The one-time pad can communicate with unconditional security. However, it requires that the number of bits in the secret key must be as great as the number of bits of information in the message. Quantum cryptography such as quantum key distribution (QKD)[2,3] provides unconditional security in theory since the security is assured by the quantum mechanical principle rather than difficulty of computation.

With the development of QKD, many quantum cryptography applications spring up, such as quantum private comparison of equality (QPCE), which is the quantum scheme for the problem of private equality comparison (PCE). PCE[4–6] resolves the problem that two millionaires want to know whether they happen to be equally rich, while neither millionaire wants to simply disclose their wealth. In 2009, Yang *et al.*[7] first proposed a QPCE scheme. Since then, many other novel QPC protocols based on different states have been put forward.[8–20] Based on triplet Greenberger–Horne–Zeilinger (GHZ) states, Chen *et al.*[8] proposed a QPC protocol. However, by means of intercept-resend attack[10] one can retrieve another's secret information,[9] due to the fact that the positions of detecting particles or the measurement basis in the eavesdropping check phase are determined by the participants. Lin *et al.*[9] put forward two solutions to avoid this attack, i.e., they let the third party (TP) determine the positions and the measurement basis. Liu *et al.* presented QPC protocols based on triplet W state,[11] four-particle χ-type state entanglement swapping,[12] Bell state[13] and triplet GHZ state,[14] respectively. Lin *et al.*[16] and Huang *et al.*[17] considered the QPCE protocols under a noise environment. In general, the existing QPCE protocols have a semi-honest TP at least to help the two parties (Alice and Bob) to compare the equality of privacy. This kind of semi-honest TP is called the first kind of TP in Ref. [20], which executes the protocol loyally and records all the results of its intermediate computations while he might try to steal the information from the record. The TP (the first kind) is thought to be unreasonable by Yang *et al.*[15] They thought that the first kind of TP should be replaced by the implementation of a semi-honest TP (the second kind of TP[20]), which is allowed to misbehave on its own but cannot conspire with either of two parties, which is the reasonable assumption for QPC. That is, the second kind of semi-honest TP cannot be corrupted by others (including the participants) and cannot learn any valuable information about participants' secrets through active and passive attacks.[15] In addition, QPCE protocols should satisfy another two principles. First, no matter whether TP will know the positions of different values in the information compared or not, he/she will not be able to know the actual value of the bit. Secondly, all outsiders and the two players should only know the result of the comparison (i.e., identical or different), while not the positions of the different information.[16]

*Supported by the National Natural Science Foundation of China under Grant Nos 61402058, 61572086 and 61370203, the Fund for Middle and Young Academic Leaders of Chengdu University of Information Technology under Grant No J201511, the Science and Technology Support Project of Sichuan Province under Grant No 2013GZX0137, the Fund for Young Persons Project of Sichuan Province under Grant No 12ZB017, and the Foundation of Cyberspace Security Key Laboratory of Sichuan Higher Education Institutions under Grant No szjj2014-074.

**Corresponding author. Email: cyttkl@cuit.edu.cn

© 2016 Chinese Physical Society and IOP Publishing Ltd

In most existing QPCE protocols, only two-user private comparison is implemented simultaneously. Few QPCE protocols compare privacy of more than two users simultaneously. Chang *et al.*[21] proposed a pioneering QPCE protocol for n users, which allows n users' private information to be compared within one protocol execution, where TP is the first kind of semi-honest TP. In our protocol, we present a special attack to the multi-user QPEC protocol, which allows a semi-honest TP with less constraint (the second kind of semi-honest TP) to obtain all the private information of the users without introducing any disturbance. The basic idea of this attack is that TP measures the particles before he/she distributes them to the users. When the user publishes C_i (the result of bitwise XOR the user's secret and a key obtained by measuring the particles that TP sent to him) to TP, TP will know each user's secret without being found. Furthermore, we propose the modification scheme to the protocol so that it can withstand this special attack.

Let us briefly describe the four-user QPCE protocol first.

The four-particle GHZ state is shown as follows:

$$\begin{aligned}
|\psi_1^{\pm}\rangle &= 1/\sqrt{2}(|0000\rangle \pm |1111\rangle), |\psi_2^{\pm}\rangle \\
&= 1/\sqrt{2}(|0001\rangle \pm |1110\rangle), \\
|\psi_3^{\pm}\rangle &= 1/\sqrt{2}(|0010\rangle \pm |1101\rangle), |\psi_4^{\pm}\rangle \\
&= 1/\sqrt{2}(|0011\rangle \pm |1100\rangle), \\
|\psi_5^{\pm}\rangle &= 1/\sqrt{2}(|0100\rangle \pm |1011\rangle), |\psi_6^{\pm}\rangle \\
&= 1/\sqrt{2}(|0101\rangle \pm |1010\rangle), \\
|\psi_7^{\pm}\rangle &= 1/\sqrt{2}(|0110\rangle \pm |1001\rangle), |\psi_8^{\pm}\rangle \\
&= 1/\sqrt{2}(|0111\rangle \pm |1000\rangle). \qquad (1)
\end{aligned}$$

The four-particle GHZ-like state is shown as follows:

$$\begin{aligned}
|\phi_1^{\pm}\rangle &= 1/\sqrt{2}(|++++\rangle \pm |----\rangle), \\
|\phi_2^{\pm}\rangle &= 1/\sqrt{2}(|+++-\rangle \pm |---+\rangle), \\
|\phi_3^{\pm}\rangle &= 1/\sqrt{2}(|++-+\rangle \pm |--+-\rangle), \\
|\phi_4^{\pm}\rangle &= 1/\sqrt{2}(|++--\rangle \pm |--++\rangle), \\
|\phi_5^{\pm}\rangle &= 1/\sqrt{2}(|+-++\rangle \pm |-+--\rangle), \\
|\phi_6^{\pm}\rangle &= 1/\sqrt{2}(|+-+-\rangle \pm |-+-+\rangle), \\
|\phi_7^{\pm}\rangle &= 1/\sqrt{2}(|+--+\rangle \pm |-++-\rangle), \\
|\phi_8^{\pm}\rangle &= 1/\sqrt{2}(|+---\rangle \pm |-+++\rangle). \qquad (2)
\end{aligned}$$

(i) TP prepares m four-particle GHZ class states randomly chosen from the GHZ state $|\psi_i\rangle_{1234}$ or the GHZ-like state $|\phi_i\rangle_{1234}$, where $i = 1$–8. Then, TP divides these m states into four particle sequences, $S_{\rm A}$, $S_{\rm B}$, $S_{\rm C}$ and $S_{\rm D}$, which are formed by all the first, second, third and forth particles of these GHZ class states, respectively. To detect the presence of eavesdroppers, TP also generates enough detecting photons randomly in $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ to form the detecting sequences (i.e., $D_{\rm A}$, $D_{\rm B}$, $D_{\rm C}$ and $D_{\rm D}$). TP randomly mixes the detecting sequences to the four sequences $S_{\rm A}$, $S_{\rm B}$, $S_{\rm C}$ and $S_{\rm D}$ to obtain four new sequences $S'_{\rm A}$, $S'_{\rm B}$, $S'_{\rm C}$ and $S'_{\rm D}$. Finally, TP sends the sequences $S'_{\rm A}$, $S'_{\rm B}$, $S'_{\rm C}$ and $S'_{\rm D}$ to Alice, Bob, Charlie and David, respectively.

(ii) After Alice, Bob, Charlie and David receive the particle sequences, they preserve the particle sequences in short-time quantum registers and send the acknowledgements to TP. Then, TP and the four users use the detecting photons to check the security of their quantum channels. In the procedure of detecting eavesdropping, TP announces the positions and bases of the detecting sequences. According to the announced information, Alice, Bob, Charlie and David can extract $D_{\rm A}$, $D_{\rm B}$, $D_{\rm C}$ and $D_{\rm D}$ from $S'_{\rm A}$, $S'_{\rm B}$, $S'_{\rm C}$ and $S'_{\rm D}$, 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, TP will abort this communication and restart the protocol. Otherwise, TP moves to the next step.

(iii) After the procedure of eavesdropping check, TP announces which state is in the GHZ state and which is in the GHZ-like state. According to the type of initial states announced by TP, Alice, Bob, Charlie and David can measure every particle of $S_{\rm A}$, $S_{\rm B}$, $S_{\rm C}$ and $S_{\rm D}$ in the corresponding basis, respectively. That is, if the ith 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 all the particles, 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).

(iv) Alice, Bob, Charlie and David compute $C_1 = M_1 \oplus K_1$, $C_2 = M_2 \oplus K_2$, $C_3 = M_3 \oplus K_3$ and $C_4 = M_4 \oplus K_4$, where $\oplus$ is a bitwise exclusive-OR operation, and M_i denotes 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.

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

$$\begin{aligned}
R_{(i,j)} &= C_i \oplus C_j \\
&= M_i \oplus K_i \oplus M_j \oplus K_j \\
&= M_i \oplus M_j \oplus K_i \oplus K_j. \qquad (3)
\end{aligned}$$

According to the property of GHZ class state, TP can infer the value $K_{(i,j)} = K_i \oplus K_j$ from the initial state of GHZ state or GHZ-like state without knowing the

individual values K_i and K_j. TP then obtains $M_i \oplus M_j$

$$\begin{aligned} K_{(i,j)} \oplus R_{(i,j)} &= (K_i \oplus K_j) \oplus (M_i \oplus M_j \oplus K_i \oplus K_j) \\ &= (M_i \oplus M_j) \oplus (K_i \oplus K_j \oplus K_i \oplus K_j) \\ &= M_i \oplus M_j. \end{aligned} \tag{4}$$

Hence, if all bits in $K_{(i,j)} \oplus R_{(i,j)}$ are 0, then M_i and M_j will be the same. Otherwise, M_i and M_j will be different. In this way, TP can carry out 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 QPCE protocol. The process of multi-user QPCE protocol is similar to the four-user QPCE protocol, and will not be described here.

Obviously, in this multi-user QPCE protocol, the users trust TP almost completely. They think that TP will carry out the protocol loyally and record all the results of its intermediate computations. The only dishonest action they thought of as TP is to steal the information from the record. However, this assumption of TP is unreasonable.[16] To obtain secrets of the users, TP may attempt his best, i.e., through active and passive attacks, if only he/she will not be found by the users.

We analyze the security of multi-user QPCE protocol, and show that if TP measures the particles before he/she distributes them to the users, when the users announce C_i to TP, TP will know each user's secret without being found.

In step 1, TP measures $S_{\rm A}$, $S_{\rm B}$, $S_{\rm C}$ and $S_{\rm D}$ with Z-basis or X-basis according to the GHZ state or the GHZ-like state TP prepared. Then TP will obtain classical keys K_1, K_2, K_3 and K_4. Here TP and all users pre-agree that measurement results $|0\rangle$ and $|+\rangle$ are decoded as 0, and $|1\rangle$ and $|-\rangle$ are decoded as 1. TP randomly mixes the detecting sequences $D_{\rm A}$, $D_{\rm B}$, $D_{\rm C}$ and $D_{\rm D}$ to the four particle sequences $S_{\rm A}$, $S_{\rm B}$, $S_{\rm C}$ and $S_{\rm D}$, respectively, and forms four new particle sequences $S'_{\rm A}$, $S'_{\rm B}$, $S'_{\rm C}$ and $S'_{\rm D}$. TP sends $S'_{\rm A}$, $S'_{\rm B}$, $S'_{\rm C}$ and $S'_{\rm D}$ to Alice, Bob, Charlie and David, respectively.

In step 2, after Alice, Bob, Charlie and David receive $S'_{\rm A}$, $S'_{\rm B}$, $S'_{\rm C}$ and $S'_{\rm D}$, they preserve the quantum states in short-time quantum registers and send the acknowledgements to TP. Then, they come to the procedure of detecting eavesdropping; TP announces the positions and bases of detecting sequences. According to the announced information, Alice, Bob, Charlie and David extract $D_{\rm A}$, $D_{\rm B}$, $D_{\rm C}$, $D_{\rm D}$, 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. Obviously, in the procedure of detecting eavesdropping, the misbehavior of TP that measures $S_{\rm A}$, $S_{\rm B}$, $S_{\rm C}$ and $S_{\rm D}$ before he/she sends them to Alice, Bob, Charlie and David will not increase the probability to abort this communication. That is, Alice, Bob, Charlie and David cannot find the misbehavior of TP.

In step 3, TP announces which state is in the GHZ state and which is 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 $S_{\rm A}$, $S_{\rm B}$, $S_{\rm C}$ and $S_{\rm D}$ in the corresponding basis. Then Alice, Bob, Charlie and David will obtain classical keys K_1, K_2, K_3 and K_4, respectively, according to their pre-agreement (measurement results $|0\rangle$ and $|+\rangle$ are decoded as 0, and $|1\rangle$ and $|-\rangle$ are decoded as 1).

In step 4, Alice, Bob, Charlie and David compute $C_1 = M_1 \oplus K_1$, $C_2 = M_2 \oplus K_2$, $C_3 = M_3 \oplus K_3$ and $C_4 = M_4 \oplus K_4$, where $\oplus$ is a bitwise exclusive-OR operation, and M_i denotes Alice's, Bob's, Charlie's and David's private information, respectively. Then they send C_1, C_2, C_3 and C_4 to TP via the authenticated classical channels, respectively. TP obtains the private information of Alice, Bob, Charlie and David by computing $M_1 = C_1 \oplus K_1$, $M_2 = C_2 \oplus K_2$, $M_3 = C_3 \oplus K_3$ and $M_4 = C_4 \oplus K_4$. TP compares the equality of the private information of the users and sends the result to the users.

Obviously, in the multi-user QPCE protocol, if we relax the constraint of TP, the private information of the users will be totally leaked out to TP.

Up to now, we have proposed a special TP attack, by which TP obtains the private information of the users without being found. In fact, such an attack works only when the users send C_i to TP individually. Thus we can make some slight modifications to the protocols so that they can resist the proposed attack.

In step 4, Alice, Bob, Charlie and David compute $C_1 = M_1 \oplus K_1$, $C_2 = M_2 \oplus K_2$, $C_3 = M_3 \oplus K_3$ and $C_4 = M_4 \oplus K_4$, respectively. Then Alice converts C_1 to particle sequence $S^*_{\rm A}$ according to the rule that 0 to $|0\rangle$ or $|+\rangle$ randomly and 1 to $|1\rangle$ or $|-\rangle$ randomly. Alice mixes some detecting photons (random in states $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$) in $S^*_{\rm A}$. By carrying this out, Alice forms new sequence $S^{*'}_{\rm A}$. Alice sends $S^{*'}_{\rm A}$ to Bob.

(1) After Bob receives $S^{*'}_{\rm A}$, Alice publishes the bases and positions of detecting photons. Bob extracts detecting photons and measures them, if the QBER is lower than a threshold they continue to carry out the protocol, otherwise they terminate it. Similar to Alice and Bob, Charlie forms new sequence $S^{*'}_{\rm C}$ and sends it to David.

(2) Alice (Charlie) announces the basis of $S^*_{\rm A}$ ($S^*_{\rm C}$), Bob (David) measures $S^*_{\rm A}$ ($S^*_{\rm C}$) with Z-basis or X-basis and obtains C_1 (C_3). Bob (David) computes $C_1 \oplus C_2 = C_{\rm AB}$ ($C_3 \oplus C_4 = C_{\rm CD}$).

Notice that here Bob (David) cannot infer K_1 from K_2 (K_3 from K_4), therefore Bob (David) cannot infer M_1 from C_1 (M_3 from C_3).

Bob and David publish $C_{\rm AB}$ ($C_{\rm AB} = C_1 \oplus C_2$) and $C_{\rm CD}$ ($C_{\rm CD} = C_3 \oplus C_4$), respectively.

TP compares the equality of their privacy.

$$C_{\rm AB} = C_1 \oplus C_2 = M_1 \oplus K_1 \oplus M_2 \oplus K_2, \tag{5}$$

$$M_1 \oplus M_2 = C_{\rm AB} \oplus K_1 \oplus K_2, \tag{6}$$

due to the fact that TP knows $C_{\rm AB}$ and the result of $K_1 \oplus K_2$, TP can compare the equality of M_1 and M_2.

Similarly, TP can compare the equality of M_3 and M_4 according to $M_3 \oplus M_4 = C_{\rm CD} \oplus K_3 \oplus K_4$.

If Alice and Charlie want to know the equality of their privacy, Alice will send $S_{\rm A}^{*'}$ to Charlie. Charlie publishes $C_{\rm AC}$ ($C_{\rm AC} = C_1 \oplus C_3$). TP can compare the equality of M_1 and M_3 according to $M_1 \oplus M_3 = C_{\rm AC} \oplus K_1 \oplus K_3$.

TP is assumed to be semi-honest, that is, TP will not conspire with any other one. Therefore, we consider only the situation that TP attacks actively or passively on his/her own. The possible attack TP may perform is that TP measures each particle before he/she sends them to Alice, Bob, Charlie and David. By carrying this out, TP can obtain K_1, K_2, K_3 and K_4. After Bob and David publish $C_{\rm AB} = C_1 \oplus C_2$ and $C_{\rm CD} = C_3 \oplus C_4$, by computing $C_1 \oplus C_2 \oplus K_1 \oplus K_2 = M_1 \oplus K_1 \oplus M_2 \oplus K_2 \oplus K_1 \oplus K_2 = M_1 \oplus M_2$ and $C_3 \oplus C_4 \oplus K_3 \oplus K_4 = M_3 \oplus K_3 \oplus M_4 \oplus K_4 \oplus K_3 \oplus K_4 = M_3 \oplus M_4$, TP can only obtain $M_1 \oplus M_2$ and $M_3 \oplus M_4$. Therefore, even if TP measures each particle before he/she sends them to Alice, Bob, Charlie and David, TP cannot obtain the secret of the participants.

First of all, the users will not conspire with other users to risk giving the private information away themselves. Therefore, Alice, Bob, Charlie and David will not tell anyone about their measurement results in step 3, which will lead to the leakage of their keys K_1, K_2, K_3 or K_4. The way Bob conspires with David is that David tells Bob C_3 and Bob tells David C_1. If Bob colludes with David, Bob tells David C_1 and David tells Bob C_3 in secret. Then after Bob and David publish $C_{\rm AB}$ ($C_{\rm AB} = C_1 \oplus C_2$) and $C_{\rm CD}$ ($C_{\rm CD} = C_3 \oplus C_4$), both Bob and David know C_1, C_2, C_3 and C_4, however which will not lead to leakage of private information of any users, as is shown in Eq. (7). That is, the conspiracy attack among participants will not succeed,

$$\begin{aligned}
&C_1 \oplus C_2 \oplus K_1 \\
&= M_1 \oplus K_1 \oplus M_2 \oplus K_2 \oplus K_1 \\
&= M_1 \oplus M_2 \oplus K_2, \\
&C_1 \oplus C_2 \oplus K_2 \\
&= M_1 \oplus K_1 \oplus M_2 \oplus K_2 \oplus K_2 \\
&= M_1 \oplus M_2 \oplus K_1, \\
&C_2 \oplus C_3 \oplus K_2 \\
&= M_2 \oplus K_2 \oplus M_3 \oplus K_3 \oplus K_2 \\
&= M_2 \oplus M_3 \oplus K_3, \\
&C_3 \oplus C_4 \oplus K_4 \\
&= M_3 \oplus K_3 \oplus M_4 \oplus K_4 \oplus K_4 \\
&= M_3 \oplus M_4 \oplus K_3, \\
&C_3 \oplus C_4 \oplus K_3 \\
&= M_3 \oplus K_3 \oplus M_4 \oplus K_4 \oplus K_3 \\
&= M_3 \oplus M_4 \oplus K_4, \\
&C_1 \oplus C_4 \oplus K_4 \\
&= M_1 \oplus K_1 \oplus M_4 \oplus K_4 \oplus K_4 \\
&= M_1 \oplus M_4 \oplus K_1, \\
&C_1 \oplus C_2 \oplus C_3 \oplus K_2 \\
&= M_1 \oplus K_1 \oplus M_2 \oplus K_2 \oplus M_3 \oplus K_3 \oplus K_2 \\
&= M_1 \oplus M_2 \oplus M_3 \oplus K_1 \oplus K_3, \\
&C_2 \oplus C_3 \oplus C_4 \oplus K_2 \\
&= M_2 \oplus K_2 \oplus M_3 \oplus K_3 \oplus M_4 \oplus K_4 \oplus K_2 \\
&= M_2 \oplus M_3 \oplus M_4 \oplus K_3 \oplus K_4, \\
&C_1 \oplus C_2 \oplus C_4 \oplus K_2 \\
&= M_1 \oplus K_1 \oplus M_2 \oplus K_2 \oplus M_4 \oplus K_4 \oplus K_2 \\
&= M_1 \oplus M_2 \oplus M_4 \oplus K_1 \oplus K_4, \\
&C_1 \oplus C_3 \oplus C_4 \oplus K_4 \\
&= M_1 \oplus K_1 \oplus M_3 \oplus K_3 \oplus M_4 \oplus K_4 \oplus K_4 \\
&= M_1 \oplus M_3 \oplus M_4 \oplus K_1 \oplus K_3, \\
&C_1 \oplus C_2 \oplus C_4 \oplus K_4 \\
&= M_1 \oplus K_1 \oplus M_2 \oplus K_2 \oplus M_4 \oplus K_4 \oplus K_4 \\
&= M_1 \oplus M_2 \oplus M_4 \oplus K_1 \oplus K_2, \\
&C_2 \oplus C_3 \oplus C_4 \oplus K_4 \\
&= M_2 \oplus K_2 \oplus M_3 \oplus K_3 \oplus M_4 \oplus K_4 \oplus K_4 \\
&= M_2 \oplus M_3 \oplus M_4 \oplus K_2 \oplus K_3, \\
&C_1 \oplus C_2 \oplus C_3 \oplus C_4 \oplus K_1 \\
&= M_1 \oplus K_1 \oplus M_2 \oplus K_2 \oplus M_3 \oplus K_3 \oplus M_4 \oplus K_4 \oplus K_1, \\
&= M_1 \oplus M_2 \oplus M_3 \oplus M_4 \oplus K_2 \oplus K_3 \oplus K_4, \\
&C_1 \oplus C_2 \oplus C_3 \oplus C_4 \oplus K_4 \\
&= M_1 \oplus K_1 \oplus M_2 \oplus K_2 \oplus M_3 \oplus K_3 \oplus M_4 \oplus K_4 \oplus K_4, \\
&= M_1 \oplus M_2 \oplus M_3 \oplus M_4 \oplus K_1 \oplus K_2 \oplus K_3.
\end{aligned} \tag{7}$$

Individual attack means performing attack by their own without conspiring with others. Bob (David) cannot perform an individual attack although he knows C_1 (C_3), due to the fact that he does not know K_1 (K_3). If Bob (David) intercepts and measures particles when TP sends particle-1 sequence (particle-3 sequence) to Alice (Charlie), due to the fact that the bases and positions of detecting photons in each particle sequence is controlled by TP, he will be found by TP in eavesdropping detection, and the protocol will be stopped.

The outside eavesdropper Eve cannot obtain the secret of the participants. First, if Eve intercepts and measures particles when TP distributes the particle sequence to the participants, Eve will be found by TP in eavesdropping detection. Therefore, Eve cannot obtain K_1, K_2, K_3 or K_4. Secondly, Eve cannot obtain any useful information from $C_{\rm BA} = C_1 \oplus C_2$ and $C_{\rm DC} = C_3 \oplus C_4$, due to the fact that K_1, K_2, K_3 and K_4 are real random numbers, C_1, C_2, C_3 and C_4 are the results of one-time pad of M_1, M_2, M_3 and

M_4, respectively.

In summary, we have presented a special TP attack to the multi-user QPCE protocol, which allows a semi-honest TP with less constraint to obtain all the private information of the users without introducing any disturbance. The basic idea of this attack is that TP measures the particles before he/she distributed them to the users, when the users announce C_i to TP, TP will know each user's secret without being found. Furthermore, we propose the modification scheme to the protocols so that they can withstand this special attack.

References

[1] Rivest R L, Shamir A and Adleman L 1978 *Commun. ACM* **21** 120
[2] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. Comput. Syst. Signal Process.* p 175
[3] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[4] Yao A C 1982 *Proceedings of the 23rd Annual IEEE Symposium on Foundations of Computer Science* p 160
[5] Boudot F, Schoenmakers B and Traore J 2001 *Discrete Appl. Math.* **111** 23
[6] Lo H K 1997 *Phys. Rev.* A **56** 1154
[7] Yang Y G and Wen Q Y 2009 *J. Phys. A: Math. Theor.* **42** 055305
[8] Chen X B, Xu G, Niu X X, Wen Q Y and Yang Y X 2010 *Opt. Commun.* **283** 1561
[9] Lin J, Tseng H Y and Hwang T 2011 *Opt. Commun.* **284** 2412
[10] Gao F, Guo F Z, Wen Q Y and Zhu F C 2008 *Phys. Rev. Lett.* **101** 208901
[11] Liu W, Wang Y B andJiang Z T 2011 *Opt. Commun.* **284** 3160
[12] Liu W, Wang Y B, Jiang Z T and Cao Y Z 2012 *Int. J. Theor. Phys.* **51** 69
[13] Liu W, Wang Y B and Cui W 2012 *Commun. Theor. Phys.* **57** 583
[14] Liu W and Wang Y B 2012 *Int. J. Theor. Phys.* **51** 3596
[15] Yang Y G, Xia J and Jia X 2013 *Quantum Inf. Process.* **12** 877
[16] Huang W, Wen Q Y, Liu B, Gao F and Sun Y 2013 *Sci. Chin. Phys. Mech. & Astron.* **56** 1670
[17] Li Y B, Qin S J, Yuan Z, Huang W and Sun Y 2013 *Quantum Inf. Process.* **12** 2191
[18] Lin S, Sun Y, Liu X F and Yao Z Q 2013 *Quantum Inf. Process.* **12** 559
[19] Liu W J, Liu C, Wang H B and Jia T T 2013 *Iete Tech. Rev.* **30** 439
[20] Zhang W W and Zhang K J 2013 *Quantum Inf. Process.* **12** 1981
[21] Chang Y J, Tsai C W and Hwang T 2013 *Quantum Inf. Process.* **12** 1077