Int J Theor Phys (2016) 55:1710–1718
DOI 10.1007/s10773-015-2810-0

Secure Quantum Private Comparison Protocol Based on the Entanglement Swapping Between Three-Particle W-Class State and Bell State

Jian Li[1,2,3] · Lu Jia[1] · Hong-Fu Zhou[1] · Ting-Ting Zhang[1]

Received: 23 March 2015 / Accepted: 4 September 2015 / Published online: 24 September 2015

Abstract We propose a new quantum private comparison protocol with the help of a semi-honest third party (TP), enabling two participants to compare the equality of their private inputs without exposing any information about their respective private inputs. Different from previous protocols, our protocol utilizes the properties of entanglement swapping between three-particle W-Class state and Bell state. The presented protocol can ensure correctness, fairness and security. Meanwhile, all the quantum particles undergo a one-way transmission, and all the participants including TP are just required having the ability to perform Bell-state measurement and exclusive-or operation which make our protocol more feasible and efficient. At last, the security of this protocol with respect to various kinds of attacks is analyzed in detail.

Keywords Secure quantum private comparison · Three particle W-Class state · Entanglement swapping · Quantum cryptography

1 Introduction

With the development of quantum cryptography, there exist more and more interesting applications based on quantum cryptography since the first quantum key distribution protocol(BB84) was proposed by Benett and Brassard [1].

✉ Jian Li
jelolulu@163.com

[1] School of Computer, Beijing University of Posts and Telecommunications, Beijing 100876, China

[2] Hefei National Laboratory for Physical Sciences at the Microscale, University of Science and Technology of China, Hefei 230026, China

[3] Science and Technology on Communication Security Laboratory, Sichuan 610041, Chengdu, China

Secure multi-party computation (SMC), which has been extensively studied in cryptography domain, is to compute a function jointly in a distributed network where each party holds one private input, and that in the end only the evaluation result is known and other information such as their private inputs are not revealed. In theory, the general SMC problem is solvable but for some special cases of SMC, general solutions are impractical and special solutions should be developed. At present, special SMC problem is mainly researched in classical setting, but Shor pointed out [2] that SMC problems can be solved by models based on quantum setting with higher efficiency. This view point leads us to explore special SMC problem in the quantum field. Recently some special SMC problems have been solved in quantum setting, such as quantum protocol for anonymous voting and surveying [3, 4], quantum anonymous ranking [5], quantum auction [6–8], quantum protocol for millionaire problem [9], and so on.

Quantum private comparison of equality(QPCE), which was first introduced by Yao in classical cryptography [10] for the millionaires' problem, is a fundamental special SMC problem and has become an important branch in quantum cryptography. Extended from the millionaires' problem in which two millionaires want to know whether they are equally rich without disclosing their amount of assets, QPCE aims to achieve the goal that two parties can determine the equality of their private inputs without leaking their own information to each other, based on the unique properties of quantum mechanics. It is a pity that for active adversaries, Lo [11] shows that the equality function cannot be computed securely in a two-party scenario, even in quantum cryptography. However, if some additional assumptions(such as introducing a semi-honest third party) are made, the goal of private comparison can be obtained.

In recent years, the design and analysis of QPCE protocols have attracted much interest and attention. The first QPCE protocol was proposed by Yang et al. [12]. After that, a lot of QPCE protocols using different entangled states have been designed, such as Bell states, GHZ states, W states, and χ-type states, etc. [13–22].

In this paper, following some ideas of the protocols in Refs. [12–22], we proposed a new QPCE protocol utilizing the three-particle W-Class state and the Bell state. This protocol includes a third party TP who is assumed to be semi-honest (also called honest-but-curious), i.e., TP follows the rules of the protocol loyally (thus being honest) but in the meantime records all the information and may try to learn additional information from the protocol execution (thus being curious).

In our protocol, TP is used to prepare the initial states, do some calculations and record all intermediate computations. By comparison with the previous QPCE protocols, our protocol has the following advantages:

- The W-Class state, which can be described as $|W_C\rangle = \frac{1}{2}(|001\rangle + |010\rangle + |100\rangle + |111\rangle)$, is much more robust than the GHZ state. The maximally entangled GHZ state is also maximally fragile for it violates Bell inequalities maximally, however, the W-Class state can retain bipartite entanglement even when any qubit is traced out. This interesting property attracts us to apply entanglement swapping to it in this protocol. In addition, many quantum transmission tasks, such as quantum teleportation [23], quantum dense coding [24], etc have been presented based on the W-Class states. Thus, it is of special value to apply the W-class states in QPCE.
- Compared with most of the previous protocols [12–22], our protocol has a higher comparison efficiency, for we use two methods to reduce the number of comparisons. First,

the private inputs of two participants are divided into groups and the comparison is completed group by group. Second, in every round of comparison, two participants can compare two bits of their private information each time.

– Unitary operations, which are used in protocols [14, 15, 19–21] to get the result, are unneeded in our protocol. The comparison result can be obtained just by doing some measurements and simple calculations, thus making our protocol easier to implement.

The structure of this paper is organized as follows: in Section 2, an efficient QPCE protocol is described in detail and the security of this protocol is analyzed in Section 3. Finally, a brief discussion and the concluding summary are given in Section 4.

2 The QPCE Protocol

In this section, a different QPCE protocol using the W-class state and the Bell state $|\Phi^+\rangle$ is described in steps. Before describing it, we first show the W-Class state and the entanglement swapping principle of the W-Class state and Bell state $|\Phi^+\rangle$:

$$\begin{aligned} |W_C\rangle_{123} &= \frac{1}{2}(|001\rangle + |010\rangle + |100\rangle + |111\rangle)_{123} \\ &= \frac{1}{\sqrt{2}}(|0\rangle_1|\Psi^+\rangle_{23} + |1\rangle_1|\Phi^+\rangle_{23}) \end{aligned} \tag{1}$$

$$\begin{aligned} |W_C\rangle_{123} \bigotimes |\Phi^+\rangle_{45} &= \frac{1}{\sqrt{2}}(|0\rangle_1|\Psi^+\rangle_{23}|\Phi^+\rangle_{45} + |1\rangle_1|\Phi^+\rangle_{23}|\Phi^+\rangle_{45}) \\ &= \frac{1}{2\sqrt{2}}(|0\rangle_1|\Phi^+\rangle_{24}|\Psi^+\rangle_{35} + |0\rangle_1|\Phi^-\rangle_{24}|\Psi^-\rangle_{35} \\ &\quad +|0\rangle_1|\Psi^+\rangle_{24}|\Phi^+\rangle_{35} + |0\rangle_1|\Psi^-\rangle_{24}|\Phi^-\rangle_{35} \\ &\quad +|1\rangle_1|\Phi^+\rangle_{24}|\Phi^+\rangle_{35} + |1\rangle_1|\Phi^-\rangle_{24}|\Phi^-\rangle_{35} \\ &\quad +|1\rangle_1|\Psi^+\rangle_{24}|\Psi^+\rangle_{35} + |1\rangle_1|\Psi^-\rangle_{24}|\Psi^-\rangle_{35}) \end{aligned} \tag{2}$$

Where $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, $|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$, $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$, $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$.

The process of our protocol can be described as follows:

Input: Alice and Bob have their private integer X and Y respectively. The binary representations of X and Y in can be written as: $X = (x_0, x_1, \ldots, x_{N-1})$, $Y = (y_0, y_1, \ldots, y_{N-1})$, where $x_i, y_i \in \{0, 1\}$, and $X = \sum_{i=0}^{N-1} x_i 2^i$, $Y = \sum_{i=0}^{N-1} y_i 2^i$, $2^{N-1} \leq max X, Y \leq 2^N$.

Output: Whether $X = Y$ or not.

2.1 Preparing Step

(1) Alice(Bob) divides the N-bit binary string $X(Y)$ into $\lceil N/2L \rceil$ groups, each group having $2L$ bits. If $N \bmod 2 = 1$, Alice(Bob) inserts one 0 at the end of the N-bit binary string $X(Y)$, $X = A_{\lceil N/2L \rceil} \ldots A_2 A_1$, $Y = B_{\lceil N/2L \rceil} \ldots B_2 B_1$.

$$A_j = (x_j^0, x_j^1, \ldots, x_j^{2L-1}), B_j = (y_j^0, y_j^1, \ldots, y_j^{2L-1}) \tag{3}$$

(2) For each group $A_j(B_j)$, Alice(Bob) forms every two adjacent bits into a pair $Q_A^i = (x_j^{2i}, x_j^{2i+1})$, $Q_B^i = (y_j^{2i}, y_j^{2i+1})$.

$$A_j = (Q_A^0, Q_A^1, \ldots, Q_A^{L-1}), B_j = (Q_B^0, Q_B^1, \ldots, Q_B^{L-1}) \tag{4}$$

In order to improve the comparison efficiency and decrease the cost of the classical information, one group $A_j(B_j)$ of the private information owned by Alice(Bob) is compared in each round of comparison.

(3) In the jth round of the comparison, TP prepares an ordered sequence S_1 which consists of L three-particle W-Class states

$$\left[P_T^0 P_{A_1}^0 P_{B_1}^0, P_T^1 P_{A_1}^1 P_{B_1}^1, \ldots, P_T^{L-1} P_{A_1}^{L-1} P_{B_1}^{L-1}\right] \tag{5}$$

where the subscript T, A_1, B_1 indicates the three particles in one W-Class state. Then TP prepares an ordered sequence S_2 which consists of L Bell states $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$,

$$\left[P_{A_2}^0 P_{B_2}^0, P_{A_2}^1 P_{B_2}^1, \ldots, P_{A_2}^{L-1} P_{B_2}^{L-1}\right] \tag{6}$$

where the A_2, B_2 represent the two particles in one Bell state.

(4) TP takes the first particles of all W-Class states in S_1 to form an ordered sequence S_T

$$S_T : \left[P_T^0, P_T^1, \ldots, P_T^{L-1}\right] \tag{7}$$

TP takes the second particles of all W-Class states in S_1 and the first particles of all $|\Phi^+\rangle$ states in S_2 to form a new ordered sequence S_A.

$$S_A : \left[P_{A_1}^0 P_{A_2}^0, P_{A_1}^1 P_{A_2}^1, \ldots, P_{A_1}^{L-1} P_{A_2}^{L-1}\right] \tag{8}$$

TP takes the third particles of all W-Class states in S_1 and the second particles of all $|\Phi^+\rangle$ states in S_2 to form a new ordered sequence S_B.

$$S_B : \left[P_{B_1}^0 P_{B_2}^0, P_{B_1}^1 P_{B_2}^1, \ldots, P_{B_1}^{L-1} P_{B_2}^{L-1}\right] \tag{9}$$

(5) To prevent eavesdropping, TP prepares two bunches of decoy photons D_A and D_B randomly chosen from states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Then TP mixes the sequences S_A with D_A (S_B with D_B) to form two new sequences S'_A and S'_B and sends the sequence S'_A to Alice, S'_B to Bob.

2.2 Checking Step

(1) After the two participants receive the sequences S'_A and S'_B, TP announces the positions and the measuring bases of D_A and D_B.

(2) According to the positions, Alice and Bob pick out these decoy particles from S'_A and S'_B, and measure them in corresponding bases.

(3) Alice and Bob send their measuring results to TP for eavesdropping detection. If the error rate exceeds a suitable threshold, TP will terminate this communication and restart from the preparing step. Otherwise, the protocol can go on to the next step.

2.3 Coding Step

(1) After the checking step, Alice(Bob) recovers $S_A(S_B)$ by discarding the decoy photons.

(2) Alice(Bob) uses Bell basis to measure the ith pair $P_{A_1}^i P_{A_2}^i (P_{B_1}^i P_{B_2}^i)$ in $S_A(S_B)$. We

Table 1 $C_A^i(C_B^i)$'s values according to $M_A^i(M_B^i)$

$M_A^i(M_B^i$	$C_A^i(C_B^i)$
$\|\Phi^+\rangle$	00
$\|\Phi^-\rangle$	01
$\|\Psi^+\rangle$	10
$\|\Psi^-\rangle$	11

denote the measurement result with $M_A^i(M_B^i)$. After the measurement, Alice and Bob will obtain a two-bit value C_A^i and C_B^i respectively according to the Table 1.

(3) For every two-bit pair $Q_A^i(Q_B^i)$, Alice(Bob) calculates $R_A^i = Q_A^i \oplus C_A^i(R_B^i = Q_B^i \oplus C_B^i)$, the symbol $\oplus$ denotes the bit-wise exclusive-OR. Then Alice(Bob) gets a sequence $R_A^0 R_A^1, \ldots, R_A^{L-1}(R_B^0 R_B^1, \ldots, R_B^{L-1})$.

(4) Alice(Bob) uses quantum-one-time pad and $K_A(K_B)$ to encrypt the new sequence $R_A^0 R_A^1, \ldots, R_A^{L-1}(R_B^0 R_B^1, \ldots, R_B^{L-1})$ and sends the encrypted sequence $E_{K_A}(R_A^0 R_A^1, \ldots, R_A^{L-1})(E_{K_B}(R_B^0 R_B^1, \ldots, R_B^{L-1}))$ to TP.

2.4 Decoding Step

(1) After receiving two sequences from Alice and Bob, TP uses K_A, K_B to decrypt $E_{K_A}(R_A^0 R_A^1, \ldots, R_A^{L-1})$, $E_{K_B}(R_B^0 R_B^1, \ldots, R_B^{L-1})$.

(2) TP calculates $R_{AB}^i = R_A^i \oplus R_B^i$.

(3) TP uses the basis $\{|0\rangle, |1\rangle\}$ to measure the ith particle in S_T and gets M_C^i. Through calculating and summarizing for all cases, we find the following relation shown in Table 2.

(4) According to Table 2, if $Q_A^i = Q_B^i$, TP records the value $r = 0$, else if $Q_A^i \neq Q_B^i$, $r = 1$.

We show two cases in the Table 3. In one round of comparison, TP obtains L cbits values in all. If all values are 0, TP records $R_j = 0$ and goes on to the next round of comparison. If there is at least one value 1, TP records $R_j = 1$,then he stops the protocol and announces the final result $F = 1$ to indicate the inequality of their information.

(5) When $j = [N/2L] + 1$ and all the records $R_j = 0(j = 1, 2, \ldots, [N/2L] + 1)$, TP announces the final result $F = 0$. Alice and Bob can simultaneously know that their inputs X and Y are equal. Through at best $[N/2L] + 1$ rounds of comparison, Alice and Bob can prove each other whether their respective inputs X and Y are equal or not.

Table 2 Relation between Q_A^i and Q_B^i according to M_C^i and R_{AB}^i

$M_C^i \backslash R_{AB}^i$	00	01	10	11
$\|0\rangle$	$Q_A^i \neq Q_B^i$	$Q_A^i \neq Q_B^i$	$Q_A^i = Q_B^i$	$Q_A^i \neq Q_B^i$
$\|1\rangle$	$Q_A^i = Q_B^i$	$Q_A^i \neq Q_B^i$	$Q_A^i \neq Q_B^i$	$Q_A^i \neq Q_B^i$

Table 3 Two cases of Q_A^i, Q_B^i's values

Q_A^i	Q_B^i	M_A^i	M_B^i	C_A^i	C_B^i	R_A^i	R_B^i	R_{AB}^i	M_C^i	r
00	00	$\|\Phi^+\rangle$	$\|\Phi^+\rangle$	00	00	00	00	00	$\|1\rangle$	0
		$\|\Phi^+\rangle$	$\|\Psi^+\rangle$	00	10	00	10	10	$\|0\rangle$	0
		$\|\Phi^-\rangle$	$\|\Phi^-\rangle$	01	01	01	01	00	$\|1\rangle$	0
		$\|\Phi^-\rangle$	$\|\Psi^-\rangle$	01	11	01	11	10	$\|0\rangle$	0
		$\|\Psi^+\rangle$	$\|\Phi^+\rangle$	10	00	10	00	10	$\|0\rangle$	0
		$\|\Psi^+\rangle$	$\|\Psi^+\rangle$	10	10	10	10	00	$\|1\rangle$	0
		$\|\Psi^-\rangle$	$\|\Phi^-\rangle$	11	01	11	01	10	$\|0\rangle$	0
		$\|\Psi^-\rangle$	$\|\Psi^-\rangle$	11	11	11	11	00	$\|1\rangle$	0
00	01	$\|\Phi^+\rangle$	$\|\Phi^+\rangle$	00	00	00	01	01	$\|1\rangle$	1
		$\|\Phi^+\rangle$	$\|\Psi^+\rangle$	00	10	00	11	11	$\|0\rangle$	1
		$\|\Phi^-\rangle$	$\|\Phi^-\rangle$	01	01	01	00	01	$\|1\rangle$	1
		$\|\Phi^-\rangle$	$\|\Psi^-\rangle$	01	11	01	10	11	$\|0\rangle$	1
		$\|\Psi^+\rangle$	$\|\Phi^+\rangle$	10	00	10	01	11	$\|0\rangle$	1
		$\|\Psi^+\rangle$	$\|\Psi^+\rangle$	10	10	10	11	01	$\|1\rangle$	1
		$\|\Psi^-\rangle$	$\|\Phi^-\rangle$	11	01	11	00	11	$\|0\rangle$	1
		$\|\Psi^-\rangle$	$\|\Psi^-\rangle$	11	11	11	10	01	$\|1\rangle$	1

3 Security Analysis

In this section, attacks from all parties are analyzed, including two attack scenarios: (1) Outside eavesdropper attempts to steal two participants' inputs X or Y. (2) Two dishonest participants and the semi-honest TP may try to obtain the private information. And we will show our protocol is secure against both the outside attack and the participant attack.

3.1 Outside Attack

Assuming an outside eavesdropper Owen, We analyze Owen's chance of obtaining information about X and Y in every step of protocol.

In preparing step, Owen can attack the quantum channel when TP sends $S'_A(S'_B)$ to Alice(Bob). The Trojan horse attack can be automatically prevented since this is a one-way transmission protocol. Moreover, several other kinds of attacks, such as the intercept-resend attack, the entanglement-measure attack and the collective attack will be detected with nonzero probability during the checking step.

For example, we consider Owen takes the intercept-resend attack strategy on Bob as follows: Owen first intercepts the photon sequence S'_B (from TP to Bob in preparing step(5)), then he measures S'_B with Bell basis and gets a measurement result sequence $M_{S'_B}$. In order to prevent TP from discovering this attack in checking step(3), Owen generates a new photon sequence P_B with the same photon states as $M_{S'_B}$. He resends P_B to Bob. Then Owen may retrieve information from $M_{S'_B}$.

However, as Owen doesn't know the position of decoy single photons in S'_B, he can't discard the decoy photons when he measures S'_B with Bell basis, thus the decoy photons will destroy the correctness of the measurement and Owen's new photon sequence P_B, which has the same states with measurement result $M_{S'_B}$, will be quite different from S'_B. After

Bob has received the photon sequence P_B, he will start the eavesdropping check process, and the attack will be easily detected for the the states of decoy photons has been damaged.

In coding step, Alice(Bob) sends $R_A^0 R_A^1, \ldots, R_A^{L-1}(R_B^0 R_B^1, \ldots, R_B^{L-1})$ to TP. R_A^i and R_B^i can't reveal the information X and Y, so the outside eavesdropper can't get anything. In decoding step, TP announces only one cbit F for the comparison of secret messages. From this one cbit, outside eavesdropper can't deduce information X and Y.

So, the outside attack is invalid to this protocol.

3.2 Participant Attack

Generally, a participant is easier to attack than an outside eavesdropper, because he can get and utilize partial information legally. We will consider two kinds of attacks.

Case 1 One participant attempts to eavesdrop the other's private information.

Without loss of generality, because the role of Alice is same as that of Bob, we assume that Alice wants to learn Bob's information. Similar to the outside eavesdropper, Alice's several kinds of attack launched during the preparing step can be detected by adopting the decoy photon technique. Besides, there isn't any information transfer between Alice and Bob during the whole process in this protocol.

Now the only way for Alice to infer Bob's private information is by deriving from the measurement result M_A^i of $P_{A_1}^i P_{A_2}^i$ in her hand and R_B^i which is sent from Bob to TP. Because Alice can't get TP's measurement result M_C^i, she can't infer the measurement result M_B^i of $P_{B_1}^i P_{B_2}^i$ in Bob's hand according to (2). R_B^i is sent using the quantum-one-pad from Bob to TP thus Alice can't eavesdrop any information about R_B^i. Therefore, Alice can't infer Bob's private information.

Case 2 TP attempts to eavesdrop the participants' private information X and Y.

In this protocol, TP is semi-honest which means he is curious about the participants' private information. Besides, TP takes part in the whole process of the protocol execution, including preparing quantum carriers, doing some measurement and recording intermediate results, which provides him more power to attack. However, all the intermediate data obtained by TP which relate to the participants' private infoprmation are just R_A^i and R_B^i, which are sent to TP from Alice and Bob in coding step. Thus, TP can only infer information from R_A^i, R_B^i, and TP's measurement result M_C^i. As is shown in Table 3:

$$\begin{aligned} &P(R_A^i = 00) = P(R_A^i = 01) = P(R_A^i = 10) = P(R_A^i = 11) = \frac{1}{4} \\ &P(R_B^i = 00) = P(R_B^i = 01) = P(R_B^i = 10) = P(R_B^i = 11) = \frac{1}{4} \\ &P(M_C^i = |0\rangle) = P(M_C^i = |1\rangle) = \frac{1}{2} \end{aligned} \tag{10}$$

That is, TP obtains these measurement results with the same probability, so TP can't determinately know the value of Q_A^i, Q_B^i.

We have to point out that TP knows the comparison result r of Q_A^i and Q_B^i in each round. However, only with r, TP can't deduce the exact value of Q_A^i and Q_B^i in each round. In

Table 4 Comparison(supposing n classical bits are compared)

Protocol	Ref [14]	Ref [25]	This protocol
Quantum resource	3-qubit GHZ state	1-qubit $\|+\rangle$ state	3-qubit W-Class state and Bell state
Need of unitary operation	Yes	Yes	No
Need of hash function	No	Yes	No
Bit number compared each time	1	1	2
Comparison times	n	n	$\lceil \frac{n}{2} \rceil$
Eavesdropping detection	Unable to detect an intercept Cresend attack [26].	Collective detection is taken after all the quantum states have been operated and transmitted, thus the eavesdropping can't be detected timely.	Decoy photons are used and can detect eavesdropping well.

other words, if r=0, i.e., the partial inputs Q_A^i and Q_B^i are equal, TP derives

$$P(Q_A^i = Q_B^i = 00) = \frac{1}{4}, P(Q_A^i = Q_B^i = 01) = \frac{1}{4}$$
$$P(Q_A^i = Q_B^i = 10) = \frac{1}{4}, P(Q_A^i = Q_B^i = 11) = \frac{1}{4} \quad (11)$$

if r=1, i.e., the partial inputs Q_A^i and Q_B^i are unequal, TP derives

$$P(Q_A^i = 00, Q_B^i = 01) = \frac{1}{12}, P(Q_A^i = 00, Q_B^i = 10) = \frac{1}{12}$$
$$P(Q_A^i = 00, Q_B^i = 11) = \frac{1}{12}, P(Q_A^i = 01, Q_B^i = 00) = \frac{1}{12}$$
$$P(Q_A^i = 01, Q_B^i = 10) = \frac{1}{12}, P(Q_A^i = 01, Q_B^i = 11) = \frac{1}{12}$$
$$P(Q_A^i = 10, Q_B^i = 00) = \frac{1}{12}, P(Q_A^i = 10, Q_B^i = 01) = \frac{1}{12}$$
$$P(Q_A^i = 10, Q_B^i = 11) = \frac{1}{12}, P(Q_A^i = 11, Q_B^i = 00) = \frac{1}{12}$$
$$P(Q_A^i = 11, Q_B^i = 01) = \frac{1}{12}, P(Q_A^i = 11, Q_B^i = 10) = \frac{1}{12} \quad (12)$$

Therefore, TP doesn't have any advantage to derive any private information owned by Alice and Bob. So this protocol is secure against TP's attack.

4 Discussion and Conclusions

Before making a conclusion, it is worthwhile to make a comparison between this protocol and some previous protocols. Different from most previous QPCE protocols [14, 15, 17, 25] in which the binary bits of the private information are compared one by one, two bits

can be compared each time in our protocol by performing entanglement swapping between the W-Class state and Bell state. Other different aspects are described in Table 4. Through the comprehensive comparison, it can be seen that our protocol has a better performance on operability, efficiency and security.

In summary, we proposed a new QPCE protocol based on the three-particle W-Class state and Bell states swapping. It's a new application of the three-particle W-Class state. With the help of a semi-honest TP, two participants can know the equality of their private input X and Y, but they can't learn the information owned by each other and TP also can't learn any information about X and Y. Various kinds of attacks are discussed. The protocol can withstand these attacks well, so the security of our protocol is quite high.

In our further works, the two-party protocol can be considered to extend to the case of multi-party, such as multi-party sorting problem.

Acknowledgments This work is supported by the National Natural Science Foundation of China (Grant No. 61472048, No. 61402058, No. 61472046, No. 61202082, No. 61370194), the Beijing Natural Science Foundation (4152038), the China Postdoctoral Science Foundation funded project No. 2014M561826.

References

1. Bennett, C.H., Brassard, G.: Theor. Comput. Sci. **560**, 7 (2014)
2. Shor, P.W.: SIAM J. Comput. **26**(5), 1484 (1997)
3. Bonanome, M., Bużek, V., Hillery, M., Ziman, M.: Phys. Rev. A **84**(2), 022331 (2011)
4. Vaccaro, J.A., Spring, J., Chefles, A.: Phys. Rev. A **75**(1), 012333 (2007)
5. Huang, W., Wen, Q.Y., Liu, B., Su, Q., Qin, S.J., Gao, F.: Phys. Rev. A **89**(3), 032325 (2014)
6. Hogg, T., Harsha, P., Chen, K.Y.: Int. J. Quantum Inf. **5**(05), 751 (2007)
7. Yang, Y.G., Naseri, M., Wen, Q.Y.: Opt. Commun. **282**(20), 4167 (2009)
8. Zhao, Z., Naseri, M., Zheng, Y.: Opt. Commun. **283**(16), 3194 (2010)
9. Jia, H.Y., Wen, Q.Y., Song, T.T., Gao, F.: Opt. Commun. **284**(1), 545 (2011)
10. Yao, A.C.: In: 2013 IEEE 54th Annual Symposium on Foundations of Computer Science, pp. 160–164. IEEE (1982)
11. Lo, H.K.: Phys. Rev. A **56**(2), 1154 (1997)
12. Yang, Y.G., Wen, Q.Y.: J. Phys. A Math. Theor. **42**(5), 055305 (2009)
13. Liu, W., Wang, Y.B., Cui, W.: Commun. Theor. Phys. **57**, 583 (2012)
14. Chen, X.B., Xu, G., Niu, X.X., Wen, Q.Y., Yang, Y.X.: Opt. Commun. **283**(7), 1561 (2010)
15. Liu, W., Wang, Y.B., Jiang, Z.T.: Opt. Commun. **284**(12), 3160 (2011)
16. Liu, W., Wang, Y.B., Jiang, Z.T., Cao, Y.Z.: Int. J. Theor. Phys. **51**(1), 69 (2012)
17. Tseng, H.Y., Lin, J., Hwang, T.: Quantum Inf. Process. **11**(2), 373 (2012)
18. Liu, W.J., Liu, C., Wang, H.B., Liu, J.F., Wang, F., Yuan, X.M.: Int. J. Theor. Phys. **53**(6), 1804 (2014)
19. Sun, Z., Long, D.: Int. J. Theor. Phys. **52**(1), 212 (2013)
20. Guo, F.Z., Gao, F., Qin, S.J., Zhang, J., Wen, Q.Y.: Quantum Inf. Process. **12**(8), 2793 (2013)
21. Chen, X.B., Dou, Z., Xu, G., Wang, C., Yang, Y.X.: Quantum Inf. Process. **13**(1), 85 (2014)
22. Liu, X.T., Zhang, B., Wang, J., Tang, C.J., Zhao, J.J.: Quantum Inf. Process. **13**(1), 71 (2014)
23. Nie, Y.Y., Li, Y.H., Liu, J.C., Sang, M.H.: Int. J. Theor. Phys. **50**(10), 3225 (2011)
24. Juan, H., Liu, Y., Zhi-Xiang, N.: Chin. Phys. B **17**(5), 1597 (2008)
25. Liu, B., Gao, F., Jia, H.Y., Huang, W., Zhang, W.W., Wen, Q.Y.: Quantum Inf. Process. **12**(2), 887 (2013)
26. Lin, J., Tseng, H.Y., Hwang, T.: Opt. Commun. **284**(9), 2412 (2011)