International Journal of Theoretical Physics (2020) 59:1854–1865
https://doi.org/10.1007/s10773-020-04453-w

Quantum Private Comparison Protocol without a Third Party

WanQing Wu[1] · **XiaoXue Ma**[2]

Received: 14 November 2019 / Accepted: 18 March 2020 / Published online: 1 April 2020

Abstract
This paper presents a quantum private comparison (QPC) protocol based on Bell states. The proposed QPC protocol can secretly compare information of the two participants without the help of a third party (TP). The proposed protocol employs some decoy state photons and quantum SWAP gates to resist various outside attacks and internal attacks. This paper compares the presented quantum private comparison (QPC) protocol with other schemes in terms of different indicators. The results show that the proposed protocol has some advantages different from previous protocols.

Keywords Quantum cryptography · Quantum private comparison · Bell states

1 Introduction

Ever since quantum mechanics was introduced into the cryptography field, numerous quantum cryptographic applications have been proposed, such as quantum secure direct communication ($QSDC$) [1, 2], quantum secret sharing (QSS) [3, 4], quantum public key cryptosystem ($QPKC$) [5, 6].

Recently, quantum private comparison (QPC) becomes an important branch of quantum cryptography, which can privately compare two parties' undisclosed information for equality. In 2009 the first QPC protocol was presented by Yang and Wen based on Bell states and a hash function [7]. Since then numerous QPC protocols have been proposed to improve both the security and the qubit efficiency in [8–16], etc. Thus far, these protocols have accomplished the comparison work with the help of a semi-honest third party

✉ XiaoXue Ma
hbumxx@163.com

[1] School of Cyber Security and computer, Hebei University, Baoding 071002, People's Republic of China

[2] Department of Computer Teaching, Hebei University, Baoding 071002, People's Republic of China

(TP). But a semi-honest TP might try to steal the players private inputs, while he cannot be corrupted by the adversary.

Although Lo (1997) pointed that a QPC may not be securely evaluated with a two-party scenario under the technology of that time in [17]. With the advance in quantum entanglement swapping, many papers reconstructed the two-party QPC protocols without the help of a TP. In 2014 Lin et al. presented a QPC without a TP based on entanglement swapping and a hash function [18]. In 2016 He proposed a QPC with two parties only based on single photon sequences and hash function [19]. Soon afterwards, He proposed the device-independent version of the QPC protocol [20]. One common feature of these protocols is that they require the help of hash functions to complete the comparison in [18–20].

Quantum private comparisons without third-party help are rare. In addition, publishing more efficient and safer protocols are necessary. For the above reasons, this paper present a new QPC protocol without a third party via using the Bell states and quantum SWAP gates. The paper is organized as follows. Section 2 introduces some basic concepts. Section 3 presents a QPC protocol. Section 4 analyzes the security of the QPC protocol. Section 5 concludes the paper.

2 Background

2.1 Permutation Operation

We summarize some basic concepts about permutations. By definition, a permutation of set $A = \{1, \cdots, n\}$ is simply a bijection $\pi : A \to A$. We usually write a permutation π by writing its values as a finite sequence $\pi = (i_1, \cdots, i_n)$, where $\pi(j) = i_j$ and $j = 1, \cdots, n$. We denote all permutations of the set A on S_n. For example, let $A = \{1, 2, 3\}$, then $S_3 = \{(1, 2, 3), (1, 3, 2), (2, 1, 3), (2, 3, 1), (3, 1, 2), (3, 2, 1)\}$.

A transposition is a special permutation that fixes all but two integers, which are interchanged. For example, the following are some of the transpositions in S_3: $(1, 3, 2), (3, 2, 1), (2, 1, 3)$. We define the special notation $[s, t]$ to denote the transposition in S_n that interchanges s and t. For example, with $n = 3$, $(1, 3, 2) = [2, 3]$, $(3, 2, 1) = [1, 3]$, $(2, 1, 3) = [1, 2]$.

There are two basic facts about permutations. One is that every permutation can be written as the composition of transpositions. For example, with $n = 3$, $(3, 1, 2) = [2, 3][1, 2]$. Another is that a representation of a permutation as a composition of transpositions is not unique. For example, with $n = 3$, $(3, 1, 2) = [2, 3][1, 2] = [1, 3][2, 3]$. There are more details in [21].

Next we define a special permutation operation called N-level permutation by iterating the cyclic shift operation several times. Details as below.

Let π_k be a cyclic left-shift operation (shorted by $\lll k$) defined as $\pi_k(i) = i + k \mod r$, that is

$$\pi_k : (1, 2, \cdots, r) \to (k + 1, k + 2, \cdots, r, 1, 2, \cdots, k), \tag{1}$$

where non-negative integer $k < r$. Another cyclic right-shift operation has the same definition.

Let $S = \{a_{(1,\cdots,1,1,1)}, \cdots, a_{(1,\cdots,1,1,r)}, a_{(1,\cdots,1,2,1)}, \cdots, a_{(1,\cdots,1,2,r)}, \cdots, a_{(r,\cdots,r,1)}, \cdots, a_{(\underbrace{r,\cdots,r}_{N},r)}\}$ be a r^N-dimension set, where $r, N \geq 2$. By (1), the cyclic left-shift operation $\pi_{k_j}^{(j)}$ on set S is defined as

$$\begin{aligned}
&\pi_{k_j}^{(j)}\Bigg(a_{(\underbrace{1,\cdots,1}_{j-1},1,\underbrace{1,\cdots,1,1}_{N-j})}, \cdots, a_{(\underbrace{1,\cdots,1}_{j-1},1,\underbrace{1,\cdots,1,r}_{N-j})}, \\
&\qquad \cdots, a_{(\underbrace{r,\cdots,r}_{j-1},r,\underbrace{r,\cdots,r,1}_{N-j})}, \cdots, a_{(\underbrace{r,\cdots,r}_{j-1},r,\underbrace{r,\cdots,r,r}_{N-j})}\Bigg) \\
&= \Bigg(a_{(\underbrace{1,\cdots,1}_{j-1},\pi_{k_j}(1),\underbrace{1,\cdots,1,1}_{N-j})}, \cdots, a_{(\underbrace{1,\cdots,1}_{j-1},\pi_{k_j}(1),\underbrace{1,\cdots,1,r}_{N-j})}, \\
&\qquad \cdots, a_{(\underbrace{r,\cdots,r}_{j-1},\pi_{k_j}(r),\underbrace{r,\cdots,r,1}_{N-j})}, \cdots, a_{(\underbrace{r,\cdots,r}_{j-1},\pi_{k_j}(r),\underbrace{r,\cdots,r,r}_{N-j})}\Bigg)
\end{aligned} \tag{2}$$

where $1 \leq j \leq N$, $1 \leq k_j \leq r$.

Example 1 With $N = 2, r = 3, k_j = 2, j = 2$, it follows that

$$\begin{aligned}
&\pi_2^{(2)}(a_{(1,1)}, a_{(1,2)}, a_{(1,3)}, a_{(2,1)}, a_{(2,2)}, a_{(2,3)}, a_{(3,1)}, a_{(3,2)}, a_{(3,3)}) \\
&= (a_{(1,\pi_2(1))}, a_{(1,\pi_2(2))}, a_{(1,\pi_2(3))}, a_{(2,\pi_2(1))}, a_{(2,\pi_2(2))}, a_{(2,\pi_2(3))}, a_{(3,\pi_2(1))}, \\
&\quad a_{(3,\pi_2(2))}, a_{(3,\pi_2(3))}) \\
&= (a_{(1,3)}, a_{(1,1)}, a_{(1,2)}, a_{(2,3)}, a_{(2,1)}, a_{(2,2)}, a_{(3,3)}, a_{(3,1)}, a_{(3,2)}).
\end{aligned}$$

So the mathematical description of N-level permutation is

$$\pi = \pi_{k_N}^{(N)} \circ \cdots \circ \pi_{k_1}^{(1)}, \tag{3}$$

where $\circ$ means the compound of operation and $\pi_{k_j}^{(j)}$ is the cyclic left-shift operation in (2).

Example 2 With $N = 2, r = 3, k_1 = 2, k_2 = 2$, it performs $\pi = \pi_{k_2}^{(2)} \circ \pi_{k_1}^{(1)}$ operation and obtains

$$\begin{aligned}
&\pi_{k_2}^{(2)} \circ \pi_{k_1}^{(1)}(a_{(1,1)}, a_{(1,2)}, a_{(1,3)}, a_{(2,1)}, a_{(2,2)}, a_{(2,3)}, a_{(3,1)}, a_{(3,2)}, a_{(3,3)}) \\
&= \pi_{k_2}^{(2)}(a_{(\pi_{k_1}(1),1)}, a_{(\pi_{k_1}(1),2)}, a_{(\pi_{k_1}(1),3)}, a_{(\pi_{k_1}(2),1)}, a_{(\pi_{k_1}(2),2)}, a_{(\pi_{k_1}(2),3)}, a_{(\pi_{k_1}(3),1)}, \\
&\quad a_{(\pi_{k_1}(3),2)}, a_{(\pi_{k_1}(3),3)}) \\
&= \pi_{k_2}^{(2)}(a_{(3,1)}, a_{(3,2)}, a_{(3,3)}, a_{(1,1)}, a_{(1,2)}, a_{(1,3)}, a_{(2,1)}, a_{(2,2)}, a_{(2,3)}) \\
&= (a_{(3,\pi_2(1))}, a_{(3,\pi_2(2))}, a_{(3,\pi_2(3))}, a_{(1,\pi_2(1))}, a_{(1,\pi_2(2))}, a_{(1,\pi_2(3))}, a_{(2,\pi_2(1))}, \\
&\quad a_{(2,\pi_2(2))}, a_{(2,\pi_2(3))}) \\
&= (a_{(3,3)}, a_{(3,1)}, a_{(3,2)}, a_{(1,3)}, a_{(1,1)}, a_{(1,2)}, a_{(2,3)}, a_{(2,1)}, a_{(2,2)}).
\end{aligned}$$

Now we define an induction operation of π as follows

$$\overline{\pi} = \pi_{k_1}^{(1)} \circ \cdots \circ \pi_{k_N}^{(N)}. \tag{4}$$

Next we discuss the commutativity of N-level permutation. By the (2), (3) and (4), it directly fields the Proposition 1 as follows.

Proposition 1 *Let π_A and π_B be two N-level permutations, $\overline{\pi_A}$ and $\overline{\pi_B}$ are induction operation of π_A and π_B respectively, then $\pi_A \circ \overline{\pi_B} = \pi_B \circ \overline{\pi_A}$.*

Proof The proof is easy. Let $\pi_A = \pi_{k_N}^{(N)} \circ \cdots \circ \pi_{k_1}^{(1)}$ and $\pi_B = \pi_{s_N}^{(N)} \circ \cdots \circ \pi_{s_1}^{(1)}$ be two N-level permutations. Then it has

$$\begin{aligned}
&\pi_A \circ \overline{\pi_B}(a_{(\underbrace{1,\cdots,1}_{N},1)}, \cdots, a_{(\underbrace{1,\cdots,1}_{N},r)}, \cdots, a_{(\underbrace{r,\cdots,r}_{N},1)}, \cdots, a_{(\underbrace{r,\cdots,r}_{N},r)}) \\
&= \pi_{k_N}^{(N)} \circ \cdots \circ \pi_{k_1}^{(1)} \circ \pi_{s_1}^{(1)} \circ \cdots \circ \pi_{s_N}^{(N)}(a_{(1,\cdots,1,1)}, \cdots, a_{(1,\cdots,1,r)}, \cdots, a_{(r,\cdots,r,1)}, \\
&\quad \cdots, a_{(r,\cdots,r,r)}) \\
&= \pi_{k_N}^{(N)} \circ \cdots \circ \pi_{k_1}^{(1)}(a_{(s_1+1,\cdots,s_{N-1}+1,s_N+1)}, \cdots, a_{(s_1+1,\cdots,s_{N-1}+1,s_N+r)}, \cdots, \\
&\quad a_{(s_1+r,\cdots,s_{N-1}+r,s_N+1)}, \cdots, a_{(s_1+r,\cdots,s_{N-1}+r,s_N+r)}) \\
&= (a_{(k_1+s_1+1,\cdots,k_{N-1}+s_{N-1}+1,k_N+s_N+1)}, \cdots, a_{(k_1+s_1+1,\cdots,k_{N-1}+s_{N-1}+1,k_N+s_N+r)}, \cdots, \\
&\qquad a_{(k_1+s_1+r,\cdots,k_{N-1}+s_{N-1}+r,k_N+s_N+1)}, \cdots, a_{(k_1+s_1+r,\cdots,k_{N-1}+s_{N-1}+r,k_N+s_N+r)})
\end{aligned}$$

and

$$\begin{aligned}
&\pi_B \circ \overline{\pi_A}\left(a_{(\underbrace{1,\cdots,1}_{N},1)}, \cdots, a_{(\underbrace{1,\cdots,1}_{N},r)}, \cdots, a_{(\underbrace{r,\cdots,r}_{N},1)}, \cdots, a_{(\underbrace{r,\cdots,r}_{N},r)}\right) \\
&= \pi_{s_N}^{(N)} \circ \cdots \circ \pi_{s_1}^{(1)} \circ \pi_{k_1}^{(1)} \circ \cdots \circ \pi_{k_N}^{(N)}(a_{(1,\cdots,1,1)}, \cdots, a_{(1,\cdots,1,r)}, \cdots, a_{(r,\cdots,r,1)}, \cdots, \\
&\quad a_{(r,\cdots,r,r)}) \\
&= \pi_{s_N}^{(N)} \circ \cdots \circ \pi_{s_1}^{(1)}(a_{(k_1+1,\cdots,k_{N-1}+1,k_N+1)}, \cdots, a_{(k_1+1,\cdots,k_{N-1}+1,k_N+r)}, \cdots, \\
&\quad a_{(k_1+r,\cdots,k_{N-1}+r,k_N+1)}, \cdots, a_{(k_1+r,\cdots,k_{N-1}+r,k_N+r)}) \\
&= (a_{(k_1+s_1+1,\cdots,k_{N-1}+s_{N-1}+1,k_N+s_N+1)}, \cdots, a_{(k_1+s_1+1,\cdots,k_{N-1}+s_{N-1}+1,k_N+s_N+r)}, \cdots, \\
&\quad a_{(k_1+s_1+r,\cdots,k_{N-1}+s_{N-1}+r,k_N+s_N+1)}, \cdots, a_{(k_1+s_1+r,\cdots,k_{N-1}+s_{N-1}+r,k_N+s_N+r)}).
\end{aligned}$$

It is clear that $\pi_A \circ \overline{\pi_B} = \pi_B \circ \overline{\pi_A}$. Thus it holds. □

Example 3 For $N = 2, r = 2$, let $\pi_A = \pi_1^{(2)} \circ \pi_2^{(1)}$ and $\pi_B = \pi_2^{(2)} \circ \pi_1^{(1)}$ be two 2-level permutations, then it has

$$\begin{aligned}
&\pi_A \circ \overline{\pi_B}(a_{(1,1)}, a_{(1,2)}, a_{(2,1)}, a_{(2,2)}) \\
&= \pi_1^{(2)} \circ \pi_2^{(1)} \circ \pi_1^{(1)} \circ \pi_2^{(2)}(a_{(1,1)}, a_{(1,2)}, a_{(2,1)}, a_{(2,2)}) \\
&= \pi_1^{(2)} \circ \pi_2^{(1)}(a_{(2,1)}, a_{(2,2)}, a_{(1,1)}, a_{(1,2)}) \\
&= (a_{(2,2)}, a_{(2,1)}, a_{(1,2)}, a_{(1,1)})
\end{aligned}$$

and

$$\begin{aligned}
&\pi_B \circ \overline{\pi_A}(a_{(1,1)}, a_{(1,2)}, a_{(2,1)}, a_{(2,2)}) \\
&= \pi_2^{(2)} \circ \pi_1^{(1)} \circ \pi_2^{(1)} \circ \pi_1^{(2)}(a_{(1,1)}, a_{(1,2)}, a_{(2,1)}, a_{(2,2)}) \\
&= \pi_2^{(2)} \circ \pi_1^{(1)}(a_{(1,2)}, a_{(1,1)}, a_{(2,2)}, a_{(2,1)}) \\
&= (a_{(2,2)}, a_{(2,1)}, a_{(1,2)}, a_{(1,1)})
\end{aligned}$$

It is clear that $\pi_A \circ \overline{\pi_B} = \pi_B \circ \overline{\pi_A}$.

2.2 General Quantum SWAP Gates

In this subsection we introduce a quantum SWAP gate. The SWAP gate is seen as an important component in theory of quantum computation. For a n-qubit quantum systems $|c_1, \cdots, c_n\rangle$, the general quantum SWAP gate in [22] will act as:

$$SWAP_\pi : |c_1, \cdots, c_n\rangle = |c_{i_1}, \cdots, c_{i_n}\rangle, \tag{5}$$

where a permutation $\pi = (i_1, \cdots, i_n)$.

Let π be a permutation, then $\pi = \pi_1 \circ \cdots \circ \pi_m$, where π_i is also a transposition, $1 \leq i \leq n$. Since every permutation can be written as the composition of transpositions. By (5), we have

$$SWAP_\pi = SWAP_{\pi_1} \cdots SWAP_{\pi_m}.$$

For example, in 3-qubit system, $SWAP_{(3,1,2)}|c_1, c_2, c_3\rangle = SWAP_{[2,3]}SWAP_{[1,2]}|c_1, c_2, c_3\rangle = |c_3, c_1, c_2\rangle$. Thus, it directly fields the following Proposition 2.

Proposition 2 *Let π_A and π_B be two N-level permutations, $\overline{\pi_A}$ and $\overline{\pi_B}$ are induction operation of π_A and π_B respectively, then $SWAP_{\pi_A \circ \overline{\pi_B}} = SWAP_{\pi_B \circ \overline{\pi_A}}$ for n-qubit quantum system.*

3 The Proposed Two-Party QPC Protocol

3.1 A Description of QPC Protocol

Alice and Bob are two parties who want to compare the equality of their secret messages with same bit-length, $a, b \in \{0, 1\}^*$, respectively. They agree that the two Bell states $|\phi^0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, $|\phi^1\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ represent the classical bits 0, 1, respectively. The proposed protocol can be depicted in steps as following.

Alice divides the secret message a into m groups, which are

$$\begin{aligned}
&X_0 = \{a_1, \cdots, a_{r^2}\} = \{a_{(1,1)}, \cdots, a_{(1,r)}, \cdots, a_{(r,1)}, \cdots, a_{(r,r)}\}, \\
&X_1 = \{a_{r^2+1}, \cdots, a_{2r^2}\} = \{a^{(1)}_{(1,1)}, \cdots, a^{(1)}_{(1,r)}, \cdots, a^{(1)}_{(r,1)}, \cdots, a^{(1)}_{(r,r)}\}, \\
&\cdots, \\
&X_{m-1} = \{a_{(m-1)r^2+1}, \cdots, a_{(m-1)r^2}\} = \{a^{(m-1)}_{(1,1)}, \cdots, a^{(m-1)}_{(1,r)}, \cdots, a^{(m-1)}_{(r,1)}, \cdots, a^{(m-1)}_{(r,r)}\}.
\end{aligned}$$

If $|X_{m-1}| \neq r^2$, Alice fills in the data alternately 0 and 1 after X_{m-1}.

Bob does the same things for the secret message b and obtains

$$Y_0 = \{b_1, \cdots, b_{r^2}\} = \{b_{(1,1)}, \cdots, b_{(1,r)}, \cdots, b_{(r,1)}, \cdots, b_{(r,r)}\},$$
$$Y_1 = \{b_{r^2+1}, \cdots, b_{2r^2}\} = \{b^{(1)}_{(1,1)}, \cdots, b^{(1)}_{(1,r)}, \cdots, b^{(1)}_{(r,1)}, \cdots, b^{(1)}_{(r,r)}\},$$
$$\cdots,$$
$$Y_{m-1} = \{b_{(m-1)r^2+1}, \cdots, b_{(m-1)r^2}\} = \{b^{(m-1)}_{(1,1)}, \cdots, b^{(m-1)}_{(1,r)}, \cdots, b^{(m-1)}_{(r,1)}, \cdots, b^{(m-1)}_{(r,r)}\},$$

where $a_{(i,j)}, b_{(i,j)} \in \{0, 1\}, i, j = 1, \cdots, r^2, a_s, b_s \in \{0, 1\}, s = 1, \cdots, mr^2$ and $r \in Z^+$.

Step 1. Alice (Bob) selects two transpositions $\pi^{(1)}_{k_1}, \pi^{(2)}_{k_2}(\pi^{(1)}_{s_1}, \pi^{(2)}_{s_2})$ in (4). Then Alice (Bob) computes

$$\overline{\pi_A}(X_0) = \overline{\pi_A}(a_{(1,1)}, \cdots, a_{(1,r)}, \cdots, a_{(r,1)}, \cdots, a_{(r,r)}) = (a_{\overline{\pi_A}(1)}, \cdots, a_{\overline{\pi_A}(r^2)})$$

$$(\overline{\pi_B}(Y_0) = \overline{\pi_B}(b_{(1,1)}, \cdots, b_{(1,r)}, \cdots, b_{(r,1)}, \cdots, b_{(r,r)}) = (b_{\overline{\pi_B}(1)}, \cdots, b_{\overline{\pi_B}(r^2)}))$$

for first group $X_0(Y_0)$, where $\overline{\pi_A} = \pi^{(1)}_{k_1} \circ \pi^{(2)}_{k_2}(\overline{\pi_B} = \pi^{(1)}_{s_1} \circ \pi^{(2)}_{s_2})$.

Step 2. Alice (Bob) encodes each bit of $\overline{\pi_A}(X_0)(\overline{\pi_B}(Y_0))$ and prepares r^2 Bell states as initial states. Alice (Bob) records these initial states as

$$S_A = \{|\phi^{a_{\overline{\pi_A}(1)}}\rangle_1, \cdots, |\phi^{a_{\overline{\pi_A}(r^2)}}\rangle_{r^2}\} \quad (S_B = \{|\phi^{b_{\overline{\pi_B}(1)}}\rangle_1, \cdots, |\phi^{b_{\overline{\pi_B}(r^2)}}\rangle_{r^2}\}),$$

where $|\phi^{a_{\overline{\pi_A}(i)}}\rangle_i, |\phi^{b_{\overline{\pi_B}(i)}}\rangle_i \in \{|\phi^0\rangle, |\phi^1\rangle\}, i = 1, \cdots, r^2$. Further, Alice (Bob) divides them into two ordered sequences S_{A_1} and $S_{A_2}(S_{B_1}$ and $S_{B_2})$ composed of the 1st and 2nd particles of each Bell state respectively, that is

$$S_{A_1} = \{|\phi_1^{a_{\overline{\pi_A}(1)}}\rangle_1, \cdots, |\phi_1^{a_{\overline{\pi_A}(r^2)}}\rangle_{r^2}\} \quad (S_{B_1} = \{|\phi_1^{b_{\overline{\pi_B}(1)}}\rangle_1, \cdots, |\phi_1^{b_{\overline{\pi_B}(r^2)}}\rangle_{r^2}\}),$$

$$S_{A_2} = \{|\phi_2^{a_{\overline{\pi_A}(1)}}\rangle_1, \cdots, |\phi_2^{a_{\overline{\pi_A}(r^2)}}\rangle_{r^2}\} \quad (S_{B_2} = \{|\phi_2^{b_{\overline{\pi_B}(1)}}\rangle_1, \cdots, |\phi_2^{b_{\overline{\pi_B}(r^2)}}\rangle_{r^2}\}).$$

Step 3. Alice (Bob) randomly prepares decoy photons $\otimes D^A_j(\otimes D^B_j)$, where $|D^A_j\rangle$ $(|D^B_j\rangle) \in \{|0\rangle, |1\rangle, (|0\rangle + |1\rangle)/\sqrt{2}, (|0\rangle - |1\rangle)/\sqrt{2}\}(j = 1, 2, \cdots, k)$. Then Alice (Bob) randomly inserts $\otimes D^A_j(\otimes D^B_j)$ in $S_{A_1}(S_{B_1})$ to form a new sequence $S'_{A_1}(S'_{B_1})$, and sends it to Bob (Alice).

Step 4. After confirming that Bob (Alice) has received the quantum sequence $S'_{A_1}(S'_{B_1})$, Alice (Bob) informs the positions and the measurement bases of $\otimes D^A_j(\otimes D^B_j)$ to Bob (Alice). Subsequently, Bob (Alice) extracts the particles in $\otimes D^A_j(\otimes D^B_j)$ from $S'_{A_1}(S'_{B_1})$, and gets the sequence $S_{A_1}(S_{B_1})$. Thereafter, Alice and Bob can check the existence of an Eve by a predetermined threshold of error rate. If the error rate is limited in a predetermined threshold, there is no eve and the protocol continues. Otherwise, Alice and Bob abort the protocol and restart from Step 1.

Step 5. Bob (Alice) performs quantum swapping gate $SWAP_{\pi_B}(SWAP_{\pi_A})$ on quantum particle sequence $S_{A_1}(S_{B_1})$ and obtains

$$S''_{A_1} = \{|\phi_1^{a_{\overline{\pi_A}(1)}}\rangle_{\pi_B(1)}, \cdots, |\phi_1^{a_{\overline{\pi_A}(r^2)}}\rangle_{\pi_B(r^2)}\} \ (S''_{B_1} = \{|\phi_1^{b_{\overline{\pi_B}(1)}}\rangle_{\pi_A(1)}, \cdots, |\phi_1^{b_{\overline{\pi_B}(r^2)}}\rangle_{\pi_A(r^2)}\}).$$

Step 6. Bob (Alice) selects a binary random sequences $e^B = (e^B_1, e^B_2, \cdots, e^B_{r^2}) \in \{0, 1\}^{r^2}$ $(e^A = (e^A_1, e^A_2, \cdots, e^A_{r^2}) \in \{0, 1\}^{r^2})$. Bob (Alice) performs unitary operation U on quantum particle sequence $S''_{A_1}(S''_{B_1})$ and obtains a new quantum particle sequence $\widetilde{S}''_{A_1}(\widetilde{S}''_{B_1})$, where $U = I$ if $e^B_i = 0$ $(e^A_i = 0)$ and U is X-gate if $e^B_i = 1$ $(e^A_i = 1)$.

Step 7. Bob (Alice) randomly inserts $\otimes D_j'^A(\otimes D_j'^B)$ in $\widetilde{S}''_{A_1}$ and $S_{B_2}(\widetilde{S}''_{B_1}$ and $S_{A_2})$ to form a new sequence $S'''_{A_1}(S'''_{B_1})$ and $S'_{B_2}(S'_{A_2})$, where $|D_j'^A\rangle(|D_j'^B\rangle) \in \{|0\rangle, |1\rangle, (|0\rangle + |1\rangle)/\sqrt{2}, (|0\rangle - |1\rangle)/\sqrt{2}\}(j = 1, 2, \cdots, k)$. Then Bob (Alice) sends sequences $S'''_{A_1}(S'''_{B_1})$ and $S'_{B_2}(S'_{A_2})$ to Alice (Bob).

Step 8. Alice and Bob check the existence of an Eve just as Step 4 introduced, and obtains $\widetilde{S}''_{A_1}$, S_{B_2} and $\widetilde{S}''_{B_1}$, S_{A_2} respectively.

Step 9. Bob (Alice) performs quantum swapping gate $SWAP_{\pi_B}(SWAP_{\pi_A})$ on quantum particle sequence $S_{A_2}(S_{B_2})$, and obtains

$$S''_{A_2} = \{|\phi_2^{a_{\overline{\pi_A}}(1)}\rangle_{\pi_B(1)}, \cdots, |\phi_2^{a_{\overline{\pi_A}}(r^2)}\rangle_{\pi_B(r^2)}\} \ (S''_{B_2} = \{|\phi_2^{b_{\overline{\pi_B}}(1)}\rangle_{\pi_A(1)}, \cdots, |\phi_2^{b_{\overline{\pi_B}}(r^2)}\rangle_{\pi_A(r^2)}\}).$$

Step 10. Alice (Bob) obtains the sequence of classical results $\{a_1^{A_1} \oplus e_1^B, \cdots, a_{r^2}^{A_1} \oplus e_{r^2}^B, b_1^{B_2}, \cdots, b_{r^2}^{B_2}\}$, $(\{b_1^{B_1} \oplus e_1^A, \cdots, b_{r^2}^{B_1} \oplus e_{r^2}^A, a_1^{A_2}, \cdots, a_{r^2}^{A_2}\})$ from quantum particles $\widetilde{S}''_{A_1} S''_{B_2}(\widetilde{S}''_{B_1} S''_{A_2})$ after the $|0\rangle, |1\rangle$ basis measurement. Alice (Bob) computes the $t_i^A = a_i^{A_1} \oplus e_i^B \oplus b_i^{B_2} \oplus e_i^A$ $(t_i^B = b_i^{B_1} \oplus e_i^A \oplus a_i^{A_2} \oplus e_i^B)$, and obtains result $t^A = \{t_i^A, i = 1, \cdots, r^2\}$ $(t^B = \{t_i^B, i = 1, \cdots, r^2\})$. Alice and Bob publish the t^A and t^B respectively. If $t^A = t^B$, then they announce the compared secret information X_0 and Y_0 are identical, and perform the protocol for the next group X_j and Y_j, $j = 1, \cdots, m-1$. Otherwise, they announce the comparison are regarded as different.

3.2 An Example

Next, we taken an example when $N = 2, r = 2$. Suppose that Alice's and Bob's secret inputs are $a = a_{(1,1)}a_{(1,2)}a_{(2,1)}a_{(2,2)} = 1001$, $b = b_{(1,1)}b_{(1,2)}b_{(2,1)}b_{(2,2)} = 1001$.

Step 1. Alice selects two integers $k_1 = 1, k_2 = 2$ and computes

$$\begin{aligned}\overline{\pi_A}(a_{(1,1)}, a_{(1,2)}, a_{(2,1)}, a_{(2,2)}) &= \pi_{k_1}^{(1)} \circ \pi_{k_2}^{(2)}(a_{(1,1)}, a_{(1,2)}, a_{(2,1)}, a_{(2,2)}) \\ &= (a_{(2,1)}, a_{(2,2)}, a_{(1,1)}, a_{(1,2)}) = 0110.\end{aligned}$$

Bob selects two integers $s_1 = 1, s_2 = 1$ and computes

$$\begin{aligned}\overline{\pi_B}(b_{(1,1)}, b_{(1,2)}, b_{(2,1)}, b_{(2,2)}) &= \pi_{s_1}^{(1)} \circ \pi_{s_2}^{(2)}(b_{(1,1)}, b_{(1,2)}, b_{(2,1)}, b_{(2,2)}) \\ &= (a_{(2,2)}, a_{(2,1)}, a_{(1,2)}, a_{(1,1)}) = 1001.\end{aligned}$$

Step 2. Alice (Bob) encodes each bit and prepares 4 Bell states as initial states. Alice (Bob) records these initial states as

$$S_A = \{|\phi^0\rangle_1, |\phi^1\rangle_2, |\phi^1\rangle_3, |\phi^0\rangle_4\} \quad (S_B = \{|\phi^1\rangle_1, |\phi^0\rangle_2, |\phi^0\rangle_3, |\phi^1\rangle_4\}.$$

Further, Alice (Bob) divides them into two ordered sequences S_{A_1} and $S_{A_2}(S_{B_1}$ and $S_{B_2})$ composed of the 1st and 2nd particles of each Bell state respectively, that is

$$S_{A_1} = \{|\phi_1^0\rangle_1, |\phi_1^1\rangle_2, |\phi_1^1\rangle_3, |\phi_1^0\rangle_4\} \quad (S_{B_1} = \{|\phi_1^1\rangle_1, |\phi_1^0\rangle_2, |\phi_1^0\rangle_3, |\phi_1^1\rangle_4\}),$$

$$S_{A_2} = \{|\phi_2^0\rangle_1, |\phi_2^1\rangle_2, |\phi_2^1\rangle_3, |\phi_2^0\rangle_4\} \quad (S_{B_2} = \{|\phi_1^1\rangle_1, |\phi_1^0\rangle_2, |\phi_2^0\rangle_3, |\phi_1^1\rangle_4\}).$$

Step 3. Alice (Bob) randomly inserts decoy photons in $S_{A_1}(S_{B_1})$ to form a new sequence $S'_{A_1}(S'_{B_1})$, and sends it to Bob (Alice).

Step 4. Alice and Bob check the presence of an Eve. There is no an Eve and the protocol continues. Otherwise, Alice and Bob abort the protocol and restart from Step 1.

Step 5. Bob (Alice) performs quantum swapping gate $SWAP_{\pi_B}(SWAP_{\pi_A})$ on quantum particle sequence $S_{A_1}(S_{B_1})$ and obtains

$$S''_{A_1} = \{|\phi_1^0\rangle_4, |\phi_1^1\rangle_3, |\phi_1^1\rangle_2, |\phi_1^0\rangle_1\} \quad (S''_{B_1} = \{|\phi_1^0\rangle_3, |\phi_1^1\rangle_4, |\phi_1^1\rangle_1, |\phi_1^0\rangle_2\}).$$

Step 6. Bob (Alice) selects a binary random sequences $e^B = (0, 0, 1, 1)(e^A = (1, 1, 0, 0))$. Bob (Alice) performs unitary operation U on quantum particle sequence $S''_{A_1}(S''_{B_1})$ and obtains a new quantum particle sequence $\widetilde{S}''_{A_1}(\widetilde{S}''_{B_1})$, where $U = I$ if $e_i^B = 0$ ($e_i^A = 0$) and U is X-gate if $e_i^B = 1$ ($e_i^A = 1$).

Step 7. Alice (Bob) randomly inserts decoy photons in $\widetilde{S}''_{A_1}$ and $S_{B_2}(\widetilde{S}''_{B_1}$ and $S_{A_2})$ to form a new sequence $S'''_{A_1}(S'''_{B_1})$ and $S'_{B_2}(S'_{A_2})$, and sends them to Bob (Alice).

Step 8. Alice and Bob check the existence of an Eve just as Step 4 introduced, and obtains $\widetilde{S}''_{A_1}$, S_{B_2} and $\widetilde{S}''_{B_1}$, S_{A_2} respectively.

Step 9. Bob (Alice) performs quantum swapping gate $SWAP_{\pi_B}(SWAP_{\pi_A})$ on quantum particle sequence $S_{A_2}(S_{B_2})$, and obtains

$$S''_{A_2} = \{|\phi_2^0\rangle_4, |\phi_2^1\rangle_3, |\phi_2^1\rangle_2, |\phi_2^0\rangle_1\} \quad (S''_{B_2} = \{|\phi_2^0\rangle_3, |\phi_2^1\rangle_4, |\phi_2^1\rangle_1, |\phi_2^0\rangle_2\}).$$

Step 10. Alice (Bob) obtains the sequence of classical results $\{0, 1, 0, 1, 1, 1, 0, 0\}$, $(\{0, 1, 1, 0, 0, 0, 0, 0)$ from quantum particles $\widetilde{S}''_{A_1}S''_{B_2}(\widetilde{S}''_{B_1}S''_{A_2})$ after the $|0\rangle, |1\rangle$ basis measurement. Alice (Bob) computes the $t^A = \{0, 1, 0, 1\}$ ($t^B = \{0, 1, 0, 1\}$). Alice and Bob publish the t^A and t^B respectively. The $t^A = t^B$, then they announce the compared secret information a and b are identical.

4 Analysis

4.1 Correctness

Alice and Bob use the N-level permutation to process secret information. They encode secret information and insert decoy states randomly. Then they send the first sequence of quantum particles to each other. Alice and Bob check the presence of an Eve. They use the quantum swapping gate $SWAP_{\pi_B}$ and $SWAP_{\pi_A}$ to process the sequence of quantum particles received separately. Before sending, Alice and Bob perform some unitary operations U on quantum particle sequences according to the random number sequences selected. Then they insert the decoy states in the sequence of quantum particles, and return to each other. After checking the presence of an Eve, they respectively obtain the sequence of quantum particles $\widetilde{S}''_{A_1}$, S_{B_2} and $\widetilde{S}''_{B_1}$, S_{A_2} from each other. Furthermore, they perform quantum swapping gate $SWAP_{\pi_A}$ and $SWAP_{\pi_B}$ on quantum particle sequence S_{B_2} and S_{A_2}, separately. After the measurement, Alice and Bob obtain some corresponding encoding information respectively. That is, after performing 0, 1 basis measurement, Alice and Bob obtain the $a_i^{A_1} \oplus e_i^B, b_i^{B_2}$ and $b_i^{B_1} \oplus e_i^A, a_i^{A_2}$, respectively. Since Proposition 1, $\pi_B \circ \overline{\pi_A} = \pi_A \circ \overline{\pi_B}$ holds. From Table 1 we observe that when the secret information is the same, that is $a_i = b_i$, there is always $t_i^A \oplus t_i^B = 0$. Otherwise, when $a_i \neq b_i$, there is always $t_i^A \oplus t_i^B = 1$. So our protocol is correctness.

Table 1 The mainly parameters and their values

a_i	b_i	$a_i \oplus b_i$	$\|\phi^{a_i}\rangle$	$\|\phi^{b_i}\rangle$	$a_i^{A_1}$	$a_i^{A_2}$	$b_i^{B_1}$	$b_i^{B_2}$	$a_i^{A_1} \oplus b_i^{B_2}$	$a_i^{A_2} \oplus b_i^{B_1}$	$t_i^A \oplus t_i^B$
0	0	0	$\frac{\|00\rangle+\|11\rangle}{\sqrt{2}}$	$\frac{\|00\rangle+\|11\rangle}{\sqrt{2}}$	0	0	0	0	0	0	0
					0	0	1	1	1	1	
					1	1	0	0	1	1	
					1	1	1	1	0	0	
0	1	1	$\frac{\|00\rangle+\|11\rangle}{\sqrt{2}}$	$\frac{\|01\rangle+\|10\rangle}{\sqrt{2}}$	0	0	0	1	1	0	1
					0	0	1	0	0	1	
					1	1	0	1	0	1	
					1	1	1	0	1	0	
1	0	1	$\frac{\|01\rangle+\|10\rangle}{\sqrt{2}}$	$\frac{\|00\rangle+\|11\rangle}{\sqrt{2}}$	0	1	0	0	0	1	1
					0	1	1	1	1	0	
					1	0	0	0	1	0	
					1	0	1	1	0	1	
1	1	0	$\frac{\|01\rangle+\|10\rangle}{\sqrt{2}}$	$\frac{\|01\rangle+\|10\rangle}{\sqrt{2}}$	0	1	0	1	1	1	0
					0	1	1	0	0	0	
					1	0	0	1	0	0	
					1	0	1	0	1	1	

4.2 Outsider Attack

In presented protocol, Alice and Bob exchange compared secret information under insecure channels. In order to ensure the security of information, all parties publicly check for the existence of an Eve. There are two steps need to detect the presence of an Eve in presented protocol.

Since the Eve doesn't know the measuring bases, and the positions of all decoy photons in S'_{A_1} and S'_{B_1}. Eve will lead to an error to each decoy photon with a probability of $\frac{1}{4}$. Thus, let n be the number of decoy photons, if n is large enough, then the probability of detecting Eve's attack from the public discussion $1-(\frac{3}{4})^n$ is close to 1. In addition, in step 8, Alice and Bob check the existence of an Eve just as Step 4 introduced. Hence, the presented protocol can withstand some known outsider attacks, such as entanglement-measure attack, measurement-resend attack, and intercept-resend [23–27].

4.3 Insider Attack

In general, dishonest participant can learn the secret of other party's partial information without being detected. This congenital advantage for any participants should be limited such that it doesn't threaten the security of the presented protocol.

The presented protocol is symmetric, Alice and Bob can execute the same attack strategy. Without loss of generality, we consider the case that Bob learns the Alice's secret.

For comparing private information a, Alice divides the secret information into some groups, rearranges them according to a cyclic left-shift operation π_A and encoding the new secret information using the Bell states on Step 1 and Step 2. At Step 3, Alice randomly inserts some decoy photons in S_{A_1} and sends the quantum sequences to Bob. After checking the existence of an Eve, Bob can obtain the sequences of quantum particles S_{A_1}.

So Bob can distinguish between $a_j = 0$ and $a_j = 1$, $j = \pi_A(i)$ if Bob can distinguish between the two states $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$ and $\frac{|01\rangle+|10\rangle}{\sqrt{2}}$. Bob needs to distinguish between the density matrices

$$\begin{aligned}\rho^A &= tr_2\left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\frac{\langle 00| + \langle 11|}{\sqrt{2}}\right)\\ &= \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} = \begin{pmatrix}\frac{1}{2} & 0\\ 0 & \frac{1}{2}\end{pmatrix}\end{aligned}$$

and

$$\begin{aligned}\sigma^A &= tr_2\left(\frac{|01\rangle + |10\rangle}{\sqrt{2}}\frac{\langle 01| + \langle 10|}{\sqrt{2}}\right)\\ &= \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} = \begin{pmatrix}\frac{1}{2} & 0\\ 0 & \frac{1}{2}\end{pmatrix}.\end{aligned}$$

It is clear that $\rho^A = \sigma^A$. Then Bob cann't distinguish the Alice's initial Bell states by measuring the first photon of the j-th state.

In Step 8, Bob can obtain the quantum particle sequence S_{A_2}. But Bob only knows the π_B and doesn't know the π_A. The probability of obtaining another correct π_A is $\frac{1}{r^2}$, that is the order $\pi_A\overline{\pi_B}$ is secret for Bob. Through the particle sequences S_{A_1} and S_{A_2}, Bob only guesses the correct Bell state or the corresponding message X_0 with a probability of $\frac{1}{r^2}$.

In addition, in Step 8, Bob obtains other quantum particle sequence $\widetilde{S}''_{B_1}$. Bob doesn't obtain Alice's secret information. The reason is that Bob does not know random number sequence e^A except e^B. So Bob only guesses the correct random numbers with $\frac{1}{2^{r^2}}$ successful probability. Furthermore, the presented protocol can resist the inside attacks.

4.4 Comparison

In this subsection, the comparisons of Lin et al.'s protocol [18], He's protocol [19], and the proposed scheme is described in the following Table 2. The qubit efficiency η is defined as $\eta = \frac{\eta_c}{\eta_q}$, where η_c denotes the classical bits that can be employed, and η_q denotes the total photons.

Table 2 The comparison of the proposed protocol to the other QPCs

	Lin et al.'s [18]	He's [19]	Proposed protocol
Quantum state	Bell state	Single photon state	Bell state
Need of entanglement swapping	Yes	No	Yes
Operations for two players	Hash function	Hash function	Quantum SWAP gate
Quantum measurement for users	Bell-basis measurement	Single-photon measurement	{0, 1}-basis measure
Need of decoy states	Yes	No	Yes
Qubit efficiency (%)	50%	100%	50%
Times	Lower	Lower	Faster
Communication complexity	One	One	Two

Lin et al. use Bell states to design their QPC protocol, in which two qubits can compare one bit of information. However, the qubit efficiency can be computed as 50%. In He's protocol, single photon states are used to construct the QPC, in which one photons can compare one bit of information among two parties. Therefore, its qubit efficiency is 100%. Comparing these protocol, the presented protocol also uses the Bell states to construct the new QPC, It leads to the qubit efficiency of 50%.

Lin et al.'s and He's scheme need more quantum devices such as quantum operations, and quantum measurement to perform the comparison. For Lin et al.'s and He's scheme, both users have to perform one-to-one hash operation to encode the hash code of their information in advance, and encode each bit to the corresponding quantum states. In the proposed scheme, it does not require hash coding in advance.

In addition, in Lin et al.'s QPC, it need Bell-basis measurement to accomplish the comparison phase. In He's scheme, it requires single photon measurements. In the proposed scheme, the two players only need to perform the $\{0, 1\}$-basis measure to retrieve their own result of comparison. Thus, the proposed scheme is more efficient and practical.

5 Conclusion

In this paper, we described a protocol to compare the quantum secrets without a third party based on the Bell states and quantum SWAP gates. The proposed protocol has adopted quantum transmission strategy and the decoy state photons to prevent various types of eve attacks. In addition, Bob (Alice) only knows the $\pi_B(\pi_A)$, and doesn't know the $\pi_A(\pi_B)$. Thus they have only the same order of information arrangement, but the $\pi_A\overline{\pi_B} = \overline{\pi_A}\pi_B$ is secret for two parties. The participants' encoded secrets are protected by the entanglement of Bell states. So, it provides security for inside attackers. In summary, through the security analysis, the presented protocol is demonstrated to be secure against outsider attack and insider attack.

Acknowledgments The authors are supported by the Natural Science Foundation of HeBei Province Nos. F2017201199.

References

1. Zhang, W., Ding, D.S., Sheng, Y.B., et al.: Quantum secure direct communication with quantum memory. Phys. Rev. Lett. **118**(22), 220501 (2017)
2. He, Y.F., Ma, W.P.: Three-party quantum secure direct communication against collective noise. Quantum Inf. Process **16**(10), 252 (2017)
3. Xu, T.T., Li, Z.H., Bai, C.M., et al.: A new improving quantum secret sharing scheme. Int. J. Theor. Phys. **56**, 1–10 (2017)
4. Bai, C.M., Li, Z.H., Xu, T.T., et al.: Quantum secret sharing using the d-dimensional GHZ state. Quantum Inf. Process **16**(3), 59 (2017)
5. Wu, W.Q., Cai, Q.Y., Zhang, H.G., et al.: Quantum public key cryptosystem based on bell states. Int. J. Theor. Phys. **56**(11), 3431–3440 (2017)
6. Wu, W.Q., Cai, Q.Y., Zhang, H.G., et al.: Bit-oriented quantum public-key cryptosystem based on bell states. Int. J. Theor. Phys. **57**(12), 1–11 (2018)
7. Yang, Y.G., Cao, W.F., Wen, Q.Y.: Secure quantum private comparison. Physica Scripta **80**(6), 065002 (2009)
8. Ye, T.Y., Ji, Z.X.: Two-party quantum private comparison with five-qubit entangled states. Int. J. Theor. Phys. **56**(5), 1517–1529 (2017)

9. Pan, H.M.: Quantum private comparison based on x-type entangled states. Int. J. Theor. Phys. **56**(10), 3340–3347 (2017)
10. Ji, Z.X., Ye, T.Y.: Multi-party quantum private comparison based on the entanglement swapping of d-level cat states and d-level Bell states. Quantum Inf. Process **16**(7), 177 (2017)
11. Xu, L., Zhao, Z.: A robust and efficient quantum private comparison of equality based on the entangled swapping of GHZ-like state and χ^+ state. Int. J. Theor. Phys. **56**(8), 2671–2685 (2017)
12. 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)
13. Zhou, M.K.: Improvements of quantum private comparison protocol based on cluster states. Int. J. Theo. Phys. **2**, 1–6 (2017)
14. Wu, W.Q., Cai, Q.Y., Wu, S.M., et al.: Cryptanalysis and improvement of Ye et al's quantum private comparison protocol. Int. J. Theor. Phys. **58**(6), 1892–1900 (2019)
15. Hung, S.M., Hwang, S.L., Hwang, T., et al.: Multiparty quantum private comparison with almost dishonest third parties for strangers. Quantum Inf. Process. **16**(2), 36 (2017)
16. Wu, W.Q., Cai, Q.Y., Wu, S.M., et al.: Cryptanalysis of He's quantum private comparison protocol and a new protocol. Int. J. Quantum Inf. **17**(3), 1950026 (2019)
17. Lo, H.K.: Insecurity of quantum secure computations. Phys. Rev. A **56**(2), 1154–1162 (1998)
18. Lin, J., Yang, C.W., Hwang, T.: Quantum private comparison of equality protocol without a third party. Quantum Inf. Process. **13**(2), 157 (2013)
19. He, G.P.: Quantum private comparison protocol without a third party. Int. J. Quantum Inf. **15**(2), 1750014 (2016)
20. He, G.P.: Device-independent quantum private comparison protocol without a third party. arXiv:1710.05051
21. Gockenbach, M.S.: Finite-dimensional linear algebra. CRC Press, Boca Raton (2010)
22. Wilmott, C., Wild, P.: On a generalized quantum SWAP gate. Int. J. Quantum Inf. **10**(03), 1250034 (2008)
23. Wang, T.Y., Wen, Q.Y., Zhu, F.C.: Cryptanalysis of multiparty quantum secret sharing with Bell states and Bell measurements. Optics Communications **284**(6), 1711–1713 (2011)
24. Wang, W., Cao, H.: An Improved Multiparty Quantum Secret Sharing with Bell States and Bell Measurement. Int. J. Theor. Phys. **52**(6), 2099–2111 (2013)
25. Lin, J., Hwang, T.: An enhancement on Shi others.'s multiparty quantum secret sharing protocol. Opt. Commun. **284**(5), 1468–1471 (2011)
26. Tseng, H.Y., Lin, J., Hwang, T.: New quantum private comparison protocol using EPR pairs. Quantum Inf. Process. **11**(2), 373–384 (2012)
27. Zhou, M.K.: Improvements of quantum private comparison protocol based on cluster states. Int. J. Theor. Phys. **2**, 1–6 (2017)