Int J Theor Phys (2014) 53:2167–2176
DOI 10.1007/s10773-013-1983-7

An Efficient Protocol for the Private Comparison of Equal Information Based on Four-Particle Entangled W State and Bell Entangled States Swapping

Jian Li · Hong-Fu Zhou · Lu Jia · Ting-Ting Zhang

Received: 27 October 2013 / Accepted: 21 December 2013 / Published online: 9 January 2014

Abstract In order to enable two participants to compare the equality of their information without leaking any information about their respective private inputs, an efficient protocol with the assistance of a semi-honest third party is proposed. Different from previous protocols, this protocol based on four-particle entangled W state and Bell Entangled States swapping. One party cannot learn the other's private information. And the third party also cannot learn any information about the private information except the comparing results. Last, the correctness of the protocol is analyzed and for proving the security of the protocol, various kinds of outside attacks and participant attacks are discussed.

Keywords Quantum private comparison · Four-particle entangled W state · Bell Entangled States · Correctness · Security

1 Introduction

Since the first quantum key distribution protocol (BB84) was presented by Bennett and Brassard [1] in 1984, a lot of quantum cryptographic protocols have been presented to solve various secure problems, for example, quantum key distribution (QKD) [1–10], quantum secure multiparty computation (QSMC) [11–15], quantum secret sharing (QSS) [16–19], quantum secure direction communication (QSDC) [20–27], quantum teleportation (QT) [28, 29], quantum oblivious transfer (QOT) [30–32], quantum coin-flipping (QCF) [33], and so on.

In recent years, quantum private comparison (QPC) has become an important branch of quantum cryptography. And many protocols about QPC have been proposed. Yang et al. [34] proposed the first QPC protocol utilizing Einstein–Podolsky–Rosen (EPR) pairs. Later, Chen et al. [35] presented an efficient protocol for QPC protocol using the triplet entangled state and single-particle measurement. Liu et al. [36–39] designed four different QPC protocols based on the triplet entangled W states, Bell entangled states, χ-type genuine four-particle entangled states and GHZ entangled states, respectively. Certainly, there are

J. Li · H.-F. Zhou (✉) · L. Jia · T.-T. Zhang
School of Computer, Beijing University of Posts and Telecommunications, Beijing 100876, China
e-mail: 245237446@qq.com

many correlative protocols based on other different states, such as [40–45]. These protocols all included a third party.

Therefore, following some ideas in Refs. [34–45], an efficient QPC protocol utilizing four-particle entangled W state and Bell Entangled States is proposed. The protocol can enable two parties to compare the equality of their information and preserve their respective private inputs. The four-particle entangled W state is $|W\rangle = \frac{1}{2}(|0001\rangle + |0010\rangle + |0100\rangle + |1000\rangle)$ and Bell Entangled States is $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. In the protocol, two parties could compare two bits of information in every round and no party needs unitary operations. Similar to Refs. [34–45], the protocol includes a semi-honest third party, i.e., TP. The role of TP is to perform the protocol loyally and record all the results of its intermediate computations. It can only help two parties to get whether their private information are equal or not and cannot learn anything about the private information. And the idea of the block transmission method is used to send qubits in a batch by batch way in our protocol, which was presented in [21].

The rest of this paper is organized as follows: in Sect. 2, an efficient QPC protocol for the private comparison of equal information is described in detail. Then the correctness and security of the protocol are analyzed in Sect. 3. Finally, a brief discussion and summary are given in Sect. 4.

2 The Quantum Private Comparison of Equal Information

Before describing this protocol, we show the basic principle of four-particle entangled W state and Bell Entangled States swapping. We consider the case that one state is $|W\rangle_{1234} = \frac{1}{2}(|0001\rangle + |0010\rangle + |0100\rangle + |1000\rangle)$, the other state is $|\Phi^+\rangle_{56} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, if particles 1, 3 are measured with Bell basis, the state of the whole system evolves as follows:

$$\begin{aligned}
&|W\rangle_{1234} \otimes |\Phi^+\rangle_{56} \\
&= \frac{1}{2}\big(|\Phi^+\rangle_{12}|\Psi^+\rangle_{34}|\Phi^+\rangle_{56} + |\Psi^+\rangle_{12}|\Phi^+\rangle_{34}|\Phi^+\rangle_{56} + |\Phi^-\rangle_{12}|\Psi^+\rangle_{34}|\Phi^+\rangle_{56} \\
&\quad + |\Psi^-\rangle_{12}|\Phi^+\rangle_{34}|\Phi^+\rangle_{56}\big) \\
&= \frac{1}{4}\big[|\Phi^+\rangle_{12}\big(|\Phi^+\rangle_{35}|\Psi^+\rangle_{46} + |\Phi^-\rangle_{35}|\Psi^-\rangle_{46} + |\Psi^+\rangle_{35}|\Phi^+\rangle_{46} + |\Psi^-\rangle_{35}|\Phi^-\rangle_{46}\big) \\
&\quad + |\Psi^+\rangle_{12}\big(|\Phi^+\rangle_{35}|\Phi^+\rangle_{46} + |\Phi^-\rangle_{35}|\Phi^-\rangle_{46} + |\Psi^+\rangle_{35}|\Psi^+\rangle_{46} + |\Psi^-\rangle_{35}|\Psi^-\rangle_{46}\big) \\
&\quad + |\Phi^-\rangle_{12}\big(|\Phi^+\rangle_{35}|\Psi^+\rangle_{46} + |\Phi^-\rangle_{35}|\Psi^-\rangle_{46} + |\Psi^+\rangle_{35}|\Phi^+\rangle_{46} + |\Psi^-\rangle_{35}|\Phi^-\rangle_{46}\big) \\
&\quad + |\Psi^-\rangle_{12}\big(|\Phi^+\rangle_{35}|\Phi^+\rangle_{46} + |\Phi^-\rangle_{35}|\Phi^-\rangle_{46} + |\Psi^+\rangle_{35}|\Psi^+\rangle_{46} + |\Psi^-\rangle_{35}|\Psi^-\rangle_{46}\big)\big] \quad (1)
\end{aligned}$$

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 protocol for quantum private comparison is described as follow:

Input: Alice has a private information X, Bob has a private information Y. The binary representations of X and Y in F_{2^L} are $(x_0, x_1, \ldots, x_{L-1})$ and $(y_0, y_1, \ldots, y_{L-1})$, where $x_j, y_j \in \{0, 1\}$, $X = \sum_{j=0}^{L-1} x_j 2^j$, $Y = \sum_{j=0}^{L-1} y_j 2^j$, $j = 0, \ldots, L-1$; $2^{L-1} \le \max\{x, y\} \le 2^L$.
Output: Alice and Bob get $X = Y$ or $X \ne Y$.
A semi-honest third party: Calvin.

Supposed that two parties, Alice and Calvin, use a QKD protocol to establish a common secret key K_{AC} and two parties, Bob and Calvin, use a QKD protocol to establish a common secret keyK_{BC}.

(1) Alice (Bob) divides her (his) binary representation of $X(Y)$ into $\lceil\frac{L}{2}\rceil$ groups $G_A^1, G_A^2, \ldots, G_A^{\lceil\frac{L}{2}\rceil}(G_B^1, G_B^2, \ldots, G_B^{\lceil\frac{L}{2}\rceil})$. Each group $G_A^j(G_B^j)$ $(j = 0, \ldots, \lceil\frac{L}{2}\rceil)$ includes two binary bits in $X(Y)$. If $L \bmod 2 = 1$, Alice (Bob) adds one 0 into the last group $G_A^{\lceil\frac{L}{2}\rceil}(G_B^{\lceil\frac{L}{2}\rceil})$.

(2) Alice prepares an ordered $\lceil\frac{L}{2}\rceil$ four-particle sequence in four-particle entangled W state

$$|W\rangle = \frac{1}{2}\big(|0001\rangle + |0010\rangle + |0100\rangle + |1000\rangle\big) \tag{2}$$

We denote the $\lceil\frac{L}{2}\rceil$ four-particle sequence prepared by Alice with

$$\big[P_{A_1}^1 P_{A_2}^1 P_{B_1}^1 P_{C_1}^1, P_{A_1}^2 P_{A_2}^2 P_{B_1}^2 P_{C_1}^2, \ldots, P_{A_1}^{\lceil\frac{L}{2}\rceil} P_{A_2}^{\lceil\frac{L}{2}\rceil} P_{B_1}^{\lceil\frac{L}{2}\rceil} P_{C_1}^{\lceil\frac{L}{2}\rceil}\big] \tag{3}$$

(hereafter called sequence S_A), where the A_1, A_2, B_1, C_1 represent four particles in one four-particle entangled W state of Alice and the superscripts $1, 2, \ldots, \lceil\frac{L}{2}\rceil$ indicate the four-particle entangled W state in the sequence of Alice.

Alice divides the sequence S_A into three sequences. She takes particle A_1, A_2 from each state in S_A to form an ordered particle sequence:

$$\big[P_{A_1}^1 P_{A_2}^1, P_{A_1}^2 P_{A_2}^2, \ldots, P_{A_1}^{\lceil\frac{L}{2}\rceil} P_{A_2}^{\lceil\frac{L}{2}\rceil}\big] \tag{4}$$

which is called S_{A_1}.

She takes particle B_1 from each state in S_A to form an ordered particle sequence:

$$\big[P_{B_1}^1, P_{B_1}^2, \ldots, P_{B_1}^{\lceil\frac{L}{2}\rceil}\big] \tag{5}$$

which is called S_{B_1}.

The remaining particles inS_A

$$\big[P_{C_1}^1, P_{C_1}^2, \ldots, P_{C_1}^{\lceil\frac{L}{2}\rceil}\big] \tag{6}$$

which is called S_{C_1}.

Bob prepares an ordered $\lceil\frac{L}{2}\rceil$ EPR pairs sequence in Bell state

$$\big|\Phi^+\big\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big) \tag{7}$$

We denote the $\lceil\frac{L}{2}\rceil$ EPR pairs sequence prepared by Bob with

$$\big[P_{B_2}^1 P_{C_2}^1, P_{B_2}^2 P_{C_2}^2, \ldots, P_{B_2}^{\lceil\frac{L}{2}\rceil} P_{C_2}^{\lceil\frac{L}{2}\rceil}\big] \tag{8}$$

(hereafter called sequence S_B), where the B_2, C_2 represent two particles in one Bell state of Bob and the superscripts $1, 2, \ldots, \lceil\frac{L}{2}\rceil$ indicate the Bell State in the sequence of Bob.

Bob divides the sequence S_B into two sequences. He takes particle B_2 from each state in S_B to form an ordered particle sequence:

$$\left[P^1_{B_2}, P^2_{B_2}, \ldots, P^{\lceil \frac{L}{2} \rceil}_{B_2}\right] \tag{9}$$

which is called S_{B_2}.

The remaining particles in S_B

$$\left[P^1_{C_2}, P^2_{C_2}, \ldots, P^{\lceil \frac{L}{2} \rceil}_{C_2}\right] \tag{10}$$

which is called S_{C_2}.

(3) Alice prepares an ordered L' EPR pairs sequence in Bell state

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}\big(|01\rangle + |10\rangle\big) \tag{11}$$

We denote the L' EPR pairs sequence prepared by Alice with

$$\left[P^1_{B'_1} P^1_{C'_1}, P^2_{B'_1} P^2_{C'_1}, \ldots, P^{\lceil \frac{L}{2} \rceil}_{B'_1} P^{\lceil \frac{L}{2} \rceil}_{C'_1}\right] \tag{12}$$

(hereafter called sequence S'_A), where the B'_1, C'_1 represent two particles in one Bell state of Alice and the superscripts $1, 2, \ldots, L'$ indicate the Bell State in the sequence of Alice.

Alice divides the sequence S'_A into two sequences. She takes particle B'_1 from each state in S'_A to form an ordered particle sequence:

$$\left[P^1_{B'_1}, P^2_{B'_1}, \ldots, P^{\lceil \frac{L}{2} \rceil}_{B'_1}\right] \tag{13}$$

which is called $S_{B'_1}$.

The remaining particles in S'_A

$$\left[P^1_{C'_1}, P^2_{C'_1}, \ldots, P^{\lceil \frac{L}{2} \rceil}_{C'_1}\right] \tag{14}$$

which is called $S_{C'_1}$

Bob prepares an ordered L' EPR pairs sequence in Bell state

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big) \tag{15}$$

We denote the L' EPR pairs sequence prepared by Bob with

$$\left[P^1_{B'_2} P^1_{C'_2}, P^2_{B'_2} P^2_{C'_2}, \ldots, P^{\lceil \frac{L}{2} \rceil}_{B'_2} P^{\lceil \frac{L}{2} \rceil}_{C'_2}\right] \tag{16}$$

(hereafter called sequence S'_B), where the B'_2, C'_2 represent two particles in one Bell state of Bob and the superscripts $1, 2, \ldots, L'$ indicate the Bell State in the sequence of Bob.

Bob divides the sequence S'_B into two sequences. He takes particle B'_2 from each state in S'_B to form an ordered particle sequence:

$$\left[P^1_{B'_2}, P^2_{B'_2}, \ldots, P^{\lceil \frac{L}{2} \rceil}_{B'_2}\right] \tag{17}$$

which is called $S_{B'_2}$.

The remaining particles in S'_B

$$\left[P^1_{C'_2}, P^2_{C'_2}, \ldots, P^{\lceil \frac{L}{2} \rceil}_{C'_2}\right] \tag{18}$$

which is called $S_{C'_2}$.

Alice inserts every particle in sequence $S_{B'_1}(S_{C'_1})$ into sequence $S_{B_1}(S_{C_1})$ and gets a new sequence $S_{B^*_1}(S_{C^*_1})$. The sequence of insert positions is denoted by S_q. Alice sends $S_{B^*_1}$ to Bob and sends $S_{C^*_1}$ to Calvin. After Bob gets the $S_{B^*_1}$ and Calvin gets the $S_{C^*_1}$, Alice sends S_q to Bob.

Bob inserts every particle in sequence $S_{B'_2}(S_{C'_2})$ into sequence $S_{B_2}(S_{C_2})$ according to S_q and gets a new sequence $S_{B^*_2}(S_{C^*_2})$. Then Bob sends $S_{C^*_2}$ to Calvin.

(4) After receiving $S_{B^*_1}, S_{C^*_1}$ and $S_{C^*_2}$, Bob and Calvin check whether there is any eavesdropper in the channel by the following procedure: (a) Bob sends S_q to Calvin. (b) Bob (Calvin) chooses L' two particles from the sequence $S_{B^*_1}S_{B^*_2}(S_{C^*_1}S_{C^*_2})$ according to S_q. (c) Bob (Calvin) chooses the basis σ_z to make two particles measurement. If no eavesdropping exists, the results of Bob and Calvin should be one of the following four results, 10 and 00, 11 and 01, 00 and 10, 01 and 11. Bob and Calvin can find the existence of an eavesdropper by a predetermined threshold of error rate according to their measuring results. If the error rate exceeds the threshold they preset, they abort the scheme. Otherwise, they continue to the next step.

(5) Bob and Calvin discard the particles in $S_{B^*_1}$, $S_{B^*_2}$, $S_{C^*_1}$, $S_{C^*_2}$ which are used to check the eavesdroppers. There are two sequences owned by Bob which are denoted by $[P^1_{B_1}, P^2_{B_1}, \ldots, P^{\lceil \frac{L}{2} \rceil}_{B_1}]$, $[P^1_{B_2}, P^2_{B_2}, \ldots, P^{\lceil \frac{L}{2} \rceil}_{B_2}]$; there are two sequences owned by Calvin which are denoted by $[P^1_{C_1}, P^2_{C_1}, \ldots, P^{\lceil \frac{L}{2} \rceil}_{C_1}]$, $[P^1_{C_2}, P^2_{C_2}, \ldots, P^{\lceil \frac{L}{2} \rceil}_{C_2}]$.

For $j = 1, 2, \ldots, \lceil \frac{L}{2} \rceil$:

(5.1) Alice uses Bell basis to measure two particles $P^j_{A_1}P^j_{A_2}$ in S_{A_1}, We denote the outcome of Alice 's measurement with M^A_j. If $M^A_j = |\Phi^\pm\rangle$, then $R^A_j = 10$; $M^A_j = |\Psi^\pm\rangle$, then $R^A_j = 00$.

(5.2) Bob uses Bell basis to measure two particles $P^j_{B_1}P^j_{B_2}$ in $S_{B_1}S_{B_2}$, We denote the collapsed Bell state of Bob with M^B_j. If $M^B_j = |\Phi^+\rangle$, then $R^B_j = 00$; $M^B_j = |\Phi^-\rangle$, then $R^B_j = 01$; $M^B_j = |\Psi^+\rangle$, then $R^B_j = 10$; $M^B_j = |\Psi^-\rangle$, then $R^B_j = 11$.

(5.3) Alice (Bob) calculates $R^{A'}_j = R^A_j \oplus G^A_j(R^{B'}_j = R^B_j \oplus G^B_j)$

(6) Alice and Bob uses classic one time pad and $K_{AC}(K_{BC})$ to encrypt the binary sequence $R^{A'}_1, R^{A'}_2, \ldots, R^{A'}_{\lceil \frac{L}{2} \rceil}(R^{B'}_1, R^{B'}_2, \ldots, R^{B'}_{\lceil \frac{L}{2} \rceil})$ and sends $E_{K_{AC}}(R^{A'}_1), E_{K_{AC}}(R^{A'}_2), \ldots, E_{K_{AC}}(R^{A'}_{\lceil \frac{L}{2} \rceil})(E_{K_{BC}}(R^{B'}_1), E_{K_{BC}}(R^{B'}_2), \ldots, E_{K_{BC}}(R^{B'}_{\lceil \frac{L}{2} \rceil}))$ to Calvin.

(7) After receiving two sequences, Calvin uses $K_{AC}(K_{BC})$ to decrypt $E_{K_{AC}}(R^{A'}_1)$, $E_{K_{AC}}(R^{A'}_2), \ldots, E_{K_{AC}}(R^{A'}_{\lceil \frac{L}{2} \rceil})(E_{K_{BC}}(R^{B'}_1), E_{K_{BC}}(R^{B'}_2), \ldots, E_{K_{BC}}(R^{B'}_{\lceil \frac{L}{2} \rceil}))$ and gets $R^{A'}_1$, $R^{A'}_2, \ldots, R^{A'}_{\lceil \frac{L}{2} \rceil}(R^{B'}_1, R^{B'}_2, \ldots, R^{B'}_{\lceil \frac{L}{2} \rceil})$.

For $j = 1, 2, \ldots, \lceil \frac{L}{2} \rceil$, Calvin uses Bell basis to measure two particles $P^j_{C_1}P^j_{C_2}$ in $S_{C_1}S_{C_2}$, We denote the collapsed Bell state of Calvin with M^C_j. If $M^C_j = |\Phi^+\rangle$, then $R^C_j(r^{C1}_j r^{C2}_j) = 00$; $M^C_j = |\Phi^-\rangle$, then $R^C_j(r^{C1}_j r^{C2}_j) = 01$; $M^C_j = |\Psi^+\rangle$, then $R^C_j(r^{C1}_j r^{C2}_j) = 10$; $M^C_j = |\Psi^-\rangle$, then $R^C_j(r^{C1}_j r^{C2}_j) = 11$; Calvin calculates $R_j(r^1_j r^2_j) = R^{A'}_j \oplus R^{B'}_j$.

(8) Calvin calculates $R=\sum_{j=1}^{\lceil\frac{L}{2}\rceil}((r_j^1\oplus r_j^{C1})+(r_j^2\oplus r_j^{C2}))$ and sends R to Alice and Bob. If $R=0$, Alice and Bob know $X=Y$; otherwise, Alice and Bob know $X\neq Y$.

3 Analysis

3.1 Correctness

In this section, we show that the output of our protocol is correct. Alice has a private information X, Bob has a private information Y. The binary representations of X and Y in F_{2L} are $(x_0,x_1,\dots,x_{L-1})$ and $(y_0,y_1,\dots,y_{L-1})$, where $x_j,y_j\in\{0,1\}$, $X=\sum_{j=0}^{L-1}x_j2^j$, $Y=\sum_{j=0}^{L-1}y_j2^j$, $j=0,\dots,L-1$; $2^{L-1}\le\max\{x,y\}\le 2^L$. Alice and Bob divide their binary representations of X and Y into $\lceil\frac{L}{2}\rceil$ groups, $G_A^1,G_A^2,\dots,G_A^{\lceil\frac{L}{2}\rceil}$ and $G_B^1,G_B^2,\dots,G_B^{\lceil\frac{L}{2}\rceil}$.

For $j=1,2,\dots,\lceil\frac{L}{2}\rceil$, Alice, Bob and Calvin use four-particle entangled W state $|W\rangle_{1234}=\frac{1}{2}(|0001\rangle+|0010\rangle+|0100\rangle+|1000\rangle)$ and Bell Entangled States $|\Phi^+\rangle_{56}=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$ to compare whether G_j^A, G_j^B are equal or not. For simplicity, two cases of G_j^A, G_j^B's values are shown in Table 1 and other cases can use the same way to get. We denote Alice's measurement outcome with M_j^A, Bob's measurement outcome with M_j^B and Calvin's measurement outcome with M_j^C. The represents of M_j^A, M_j^B, M_j^C are denoted as R_j^A, R_j^B, $R_j^C(r_j^{C1}r_j^{C2})$. Alice agrees that $|\Phi^\pm\rangle$ represent information 10; $|\Psi^\pm\rangle$ represent information 00. Bob and Calvin agree that $|\Phi^+\rangle$ represent information 00; $|\Phi^-\rangle$ represent information 01; $|\Psi^+\rangle$ represent information 10; $|\Psi^-\rangle$ represent information 11.

The result $R_j^{A'}=R_j^A\oplus G_j^A$ and $R_j^{B'}=R_j^B\oplus G_j^B$ are send to Calvin. After doing $R_j(r_j^1r_j^2)=R_j^{A'}\oplus R_j^{B'}$ and $R_j'=(r_j^1\oplus r_j^{C1})+(r_j^2\oplus r_j^{C2})$, Calvin gets the result of the comparison between G_j^A and G_j^B. If $R_j'=0$, then $G_j^A=G_j^B$; otherwise $G_j^A\neq G_j^B$. After comparing every group of two binary bits G_j^A, G_j^B $(j=1,2,\dots,\lceil\frac{L}{2}\rceil)$ in X, Y, if $R=\sum_{j=1}^{\lceil\frac{L}{2}\rceil}((r_j^1\oplus r_j^{C1})+(r_j^2\oplus r_j^{C2}))=0$, Calvin knows $X=Y$; if $R=\sum_{j=1}^{\lceil\frac{L}{2}\rceil}((r_j^1\oplus r_j^{C1})+(r_j^2\oplus r_j^{C2}))\neq 0$, Calvin knows $X\neq Y$.

3.2 Security

In this section, the security of the protocol is analyzed. Firstly, the outside attack is invalid to our protocol is presented. Any information about the private information and the comparison result of private inputs will not be leaked out. Secondly, we show that the Alice and Bob cannot get any information about the private information of each other and the semi-honest third party, Calvin, also cannot get any information about the private information of Alice and Bob.

3.2.1 Outside Attack

We analyze the possibility of the outside eavesdropper to gain information about X and Y in every step of protocol.

In steps 1, 2, 5, 7, 8, there is not any information to transmit. In step 3, the outside eavesdropper can attack the quantum channel when Alice (Bob) sent $S_{B_1^*}$, $S_{C_1^*}(S_{C_2^*})$ to Bob and Calvin (Calvin). In step 4, we executed eavesdropper checking process and several kinds of outside attacks, such as the intercept-resend attack, the measure-resend attack, were detected

Table 1 Two cases of G_j^A, G_j^B's values

G_j^A	G_j^B	M_j^A	M_j^B	R_j^A	R_j^B	$R_j^{A'}$	$R_j^{B'}$	$R_j(r_j^1 r_j^2)$	M_j^C	$R_j^C(r_j^{C1} r_j^{C2})$	R_j'
00	00	$\|\Phi^+\rangle$	$\|\Phi^+\rangle$	10	00	10	00	10	$\|\Psi^+\rangle$	10	0
		$\|\Phi^+\rangle$	$\|\Phi^-\rangle$	10	01	10	01	11	$\|\Psi^-\rangle$	11	0
		$\|\Phi^+\rangle$	$\|\Psi^+\rangle$	10	10	10	10	00	$\|\Phi^+\rangle$	00	0
		$\|\Phi^+\rangle$	$\|\Psi^-\rangle$	10	11	10	11	01	$\|\Phi^-\rangle$	01	0
		$\|\Phi^-\rangle$	$\|\Phi^+\rangle$	10	00	10	00	10	$\|\Psi^+\rangle$	10	0
		$\|\Phi^-\rangle$	$\|\Phi^-\rangle$	10	01	10	01	11	$\|\Psi^-\rangle$	11	0
		$\|\Phi^-\rangle$	$\|\Psi^+\rangle$	10	10	10	10	00	$\|\Phi^+\rangle$	00	0
		$\|\Phi^-\rangle$	$\|\Psi^-\rangle$	10	11	10	11	01	$\|\Phi^-\rangle$	01	0
		$\|\Psi^+\rangle$	$\|\Phi^+\rangle$	00	00	00	00	00	$\|\Phi^+\rangle$	00	0
		$\|\Psi^+\rangle$	$\|\Phi^-\rangle$	00	01	00	01	01	$\|\Phi^-\rangle$	01	0
		$\|\Psi^+\rangle$	$\|\Psi^+\rangle$	00	10	00	10	10	$\|\Psi^+\rangle$	10	0
		$\|\Psi^+\rangle$	$\|\Psi^-\rangle$	00	11	00	11	11	$\|\Psi^-\rangle$	11	0
		$\|\Psi^-\rangle$	$\|\Phi^+\rangle$	00	00	00	00	00	$\|\Phi^+\rangle$	00	0
		$\|\Psi^-\rangle$	$\|\Phi^-\rangle$	00	01	00	01	01	$\|\Phi^-\rangle$	01	0
		$\|\Psi^-\rangle$	$\|\Psi^+\rangle$	00	10	00	10	10	$\|\Psi^+\rangle$	10	0
		$\|\Psi^-\rangle$	$\|\Psi^-\rangle$	00	11	00	11	11	$\|\Psi^-\rangle$	11	0
10	01	$\|\Phi^+\rangle$	$\|\Phi^+\rangle$	10	00	00	01	01	$\|\Psi^+\rangle$	10	2
		$\|\Phi^+\rangle$	$\|\Phi^-\rangle$	10	01	00	00	00	$\|\Psi^-\rangle$	11	2
		$\|\Phi^+\rangle$	$\|\Psi^+\rangle$	10	10	00	11	11	$\|\Phi^+\rangle$	00	2
		$\|\Phi^+\rangle$	$\|\Psi^-\rangle$	10	11	00	10	10	$\|\Phi^-\rangle$	01	2
		$\|\Phi^-\rangle$	$\|\Phi^+\rangle$	10	00	00	01	01	$\|\Psi^+\rangle$	10	2
		$\|\Phi^-\rangle$	$\|\Phi^-\rangle$	10	01	00	00	00	$\|\Psi^-\rangle$	11	2
		$\|\Phi^-\rangle$	$\|\Psi^+\rangle$	10	10	00	11	11	$\|\Phi^+\rangle$	00	2
		$\|\Phi^-\rangle$	$\|\Psi^-\rangle$	10	11	00	10	10	$\|\Phi^-\rangle$	01	2
		$\|\Psi^+\rangle$	$\|\Phi^+\rangle$	00	00	10	01	11	$\|\Phi^+\rangle$	00	2
		$\|\Psi^+\rangle$	$\|\Phi^-\rangle$	00	01	10	00	10	$\|\Phi^-\rangle$	01	2
		$\|\Psi^+\rangle$	$\|\Psi^+\rangle$	00	10	10	11	01	$\|\Psi^+\rangle$	10	2
		$\|\Psi^+\rangle$	$\|\Psi^-\rangle$	00	11	10	10	00	$\|\Psi^-\rangle$	11	2
		$\|\Psi^-\rangle$	$\|\Phi^+\rangle$	00	00	10	01	11	$\|\Phi^+\rangle$	00	2
		$\|\Psi^-\rangle$	$\|\Phi^-\rangle$	00	01	10	00	10	$\|\Phi^-\rangle$	01	2
		$\|\Psi^-\rangle$	$\|\Psi^+\rangle$	00	10	10	11	01	$\|\Psi^+\rangle$	10	2
		$\|\Psi^-\rangle$	$\|\Psi^-\rangle$	00	11	10	10	00	$\|\Psi^-\rangle$	11	2

with nonzero probability. In step 6, Alice and Bob used the quantum-one-time pad and sent $R_1^{A'}, R_2^{A'}, \ldots, R_{\lceil \frac{L}{2} \rceil}^{A'}$ ($R_1^{B'}, R_2^{B'}, \ldots, R_{\lceil \frac{L}{2} \rceil}^{B'}$) to Calvin. The outside eavesdroppers also cannot get $R_1^{A'}, R_2^{A'}, \ldots, R_{\lceil \frac{L}{2} \rceil}^{A'}$ and $R_1^{B'}, R_2^{B'}, \ldots, R_{\lceil \frac{L}{2} \rceil}^{B'}$ in this step.

So in every step of our protocol, the outside eavesdropper cannot eavesdrop any information about X and Y.

3.2.2 Participant Attack

The term “participant attack”, which emphasizes that the attacks from dishonest users are generally more powerful and should be paid more attention to, is first proposed by Gao et al. in Ref. [46] and has attracted much attention in the cryptanalysis of quantum cryptography [47–54]. In this section, we analyze the possibility of the three parties to get information about X and Y.

Case 1: Alice attempts to obtain Bob’s private information Y.

In our protocol, Alice gets nothing from Bob. So she cannot infer any information about Bob’s private information Y.

Case 2: Bob attempts to obtain Alice’s private information X.

In our protocol, Bob only get $S_{B_1^*}$ from Alice. $S_{B_1^*}$ isn’t relevant to Alice’s private information, so he cannot deduce any information about Alice’s private information X.

Case 3: Calvin attempts to obtain the private information X, Y.

Calvin can only infer private information X, Y from $R_j(r_j^1 r_j^2) = R_j^{A'} \oplus R_j^{B'} = (R_j^A \oplus G_j^A) \oplus (R_j^B \oplus G_j^B)$ and the measurement result M_j^C of $(P_{C_1}^j P_{C_2}^j)$. Because these measurement results have the same probability which is shown in Table 1, Calvin cannot deduce G_j^A, G_j^B from R_j.

In our protocol, Calvin knows the comparing results of each group. But, only with these results, he also cannot deduce the value of every group. So Calvin cannot learn the private information X, Y.

4 Discussion and Conclusions

In summary, we proposed a new QPC protocol based on four-particle entangled W state and Bell Entangled States swapping. Two parties can know whether their private information X and Y are equal or not through the help of a semi-honest Calvin. And they cannot learn private information owned by each other. Calvin also cannot learn any information about the private information X and Y except the comparing results. Comparing to others protocols, we can not only withstand outside attacks and protect the privacy of X and Y, but also not use the Pauli local unitary operation.

Acknowledgements This work is supported by the National Natural Science Foundation of China (Grant No. 61100205). This work is also supported by Project 2013RC0307 of the Fundamental Research Funds for the Central Universities.

References

1. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing, pp. 175–179 (1984)
2. Ekert, A.K.: Quantum cryptography based on Bell’s theorem. Phys. Rev. Lett. **67**, 661–663 (1991)
3. Bennett, C.H., Brassard, G., Mermin, N.D.: Quantum cryptography without Bell’s theorem. Phys. Rev. Lett. **67**, 557–559 (1992)
4. Deng, F.G., Long, G.L.: Controlled order rearrangement encryption for quantum key distribution. Phys. Rev. A **68**, 042315 (2003)
5. Wen, K., Long, G.L.: Modified Bennett-Brassard 1984 quantum key distribution protocol with two-way classical communications. Phys. Rev. A **72**, 22336 (2005)

6. Gao, F., Guo, F.Z., Wen, Q.Y., Zhu, F.C.: Quantum key distribution without alternative measurements and rotations. Phys. Lett. A **349**, 53–58 (2006)
7. Gao, F., Guo, F.Z., Wen, Q.Y., Zhu, F.C.: Quantum key distribution by constructing nonorthogonal states with Bell states. Int. J. Mod. Phys. B **24**, 4611–4618 (2010)
8. Guo, F.Z., Gao, F., Wen, Q.Y., Zhu, F.C.: A two-step channel-encrypting quantum key distribution protocol. Int. J. Quantum Inf. **8**, 1013–1022 (2010)
9. Lu, Z.X., Yu, L., Li, K., et al.: Reverse reconciliation for continuous variable quantum key distribution. Sci. China, Phys. Mech. Astron. **53**, 100–105 (2010)
10. Tan, Y.G., Cai, Q.Y.: Practical decoy state quantum key distribution with finite resource. Eur. Phys. J. D **56**, 449–455 (2010)
11. Hillery, M., Bužek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A **59**, 1829–1834 (1999)
12. Lin, S., Wen, Q.Y., Qin, S.J., et al.: Multiparty quantum secret sharing with collective eavesdropping-check. Opt. Commun. **282**, 4455–4459 (2009)
13. Li, Q., Long, D.Y., Chan, W.H., et al.: Sharing a quantum secret without a trusted party. Quantum Inf. Process. **10**, 97–106 (2011)
14. Jia, H.Y., Wen, Q.Y., Song, T.T., et al.: Quantum protocol for millionaire problem. Opt. Commun. **284**, 545–549 (2011)
15. Tsai, C.W., Hwang, T.: Multi-party quantum secret sharing based on two special entangled states. Sci. China, Phys. Mech. Astron. **55**, 460–464 (2012)
16. Karlsson, A., Koashi, M., Imoto, N.: Quantum entanglement for secret sharing and secret splitting. Phys. Rev. A **59**, 162–168 (1999)
17. Xiao, L., Long, G.L., Deng, F.G., Pan, J.W.: Efficient multiparty quantum-secret-sharing schemes. Phys. Rev. A **69**, 162–168 (2004)
18. Deng, F.G., Zhou, H.Y., Long, G.L.: Bidirectional quantum secret sharing and secret splitting with polarized single photons. Phys. Lett. A **337**, 329–334 (2005)
19. Sun, Y., Wen, Q.Y., Gao, F., Chen, X.B., Zhu, F.C.: Multiparty quantum secret sharing based on Bell measurement. Opt. Commun. **282**, 3647–3651 (2009)
20. Boström, K., Felbinger, T.: Deterministic secure direct communication using entanglement. Phys. Rev. Lett. **89**, 187902 (2002)
21. 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)
22. Deng, F.G., Long, G.L.: Secure direct communication with a quantum one-time pad. Phys. Rev. A **69**, 052319 (2004)
23. 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)
24. Wang, J., Zhang, Q., Tang, C.J.: Quantum secure communication scheme with W state. Commun. Theor. Phys. **48**, 637–640 (2007)
25. Long, G.L., Deng, F.G., Wang, C., et al.: Quantum secure direct communication and deterministic secure quantum communication. Front. Phys. China **2**, 251–272 (2007)
26. Lin, S., Wen, Q.Y., Gao, F., Zhu, F.C.: Quantum secure direct communication with χ-type entangled states. Phys. Rev. A **78**, 064304 (2008)
27. Qin, S.J., Gao, F., Wen, Q.Y., Zhu, F.C.: Robust quantum secure direct communication over collective rotating channel. Commun. Theor. Phys. **53**, 645–647 (2010)
28. Bennett, C.H., et al.: Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Phys. Rev. Lett. **70**, 1895–1899 (1993)
29. Bouwmeester, D., Pan, J.W., et al.: Experimental quantum teleportation. Nature **390**, 575–579 (1997)
30. Kerenidis, I., Wehner, S.: Long distance quantum cryptography made simple. Quantum Inf. Comput. **12**(5–6), 448–460 (2012)
31. Sikora, J.: On the existence of loss-tolerant quantum oblivious transfer protocols. Quantum Inf. Comput. **12**(7–8), 609–619 (2012)
32. Chailloux, A., Kerenidis, I., Sikora, J.: Lower bounds for quantum oblivious transfer. Quantum Inf. Comput. **13**(1–2), 158–177 (2013)
33. Ma, J.J., Guo, F.Z., Yang, Q., et al.: Semi-loss-tolerant strong coin flipping protocol using EPR pairs. Quantum Inf. Comput. **12**(5–6), 490–501 (2012)
34. 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)
35. Chen, X.B., Xu, G., Niu, X.X.: An efficient protocol for the private comparison of equal information based on the triplet entangled state and single-particle measurement. Opt. Commun. **283**, 1561–1565 (2010)
36. Liu, W., Wang, Y.B., Jiang, Z.T., et al.: A protocol for the quantum private comparison of equality with χ-type state. Int. J. Theor. Phys. **51**, 69–77 (2012)

37. Liu, W., Wang, Y.B.: Quantum private comparison based on GHZ entangled states. Int. J. Theor. Phys. **51**, 3596–3604 (2012)
38. Liu, W., Wang, Y.B., Jiang, Z.T.: An efficient protocol for the quantum private comparison of equality with W state. Opt. Commun. **284**, 3160–3163 (2011)
39. Liu, W., Wang, Y.B., Cui, W.: Quantum private comparison protocol based on Bell entangled states. Commun. Theor. Phys. **57**, 583–588 (2012)
40. Lin, J., Tseng, H.Y., Hwang, T.: Intercept–resend attacks on Chen et al.'s quantum private comparison protocol and the improvements. Opt. Commun. **284**, 2412–2414 (2011)
41. Liu, B., Gao, F., Jia, H.Y., et al.: Efficient quantum private comparison employing single photons and collective detection. Quantum Inf. Process. **12**, 887–897 (2012)
42. Tseng, H.Y., Lin, J., Hwang, T.: New quantum private comparison protocol using EPR pairs. Quantum Inf. Process. **11**, 373–384 (2012)
43. Lin, S., Sun, Y., Liu, X.F., et al.: Quantum private comparison protocol with d-dimensional Bell states. Quantum Inf. Process. **12**, 559–568 (2013)
44. Sun, Z., Long, D.: Quantum private comparison protocol based on cluster states. Int. J. Theor. Phys. **52**, 212–218 (2013)
45. Zhang, W.W., Li, D., Song, T.T., et al.: Quantum private comparison based on quantum search algorithm. Int. J. Theor. Phys. **52**, 1466–1473 (2013)
46. Gao, F., Qin, S.J., Wen, Q.Y., et al.: A simple participant attack on the Bradler-Dusek protocol. Quantum Inf. Comput. **7**, 329 (2007)
47. Lin, S., Gao, F., Guo, F.Z., et al.: Comment on "Multiparty quantum secret sharing of classical messages based on entanglement swapping". Phys. Rev. A **76**, 036301 (2007)
48. Song, T.T., Zhang, J., Gao, F., et al.: Participant attack on quantum secret sharing based on entanglement swapping. Chin. Phys. B **18**, 1333 (2009)
49. Gao, F., Wen, Q.Y., Zhu, F.C.: Comment on "Quantum exam". Phys. Lett. A **350**, 174 (2006)
50. Gao, F., Qin, S.J., Wen, Q.Y., et al.: Cryptanalysis of multiparty controlled quantum secure direct communication using Greenberger-Horne-Zeilinger state. Opt. Commun. **283**, 192 (2010)
51. Guo, F.Z., Qin, S.J., Gao, F., et al.: Participant attack on a kind of MQSS schemes based on entanglement swapping. Eur. Phys. J. D **56**, 445 (2010)
52. Lin, S., Wen, Q.Y., Gao, F., et al.: Improving the security of multiparty quantum secret sharing based on the improved Bostrom-Felbinger protocol. Opt. Commun. **281**, 4553 (2008)
53. Qin, S.J., Gao, F., Wen, Q.Y., et al.: Cryptanalysis of the Hillery-Buzek-Berthiaume quantum secretsharing protocol. Phys. Rev. A **76**, 062324 (2007)
54. Gao, F., Guo, F.Z., Wen, Q.Y., et al.: Comment on "Experimental demonstration of a quantum protocol for byzantine agreement and liar detection". Phys. Rev. Lett. **101**, 208901 (2008)