Quantum Information Processing (2019) 18:158
https://doi.org/10.1007/s11128-019-2266-x

Efficient quantum private comparison protocol based on the entanglement swapping between four-qubit cluster state and extended Bell state

Chaoyang Li[1,2] · Xiubo Chen[1] · Hengji Li[2] · Yuguang Yang[3] · Jian Li[2]

Received: 26 April 2018 / Accepted: 28 March 2019 / Published online: 9 April 2019

Abstract
Quantum private comparison (QPC) protocol can guarantee the two participants to compare the equality of their private information without leaking them. Based on the entanglement swapping between the four-qubit cluster state and extended Bell state, an efficient QPC protocol has been proposed. Three bits of the secret inputs have been compared in each comparison time, which improves the efficiency compared with the previous QPC protocols' one or two bits. Then, based on a random sequence pre-shared between the two participants, the semi-honest third party can only execute the protocol's process without obtaining the information of the participants' secrets and comparison results. Last, various kinds of attacks have been analyzed, which show that the proposed protocol is secure against the outside and participants attacks.

Keywords Quantum private comparison · Entanglement swapping · Cluster state · Semi-honest third party

1 Introduction

Benett and Brassard [1] proposed the first quantum key distribution protocol, which was commonly called BB84. From then on, along with the development of quantum cryptography [2], there exists more and more interesting applications, such as quantum key distribution [3–6], quantum secret sharing [7–9], quantum digital signature [10–14], and so on.

✉ Xiubo Chen
flyover100@163.com

1 Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China

2 School of Computer Science, Beijing University of Posts and Telecommunications, Beijing 100876, China

3 Faculty of Information Technology, Beijing University of Technology, Beijing 100124, China

The concept of the secure multiparty computation (SMC) was first proposed by Yao, which was mainly used to implement the following tasks [15,16]: In a distributed network of mutual distrust, each user can obtain the result of a function by cooperating without leaking their private information. The SMC problem is used to research in classical setting, but Shor [17] pointed out that it can be solved by models based on quantum setting with higher efficiency. Since then, more and more special SMC problems have been solved in quantum setting, such as quantum protocol for anonymous voting and surveying [18,19], quantum anonymous ranking [20,21], quantum auction [22–24], quantum protocol for millionaire problem [25], and so on.

In recent years, the design and analysis of QPC protocols have attracted many interests and attentions. The first QPC protocol was proposed by Yang [26]. Straight after, lots of QPC protocols have been presented based on different entangled states, such as Bell states, GHZ states, W states, and χ-type states [27–39].

In this paper, we propose an efficient QPC protocol, which can compare three bits in each comparison time and decrease more comparison times. This protocol is based on the entanglement swapping of the four-qubit cluster state and extended Bell state (χ state). For better finishing the task, the semi-honest TP who called Charlie is introduced to help the implementation of this comparison. But he only can obey the duty to perform the rules of the protocol and cannot obtain anything about the comparison results and the participants' private information. Furthermore, with the decoy photons and preshared random sequence, it can detect the malicious eavesdropper Eve and forbid him knowing the actual comparison results and the information of the secret inputs.

The rest of this paper is organized as follows: In Sect. 2, an efficient QPC protocol is described in detail. In Sect. 3, the security of the proposed protocol is analyzed. Then, the efficiency comparison is presented in Sect. 4. At last, conclusion is given in Sect. 5.

2 The QPC protocol

In Reference [40], a general form of an N-qubit cluster was given as follows:

$$|C_N\rangle = \frac{1}{2^{N/2}} \otimes_{a=1}^{N} \left(|0\rangle_a \delta_z^{(a+1)} + |1\rangle\right) \tag{1}$$

with the convention $\delta_z^{(N+1)} = 1$. And these states have a strong violation of local reality and are shown to be robust against decoherence [41,42]. In the case of two- and three-partite scenarios, this cluster state is the same as the Bell and GHZ states, respectively. In this paper, we choose the following four-qubit cluster state, where $N = 4$ in Eq. (1):

$$|C_4\rangle_{1234} = \frac{1}{2}(|0000\rangle + |0110\rangle + |1001\rangle - |1111\rangle) \tag{2}$$

And the whole system is the swapping of the cluster state $|C_4\rangle_{1234}$ and the extended Bell state $|\chi^+\rangle_{56}$. Here the extended Bell state is one of the basis $\{|\chi^\pm\rangle, |\omega^\pm\rangle\}$, which

can be derived by the Hadamard gate from the Bell basis $\{|\phi^{\pm}\rangle = (|00\rangle \pm |11\rangle)/\sqrt{2}$, $|\psi^{\pm}\rangle = (|01\rangle \pm |10\rangle)/\sqrt{2}\}$.

$$\begin{aligned}
|\chi^{+}\rangle &= \frac{|\phi^{-}\rangle + |\psi^{+}\rangle}{\sqrt{2}} = \frac{|00\rangle - |11\rangle + |01\rangle + |10\rangle}{2} \\
|\chi^{-}\rangle &= \frac{|\phi^{+}\rangle + |\psi^{-}\rangle}{\sqrt{2}} = \frac{|00\rangle + |11\rangle + |01\rangle - |10\rangle}{2} \\
|\omega^{+}\rangle &= \frac{|\phi^{+}\rangle - |\psi^{-}\rangle}{\sqrt{2}} = \frac{|00\rangle + |11\rangle - |01\rangle + |10\rangle}{2} \\
|\omega^{-}\rangle &= \frac{|\phi^{-}\rangle - |\psi^{+}\rangle}{\sqrt{2}} = \frac{|00\rangle - |11\rangle - |01\rangle - |10\rangle}{2}
\end{aligned} \tag{3}$$

Then, the entanglement swapping principle of the states $|C_4\rangle_{1234}$ and $|\chi^{+}\rangle_{56}$ is given below:

$$\begin{aligned}
&|C_4\rangle_{1234} \otimes |\chi^{+}\rangle_{56} \\
&= \frac{1}{2}(|0000\rangle + |0110\rangle + |1001\rangle - |1111\rangle)_{1234} \otimes \frac{1}{2}(|00\rangle - |11\rangle + |01\rangle + |10\rangle)_{56} \\
&= \frac{1}{4\sqrt{2}}(|00\rangle_{12} \otimes ((|\phi^{+}\rangle_{35} + |\phi^{-}\rangle_{35}) \otimes (|\chi^{+}\rangle_{46} + |\chi^{-}\rangle_{46}) \\
&\quad + (|\psi^{+}\rangle_{35} + |\psi^{-}\rangle_{35}) \otimes (|\omega^{+}\rangle_{46} + |\omega^{-}\rangle_{46})) \\
&\quad + |01\rangle_{12} \otimes ((|\psi^{+}\rangle_{35} - |\psi^{-}\rangle_{35}) \otimes (|\chi^{+}\rangle_{46} + |\chi^{-}\rangle_{46}) \\
&\quad + (|\phi^{+}\rangle_{35} - |\phi^{-}\rangle_{35}) \otimes (|\omega^{+}\rangle_{46} + |\omega^{-}\rangle_{46})) \\
&\quad + |10\rangle_{12} \otimes ((|\phi^{+}\rangle_{35} + |\phi^{-}\rangle_{35}) \otimes (|\omega^{+}\rangle_{46} - |\omega^{-}\rangle_{46}) \\
&\quad + (|\psi^{+}\rangle_{35} + |\psi^{-}\rangle_{35}) \otimes (|\chi^{+}\rangle_{46} - |\chi^{-}\rangle_{46})) \\
&\quad - |11\rangle_{12} \otimes ((|\psi^{+}\rangle_{35} - |\psi^{-}\rangle_{35}) \otimes (|\omega^{+}\rangle_{46} - |\omega^{-}\rangle_{46}) \\
&\quad + (|\phi^{+}\rangle_{35} - |\phi^{-}\rangle_{35}) \otimes (|\chi^{+}\rangle_{46} - |\chi^{-}\rangle_{46}))) \\
&= \frac{1}{4}(|\phi^{+}\rangle_{12}(|\phi^{+}\rangle_{35}|\chi^{-}\rangle_{46} + |\phi^{-}\rangle_{35}|\chi^{+}\rangle_{46} + |\psi^{+}\rangle_{35}|\omega^{-}\rangle_{46} + |\psi^{-}\rangle_{35}|\omega^{+}\rangle_{46}) \\
&\quad + |\phi^{-}\rangle_{12}(|\phi^{+}\rangle_{35}|\chi^{+}\rangle_{46} + |\phi^{-}\rangle_{35}|\chi^{-}\rangle_{46} + |\psi^{+}\rangle_{35}|\omega^{+}\rangle_{46} + |\psi^{-}\rangle_{35}|\omega^{-}\rangle_{46}) \\
&\quad + |\psi^{+}\rangle_{12}(|\psi^{+}\rangle_{35}|\chi^{+}\rangle_{46} - |\psi^{-}\rangle_{35}|\chi^{-}\rangle_{46} + |\phi^{+}\rangle_{35}|\omega^{+}\rangle_{46} - |\phi^{-}\rangle_{35}|\omega^{-}\rangle_{46}) \\
&\quad + |\psi^{-}\rangle_{12}(|\psi^{+}\rangle_{35}|\chi^{-}\rangle_{46} - |\psi^{-}\rangle_{35}\upsilon\chi^{+}\rangle_{46} + |\phi^{+}\rangle_{35}|\omega^{-}\rangle_{46} - |\phi^{-}\rangle_{35}|\omega^{+}\rangle_{46})) \\
&= \frac{1}{4}(|\phi^{+}\rangle_{12}(|\chi^{-}\rangle_{35}|\phi^{+}\rangle_{46} + |\chi^{+}\rangle_{35}|\phi^{-}\rangle_{46} + |\omega^{-}\rangle_{35}|\psi^{+}\rangle_{46} + |\omega^{+}\rangle_{35}|\psi^{-}\rangle_{46}) \\
&\quad + |\phi^{-}\rangle_{12}(|\chi^{+}\rangle_{35}|\phi^{+}\rangle_{46} + |\chi^{-}\rangle_{35}|\phi^{-}\rangle_{46} + |\omega^{+}\rangle_{35}|\psi^{+}\rangle_{46} + |\omega^{-}\rangle_{35}||\psi^{-}\rangle_{46}) \\
&\quad + |\psi^{+}\rangle_{12}(|\chi^{+}\rangle_{35}|\psi^{+}\rangle_{46} - |\chi^{-}\rangle_{35}|\psi^{-}\rangle_{46} + |\omega^{+}\rangle_{35}|\phi^{+}\rangle_{46} - |\omega^{-}\rangle_{35}|\phi^{-}\rangle_{46}) \\
&\quad + |\psi^{-}\rangle_{12}(|\chi^{-}\rangle_{35}|\psi^{+}\rangle_{46} - |\chi^{+}\rangle_{35}|\psi^{-}\rangle_{46} + |\omega^{-}\rangle_{35}|\phi^{+}\rangle_{46} - |\omega^{+}\rangle_{35}|\phi^{-}\rangle_{46}))
\end{aligned} \tag{4}$$

The detail steps of the proposed 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 F_{2^L} 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 $X = \sum_{i=0}^{L-1} x_i 2^i$, $Y = \sum_{i=0}^{L-1} y_i 2^i$, $2^L - 1 < \max\{X, Y\} < 2^L$.

Output: Whether $X = Y$ or not.

Charlie is a semi-honest third party, who helps the two participants Alice and Bob to compare their secrets, but he cannot obtain anything from the processing executed with Alice and Bob in the protocol. Beforehand, Alice(Bob) and Charlie use a secure QKD protocol to establish a common secret key $K_{AC}(K_{BC})$, respectively. And the two participants, Alice and Bob also share a secret key sequence $K : (k_0, k_1, \ldots, k_{L-1}), k_i \in \{0, 1\}, i = 0, 1, \ldots, (L-1)$ through a secure QKD protocol.

2.1 Preparing step

(1) Alice(Bob) divides the N-bit binary string $X(Y)$ into $\lceil N/3L \rceil$ groups, each group having $3L$ bits. If $N \bmod 3 \neq 1$, Alice(Bob) always adds $3L - (N \bmod 3L)$ 0 at the end of the N-bit binary string $X(Y)$. Then, $X = A_{\lceil N/3L \rceil - 1} \ldots A_1 A_0$, $Y = B_{\lceil N/3L \rceil - 1} \ldots B_1 B_0$.

$$A_j = \left(x_j^{3L-1}, \ldots, x_j^1, x_j^0\right), \quad B_j = \left(y_j^{3L-1}, \ldots, y_j^1, y_j^0\right), \\ j = 0, 1, \ldots, \lceil N/3L \rceil - 1 \tag{5}$$

(2) For each group $A_j(B_j)$, Alice and Bob form every three adjacent bits into a pair $Q_A^i = \left(x_j^{3i}, x_j^{3i+1}, x_j^{3i+2}\right)$, $Q_B^i = \left(y_j^{3i}, y_j^{3i+1}, y_j^{3i+2}\right)$

$$A_j = \left(Q_A^{L-1}, \ldots, Q_A^1, Q_A^0\right), \quad B_j = \left(Q_B^{L-1}, \ldots, Q_B^1, Q_B^0\right) \tag{6}$$

(3) In the jth round of the comparison, Charlie prepares an ordered sequence $S_1(S_2)$ which consists of L ordered $|C_4\rangle_{1234}$ ($|\chi^+\rangle_{56}$) states.

$$\begin{aligned} S_1&: \left[P_1^0 P_2^0 P_3^0 P_4^0, P_1^1 P_2^1 P_3^1 P_4^1, \ldots, P_1^{L-1} P_2^{L-1} P_3^{L-1} P_4^{L-1}\right] \\ S_2&: \left[P_5^0 P_6^0, P_5^1 P_6^1, \ldots, P_5^{L-1} P_6^{L-1}\right] \end{aligned} \tag{7}$$

where the subscripts {1,2,3,4 (5,6)} denote the different particle in each quantum state $S_1(S_2)$, and the superscripts $\{0, 1, \ldots, L-1\}$ denote the ith entangle quantum state prepared by Charlie.

(4) Charlie takes the first two particles of all $|C_4\rangle_{1234}$ states in S_1 to form an ordered sequence S_C.

$$S_C: \left[P_1^0 P_2^0, P_1^1 P_2^1, \ldots, P_1^{L-1} P_2^{L-1}\right] \tag{8}$$

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

$M_A^i(M_B^i)$	$\|\phi^+\rangle$	$\|\phi^-\rangle$	$\|\psi^+\rangle$	$\|\psi^-\rangle$	$\|\chi^+\rangle$	$\|\chi^-\rangle$	$\|\omega^+\rangle$	$\|\omega^-\rangle$
$C_A^i(C_B^i)$	000	001	010	011	100	101	110	111

Charlie takes the third particle of all $|C_4\rangle_{1234}$ states in S_1 and the first particle of all $|\chi^+\rangle_{56}$ states in S_2 to form an ordered sequence S_A.

$$S_A: \left[P_3^0 P_5^0, P_3^1 P_5^1, \ldots, P_3^{L-1} P_5^{L-1}\right] \tag{9}$$

Charlie takes the fourth particle of all $|C_4\rangle_{1234}$ states in S_1 and the second particle of all $|\chi^+\rangle_{56}$ states in S_2 to form an ordered sequence S_B.

$$S_B: \left[P_4^0 P_6^0, P_4^1 P_6^1, \ldots, P_4^{L-1} P_6^{L-1}\right] \tag{10}$$

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

2.2 Checking step

When Alice(Bob) receives the sequence $S'_A(S'_B)$, Charlie announces the positions and measuring basis of the decoy photons D_A and D_B. Then, Alice(Bob) measures the decoy particles with the corresponding measuring basis for eavesdropping detection. If the error rate exceeds a suitable threshold, Charlie will terminate this communication and restart from the preparing step. Otherwise, the protocol goes to the next step.

2.3 Coding step

(1) Alice(Bob) first recovers $S_A(S_B)$ by discarding the decoy photons. Then, according to the pre-shared sequence K, Alice(Bob) calculates $K = \bigoplus_{i=0}^{L-1} k_i$, the symbol $\bigoplus$ denotes the bit-wise exclusive-OR. Then, if $K = 0$, she(he) chooses the basis $\{|\phi^{\pm}\rangle, |\psi^{\pm}\rangle\}$ ($\{|\chi^{\pm}\rangle, |\omega^{\pm}\rangle\}$) to measure the ith pair $P_3^i P_5^i$ ($P_4^i P_6^i$) in $S_A(S_B)$, and if $K = 1$, she(he) chooses the basis $\{|\chi^{\pm}\rangle, |\omega^{\pm}\rangle\}$ ($\{|\phi^{\pm}\rangle, |\psi^{\pm}\rangle\}$). And we denote the measurement results with $M_A^i(M_B^i)$. After the measurement, according to Table 1, Alice and Bob will obtain a three-bit value C_A^i and C_B^i, respectively.

(2) Alice(Bob) calculates $R_A^i = Q_A^i \bigoplus C_A^i$ ($R_B^i = Q_B^i \bigoplus C_B^i$), where $Q_A^i(Q_B^i)$ is derived from Preparing step (2). Then, Alice(Bob) encrypts the sequence $R_A^0 R_A^1, \ldots, R_A^{L-1}$ ($R_B^0 R_B^1, \ldots, R_B^{L-1}$) with $K_{AC}(K_{BC})$ and sends it to Charlie by quantum-one-time pad.

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

$M_C^i \backslash R_{AB}^i$	000	001	010	011	100	101	110	111
$\|\phi^+\rangle$	$\neq$	$\neq$	$\neq$	$\neq$	$\neq$	=	$\neq$	$\neq$
$\|\phi^-\rangle$	$\neq$	$\neq$	$\neq$	$\neq$	=	$\neq$	$\neq$	$\neq$
$\|\psi^+\rangle$	$\neq$	$\neq$	$\neq$	$\neq$	$\neq$	$\neq$	=	$\neq$
$\|\psi^-\rangle$	$\neq$	$\neq$	$\neq$	$\neq$	$\neq$	$\neq$	$\neq$	=

2.4 Decoding step

(1) Charlie decrypts the two encrypted sequences from Alice and Bob by K_{AB}, K_{AC}, and calculates $R_{AB}^i = R_A^i \bigoplus R_B^i$. Then, Charlie uses the Bell basis to measure the ith pair in S_C and gets M_C^i. Through calculating and summarizing for all cases, we find the following relations shown in Table 2.

(2) As shown in Table 2, we can get the relation between Q_A and Q_B. If $R_{AB}^i = 101$ and $M_C^i = |\phi^+\rangle$ ($R_{AB}^i = 100$ and $M_C^i = |\phi^-\rangle$, $R_{AB}^i = 110$ and $M_C^i = |\psi^+\rangle$, $R_{AB}^i = 111$ and $M_C^i = |\psi^-\rangle$), the $Q_A^i = Q_B^i$. Else the $Q_A^i \neq Q_B^i$. If all the $Q_A^i = Q_B^i$, then $Q_A = Q_B$. Once at least one data element $Q_A^i \neq Q_B^i$, then $Q_A \neq Q_B$. Then, two cases are shown in following Table 3.

3 Security analysis

In this section, we will give the security analysis of the proposed protocol. There are two types of attack as the outside attack and dishonest participant attack. Type I: The outside eavesdropper attempts to steal two participants' inputs X or Y. Type II: The dishonest participants and TP may try to obtain the private information.

3.1 Outside attack

For the outside eavesdropper Eve, he has many means to attack the protocol, such as the intercept-resend attack, the entanglement-measure attack, the collective attack, and the Trojan horse attack. However, the entanglement-measure attack and the collective attack will be detected with nonzero probability during the checking step. And the Trojan horse attack also can be automatically prevented due to the one-way transmission.

Moreover, the chance which would be used by Eve to steal the secret inputs by the intercept-resend attack is the transmission of $S'_A(S'_B)$ and encrypted sequence $R_A^i(R_B^i)$ in the preparing step and coding step, respectively. For example, we consider Eve takes the intercept-resend attack strategy on Alice as follows:

Case 1 In the preparing step

Eve first intercepts the sequence S'_A (from Charlie to Alice in preparing step (5)) and then he measures S'_A with the basis $\{|\phi^{\pm}\rangle, |\psi^{\pm}\rangle\}$ ($\{|\chi^{\pm}\rangle, |\omega^{\pm}\rangle\}$). Then, a measurement result sequence M'_A is obtained by Eve. According to the measurement result M'_A,

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

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
000	000	$\|\phi^+\rangle$	$\|\chi^-\rangle$	000	101	000	101	101	$\|\phi^+\rangle$
		$\|\phi^-\rangle$	$\|\chi^+\rangle$	001	100	001	100	101	$\|\phi^+\rangle$
		$\|\psi^+\rangle$	$\|\omega^-\rangle$	010	111	010	111	101	$\|\phi^+\rangle$
		$\|\psi^-\rangle$	$\|\omega^+\rangle$	011	110	011	110	101	$\|\phi^+\rangle$
		$\|\phi^+\rangle$	$\|\chi^+\rangle$	000	100	000	100	100	$\|\phi^-\rangle$
		$\|\phi^-\rangle$	$\|\chi^-\rangle$	001	101	001	101	100	$\|\phi^-\rangle$
		$\|\psi^+\rangle$	$\|\omega^+\rangle$	010	110	010	110	100	$\|\phi^-\rangle$
		$\|\psi^-\rangle$	$\|\omega^-\rangle$	011	111	011	111	100	$\|\phi^-\rangle$
		$\|\psi^+\rangle$	$\|\chi^+\rangle$	010	100	010	100	110	$\|\psi^+\rangle$
		$\|\psi^-\rangle$	$\|\chi^-\rangle$	011	101	011	101	110	$\|\psi^+\rangle$
		$\|\phi^+\rangle$	$\|\omega^+\rangle$	000	110	000	110	110	$\|\psi^+\rangle$
		$\|\phi^-\rangle$	$\|\omega^-\rangle$	001	111	001	111	110	$\|\psi^+\rangle$
		$\|\psi^+\rangle$	$\|\chi^-\rangle$	010	101	010	101	111	$\|\psi^-\rangle$
		$\|\psi^-\rangle$	$\|\chi^+\rangle$	011	100	011	100	111	$\|\psi^-\rangle$
		$\|\phi^+\rangle$	$\|\omega^-\rangle$	000	111	000	111	111	$\|\psi^-\rangle$
		$\|\phi^-\rangle$	$\|\omega^+\rangle$	001	110	001	110	111	$\|\psi^-\rangle$
010	101	$\|\phi^+\rangle$	$\|\chi^-\rangle$	000	101	010	000	010	$\|\phi^+\rangle$
		$\|\phi^-\rangle$	$\|\chi^+\rangle$	001	100	011	001	010	$\|\phi^+\rangle$
		$\|\psi^+\rangle$	$\|\omega^-\rangle$	010	111	000	010	010	$\|\phi^+\rangle$
		$\|\psi^-\rangle$	$\|\omega^+\rangle$	011	110	001	011	010	$\|\phi^+\rangle$
		$\|\phi^+\rangle$	$\|\chi^+\rangle$	000	100	010	001	011	$\|\phi^-\rangle$
		$\|\phi^-\rangle$	$\|\chi^-\rangle$	001	101	011	000	011	$\|\phi^-\rangle$
		$\|\psi^+\rangle$	$\|\omega^+\rangle$	010	110	000	011	011	$\|\phi^-\rangle$
		$\|\psi^-\rangle$	$\|\omega^-\rangle$	011	111	001	010	011	$\|\phi^-\rangle$
		$\|\psi^+\rangle$	$\|\chi^+\rangle$	010	100	000	001	001	$\|\psi^+\rangle$
		$\|\psi^-\rangle$	$\|\chi^-\rangle$	011	101	001	000	001	$\|\psi^+\rangle$
		$\|\phi^+\rangle$	$\|\omega^+\rangle$	000	110	010	011	001	$\|\psi^+\rangle$
		$\|\phi^-\rangle$	$\|\omega^-\rangle$	001	111	011	010	001	$\|\psi^+\rangle$
		$\|\psi^+\rangle$	$\|\chi^-\rangle$	010	101	000	000	000	$\|\psi^-\rangle$
		$\|\psi^-\rangle$	$\|\chi^+\rangle$	011	100	001	001	000	$\|\psi^-\rangle$
		$\|\phi^+\rangle$	$\|\omega^-\rangle$	000	111	010	010	000	$\|\psi^-\rangle$
		$\|\phi^-\rangle$	$\|\omega^+\rangle$	001	110	011	011	000	$\|\psi^-\rangle$

Eve generates the new quantum sequence S_A'' and resends it to Alice for preventing Charlie to perceive the attack. Nevertheless, Eve doesn't know the position of the decoy single photons in S_A', he cannot abandon the decoy photos when he measures the quantum sequence S_A'. Therefore, the decoy photons will destroy the correctness of the measurement results and Eve's new quantum sequence S_A'', and the sequence S_A'' will quite different from S_A'. Once Alice start the eavesdropping process when she

received the photon sequence S''_A, the attack will be easily detected since that the decoy photons have been damaged. In the coding step, the outside eavesdropper cannot get any information of X and Y from R^i_A and R^i_B.

Case 2 In the decoding step

Charlie announces only one $c$bit F for the comparison of secret messages. From this one $c$bit, outside eavesdropper cannot deduce any information of X and Y. In addition, in this protocol, even if Eve gets the accurate particle pairs, he cannot get the right measurement results. According to the pre-shared sequence $(k_0, k_1, \ldots, k_{L-1})$ through a secure QKD protocol between Alice and Bob, and they will measure the particles with different basis according to $K = \bigoplus_{i=0}^{L-1} k_i$. Then, the right basis to chose can get the right measurement results. As Eve cannot know the pre-shared sequence between Alice and Bob, he cannot choose the right basis and get the right measurement results.

Hence, this protocol is secure against the outside attack.

3.2 Participant attack

Generally, the participants always have more opportunities and advantages to attack than an outside eavesdropper. Next, we will give three cases to analyze the possibility of the three parties to get information about X or Y, respectively.

Case 1 Alice(Bob) attempts to obtain Bob(Alice)'s secrets.

In the whole process of the protocol, Alice(Bob) doesn't transmit any information to Bob(Alice) except K, but the pre-shared sequence K only determines the choice of the measurement basis. Therefore, Alice(Bob) cannot infer any information about Bob(Alice)'s secrets.

Case 2 Charlie attempts to obtain Alice(Bob)'s secrets.

Gao [39] points out that the setting in coding step (1) will leak Alice(or Bob)'s private information by malicious Charlie' fake single attack. In this paper, by the pre-shared sequence K between Alice and Bob, Charlie cannot get the right measurement basis to measure the particle pairs in $S_A(S_B)$. Then, he cannot get the right measurement results $M^i_A(M^i_A)$ and infer Alice(Bob)'s secret inputs accurately. Moreover, the secret inputs have been divided into $\lceil N/3L \rceil$, $(L = 1, 2, \ldots)$ groups, while each group has $3L$ bits. And Alice(Bob) always adds $3L - (N \bmod 3L)$ 0 at the end of the N-bit binary string $X(Y)$, so Charlie cannot know the real length of them. From above reasons, Charlie cannot obtain any information about Alice(Bob)'s secrets.

Case 3 Charlie attempts to obtain the comparison results.

Charlie only know the results R^i_{AB} and M^i_C, and he cannot know the comparison principle between Alice and Bob. Due to the pre-shared sequence K, Alice and Bob get the comparison results according to Table 2. The sequence K is pre-shared by a secure QKD protocol between Alice and Bob, and Charlie has no information about it, so he cannot obtain the correct measurement results, then he cannot know the comparison results.

Hence, this protocol is secure against the participant attack.

Table 4 Comparison among the similar QPC protocols

Protocol	Ref. [28]	Ref. [31]	Ref. [32]	Ref. [37]	This protocol
Quantum resource	3-qubit GHZ state	4-qubit W-state and Bell state	Single photon	4-qubit W-state and χ state	4-qubit Cluster state and χ state
Need of unitary operation	Yes	No	Yes	No	No
Bit number compared each time	1	2	1	2	3
Comparison times	L	$\lceil N/2L \rceil$	L	$\lceil N/2 \rceil$	$\lceil N/3L \rceil$
Qubit efficiency η	33.3%	33.3%	25%	33.3%	50%

Table 5 Time complexity comparison with similar protocols

Protocol	Classical computations	Quantum measurements	Unitary operations
Ref. [28]	$3N$	$D + 3N$	2N
Ref. [31]	$3L * \lceil N/2L \rceil$	$D + 3L * \lceil N/2L \rceil$	0
Ref. [32]	$2N$	$D + N$	$2N$
Ref. [37]	$3 * \lceil N/2 \rceil$	$D + 3 * \lceil N/2 \rceil$	0
This protocol	$3L * \lceil N/3L \rceil$	$D + 3L * \lceil N/3L \rceil$	0

4 Efficiency comparison

Considering the qubit efficiency, which was the percentage value between the classic bits and quantum particles in every comparison time. In this protocol, it can encode three-bit data element to three-bit stochastic codes so that three-bit secret inputs can be compared in one comparison time, and the qubit efficiency is 50%. However, the most previous protocols can only compare one or two bits in every comparison time. And the comparison results with some similar previous protocols are shown in Table 4.

In addition, we can simply estimate the classical computations and quantum operations involved in this scheme. As the classical bit-wise exclusive-OR $\bigoplus$ operations in the coding step and decoding step are $3L$ among once group comparison, the whole scheme needs $3L * \lceil N/3L \rceil$ classical operations. Here, we do not consider the classical of the pre-shared sequence in coding step since that it can be calculated in the spare time. While the quantum operations, there need $D + 3L * \lceil N/3L \rceil$ quantum measurements operated by the three participants, where D denotes the measurement of decoy photons. Unfortunately, Ref. [32] also needs $2N$ unitary operations, but there is no need for that in other protocols. Then, the detail comparison results with other similar protocols are shown in Table 5.

As a conclusion, the comparison results in Table 4 and Table 5 have shown that our proposed scheme is more efficient than other protocols.

5 Conclusion

In this paper, an efficient QPC protocol based on the entanglement swapping between the four-qubit cluster state and extended Bell state has been presented. The four-qubit cluster state $|C_4\rangle$ is different from the 4-qubit W-state as that it is hard to destroy the entanglement by local operations. And it also has a strong violation of local reality and shows to be robust against decoherence.

Then, with the help of semi-honest TP, two participants can compare the equality of their private information without leaking them. But he only can obey the duty to perform the rules of the protocol and cannot obtain anything about the comparison results and the participants' private information. Furthermore, with the decoy photons and pre-shared random sequence, it can detect the malicious eavesdropper Eve and forbid him stealing the actual comparison results and the secret inputs. What's more, this protocol has proved to be safe against the outside and participants attacks. Meanwhile, the efficiency comparison shows that the proposed scheme is more efficient than similar previous protocols.

Acknowledgements Project supported by the National Natural Science Foundation of China (Grant Nos. U1636106 and 61671087), Natural Science Foundation of Beijing Municipality under Grant 4182006, The Major Science and Technology Support Program of Guizhou Province under Grant 20183001, The Open Foundation of Guizhou Provincial Key Laboratory of Public Big Data under Grant 2018BDKFJJ016 and BUPT Excellent Ph.D. Students Foundation (Grant No. CX2019227).

References

1. Bennett, C.H., Brassard, G.: Quantum cryptography: public-key distribution and coin tossing. In: IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, pp. 175–179. IEEE, New York (1984)
2. Li, J., Li, N., Zhang, Y., Wen, S., et al.: Special issue on quantum communication: a survey on quantum cryptography. Chin. J. Electron. **27**(2), 223–228 (2018)
3. Bennett, C.H., Wiesner, S.J.: Communication via one and two particle operators on Einstein–Podolsky–Rosen states. Phys. Rev. Lett. **69**, 2881–2884 (1992)
4. Bostrom, K., Felbinger, T.: Deterministic secure direct communication using entanglement. Phys. Rev. Lett. **89**, 187902 (2002)
5. Li, J., Li, N., Li, L.L., Wang, T.: One step quantum key distribution based on EPR entanglement. Sci. Rep. **6**(28767), 1–6 (2016)
6. Li, L.L., Li, J., Li, H.J., Tian, Y., Zheng, Y., Yang, Y.G.: Deterministic quantum secure direct communication protocol based on Omega state. IEEE Access **7**, 6915–6921 (2019)
7. Hillery, M., Buzek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A **59**, 1829–1834 (1999)
8. Kogias, I., Xiang, Y., He, Q., et al.: Unconditional security of entanglement-based continuous-variable quantum secret sharing. Phys. Rev. A **95**, 012315 (2017)
9. Chen, X.B., Tang, X., Xu, G., Dou, Z., Chen, Y.L., et al.: Cryptanalysis of secret sharing with a single d-level quantum system. Quantum Inf. Process. **17**(9), 225 (2018)
10. Wang, T.Y., Ma, J.F., Cai, X.Q.: The postprocessing of quantum digital signatures. Quantum Inf. Process. **16**(1), 19 (2017)
11. Wang, T.Y., Wei, Z.L.: One-time proxy signature based on quantum cryptography. Quantum Inf. Process. **11**(2), 455–463 (2012)
12. Yang, Y.G., Lei, A.H., Liu, A.Z., Zhou, Y.H., Shi, W.M.: Arbitrated quantum signature scheme based on cluster states. Quantum Inf. Process. **15**(6), 2487–2497 (2016)
13. Wang, T.Y., Cai, X.Q., Zhang, R.L.: Security of a sessional blind signature based on quantum cryptograph. Quantum Inf. Process. **13**(8), 1677–1685 (2014)

14. Wang, T.Y., Cai, X.Q., Ren, Y.L., Zhang, R.L.: Security of quantum digital signatures for classical messages. Sci. Rep. **5**, 9231 (2015)
15. Yao, A.C.: Protocols for secure computations. In: Proceedings of the 23rd Annual Symposium on Foundations of Computer Science, pp. 160–164 (1982)
16. Du, W., Atallah, M.J.: Secure multi-party computation problems and their applications: a review and open problems. In: Proceedings of the 2001 Workshop on New Security Paradigms, Cloudcroft, America, pp. 13–22. ACM, New York (2001)
17. Shor, Peter W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput. **26**(5), 1484–1509 (1997)
18. Bonanome, M., Bužek, V., Hillery, M., et al.: Toward protocols for quantum-ensured privacy and secure voting. Phys. Rev. A **84**(2), 022331 (2011)
19. Vaccaro, J.A., Spring, J., Chefles, A.: Quantum protocols for anonymous voting and surveying. Phys. Rev. A **75**(1), 012333 (2007)
20. Huang, W., Wen, Q.Y., Liu, B., et al.: Quantum anonymous ranking. Phys. Rev. A **89**(3), 032325 (2014)
21. Wang, T.Y., Wen, Q.Y., Zhu, F.C.: Economical quantum anonymous transmissions. J. Phys. B At. Mol. Opt. Phys. **43**(24), 245501 (2010)
22. Hogg, T., Harsha, P., Chen, K.Y.: Quantum auctions. Int. J. Quantum Inf. **5**(05), 751–780 (2007)
23. Yang, Y.G., Naseri, M., Wen, Q.Y.: Improved secure quantum sealed-bid auction. Opt. Commun. **282**(20), 4167–4170 (2009)
24. Zhao, Z., Naseri, M., Zheng, Y.: Secure quantum sealed-bid auction with post-confirmation. Opt. Commun. **283**(16), 3194–3197 (2010)
25. Jia, H.Y., Wen, Q.Y., Song, T.T., et al.: Quantum protocol for millionaire problem. Opt. Commun. **284**(1), 545–549 (2011)
26. 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)
27. Wen, L., Wang, Y.B., Cui, W.: Quantum private comparison protocol based on Bell entangled states. Commun. Theor. Phys. **57**(4), 583 (2012)
28. Chen, X.B., Xu, G., Niu, X.X., et al.: 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)
29. Liu, W., Wang, Y.B., Jiang, Z.T.: An efficient protocol for the quantum private comparison of equality with *W* state. Opt. Commun. **284**(12), 3160–3163 (2011)
30. Tseng, H.Y., Lin, J., Hwang, T.: New quantum private comparison protocol using EPR pairs. Quantum Inf. Process. **11**(2), 373–384 (2012)
31. Li, J., Zhou, H.F., Jia, L., et al.: An efficient protocol for the private comparison of equal information based on four-particle entangled *W* state and Bell entangled states swapping. Int. J. Theor. Phys. **53**(7), 2167–2176 (2014)
32. Wei, H., Wen, Q.Y., Liu, B., et al.: Robust and efficient quantum private comparison of equality with collective detection over collective-noise channels. Sci. China Phys. Mech. Astron. **56**(9), 1670–1678 (2013)
33. Chen, X.B., Dou, Z., Xu, G., et al.: A class of protocols for quantum private comparison based on the symmetry of states. Quantum Inf. Process. **13**(1), 85–100 (2014)
34. Liu, X., Zhang, B., Wang, J., et al.: Differential phase shift quantum private comparison. Quantum Inf. Process. **13**(1), 71–84 (2014)
35. Li, J., Jia, L., Zhou, H.F., et al.: Secure quantum private comparison protocol based on the entanglement swapping between three-particle *W*-class state and bell state. Int. J. Theor. Phys. **55**(3), 1710–1718 (2016)
36. Xu, L., Zhao, Z.: Quantum private comparison protocol based on the entanglement swapping between χ^+ state and *W*-class state. Quantum Inf. Process. **16**(12), 302 (2017)
37. Xu, L., Wang, J., Ahmed, H., et al.: A new quantum private comparison protocol. In: AOPC 2017: Fiber Optic Sensing and Optical Communications. International Society for Optics and Photonics, vol. 10464, p. 104640M (2017)
38. Liu, B., Xiao, D., Huang, W., et al.: Quantum private comparison employing single-photon interference. Quantum Inf. Process. **16**(7), 180 (2017)
39. Gao, X., Zhang, S.B., Chang, Y., et al.: Cryptanalysis of the quantum private comparison protocol based on the entanglement swapping between three-particle *W*-class state and Bell state. Int. J. Theor. Phys. **57**(6), 1–7 (2018)

40. Briegel, H.J., Raussendorf, R.: Persistent entanglement in arrays of interacting particles. Phys. Rev. Lett. **86**(5), 910 (2001)
41. Hein, M., Dür, W., Briegel, H.J.: Entanglement properties of multipartite entangled states under the influence of decoherence. Phys. Rev. A **71**(3), 032350 (2005)
42. Walther, P., Resch, K.J., Rudolph, T., et al.: Experimental one-way quantum computing. Nature **434**(7030), 169 (2005)