An efficient protocol for the quantum private comparison of equality with W state

Wen Liu *, Yong-Bin Wang, Zheng-Tao Jiang

School of Computer Science, Communication University of China, Beijing 100024, China

A R T I C L E   I N F O

Article history:
Received 12 October 2010
Received in revised form 5 February 2011
Accepted 9 February 2011
Available online 26 February 2011

Keywords:
Quantum private comparison
W state
Single-particle measurement
Correctness
Security

A B S T R A C T

We propose an efficient quantum protocol for comparing the equal information with the help of a semi-honest third party (TP). Our protocol utilizes the triplet W states and the single-particle measurement. A precise proof of security of the protocol is presented. The security of this protocol with respect to various kinds of outside attacks is discussed. Outside eavesdroppers cannot learn any information about the private information. The security of this protocol with respect to various kinds of party attacks is also discussed. One party cannot learn any information about the other's private information. The TP cannot learn any information about the private information, even about the comparison result or the length of secret inputs.

1. Introduction

In the last decade many interesting applications have been developed based on quantum information, such as quantum key distribution (QKD) [1–8], quantum secret sharing (QSS) and authentication [9–17], quantum secure direction communication (QSDC) [18–23], quantum teleportation [24–26], and so on. Secure multi-party computation (SMC) deals with computing a function on secret inputs in a distributed network where each party holds one of the secret inputs, and that no more information is revealed to a party in the computation than can be inferred from that party's input and output. In theory, the general SMC problem can be solved by circuit cluster, but Goldreich pointed out [27,28] that the general solution for special SMC problem is impractical and special solution for special SMC problem should be developed for efficiency reasons. At present, the research on special SMC problem is of great interest in classical setting [29]. And in [30], Shor pointed out that SMC tasks can be performed more efficiently by models based on quantum setting than those based on classical setting. This viewpoint leads us to explore the special SMC problems based on quantum information. Recently many special SMC problems have been solved in quantum setting, such as secure multiparty quantum summation [31], quantum protocols for anonymous voting and surveying [32], etc.

The problem for private comparison of equality or socialist millionaires' problem [33] is an important special SMC problem. Two millionaires want to know whether they happen to be equally rich, but neither millionaire wants to simply disclose its wealth information to the other. It's an extended problem of the millionaire's problem, introduced by Yao [34,35] in which two millionaires wish to compare their riches to determine who is richer without disclosing any information about their riches to each other. The problem for private comparison of equality based on classical cryptography was studied in [36–39] and they cannot withstand powerful quantum computers. Recently, Yang et al. [40] proposed an efficient quantum private comparison protocol based on the decoy photon and two-photon entangled Einstein–Podolsky–Rosen (EPR) pairs. Yang’s protocol included a dishonest TP. Chen et al. [41] proposed a new protocol for dealing with the private comparison of equal information based on the triplet entangled states Greenberger–Horne–Zeilinger (GHZ). This protocol included a semi-honest TP. Chen et al. also pointed out that other entanglement carrier, such as non-maximally entanglement state, W state, can also be further considered for the private comparison of equal information.

In this paper, following some ideas of the quantum computation protocols [19,30,40,41], we propose a new protocol for dealing with the private comparison of equal information based on the W state \( | \rangle = \frac{1}{\sqrt{3}} (|001 \rangle + |010 \rangle + |100 \rangle ) \). Similar to some previous protocols [40,41], our protocol includes a third party, i.e., TP. The role of TP is only to do some calculations. By comparison, this protocol has its own advantages. The W state is more robust against loss of any single qubit than GHZ state. The parties are only required to carry out the simpler single-particle measurement instead of the two-particle Bell-basis measurement. The TP cannot learn anything about the private information, even about the comparison result or the length of secret inputs. And we also use the block transmission method to send qubits in a batch by batch way, which was proposed in [18].

The structure of this paper is as follows: we propose an efficient quantum private comparison for equal information protocol in...
Section 2 and we analyze the protocol of this protocol in Section 3. A brief discussion and the concluding summary are given in Section 4.

2. The quantum private comparison of equal information

The following protocol allows two parties, Alice and Bob, to determine whether their private information $X$ and $Y$ are equal, but except the result Bob learns nothing about $X$ and Alice learns nothing about $Y$.

The protocol for quantum private comparison of equal information 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 $F_{2^n}$ are $(x_0, x_1, \ldots, x_{n-1})$, $(y_0, y_1, \ldots, y_{n-1})$, where $x_i, y_i \in \{0, 1\}$; $X = \sum_{i=0}^{n-1} x_i 2^i$, $Y = \sum_{i=0}^{n-1} y_i 2^i$; $2^{n-1} \leq \max(x, y) \leq 2^n$.

Output: $X = Y$ or $X \neq Y$.

The 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 key $K_{BC}$.

(a) Two parties, Alice and Bob, agree that $|01\rangle$, $|10\rangle$, $|01\rangle$ represent information 1, $|10\rangle$, $|00\rangle$ represent information 0.

(b) Alice and Bob share two groups of triplet W states. Sharing a group of triplet W states could follow the way in [16]. Alice (Bob) prepares $N$ three-qubit W states, each of which is randomly in one of the two states:

$$|\psi_1\rangle = \frac{1}{\sqrt{3}} (|100\rangle + |010\rangle + |001\rangle)_{123},$$

$$|\psi_2\rangle = \frac{1}{\sqrt{3}} (|10+\rangle + |01+\rangle + |00-\rangle)_{123},$$

where 1, 2 and 3 represent the three particles of W state. We denote the ordered $N$ three qubits W states prepared by Alice (Bob) with:

$$P^A_0(1, 2, 3), P^A_1(1, 2, 3), \ldots, P^A_{N-1}(1, 2, 3)$$

(hereafter called $S_A(S_B)$ sequence), where the subscript indicates the order of the state in W sequence. Alice (Bob) takes particles 1 and 2 from each state in $S_A(S_B)$ to form an ordered particle sequence:

$$P^A_0(1, 2), P^A_1(1, 2), \ldots, P^A_{N-1}(1, 2)$$

which is called $S_A^I(S_B^I)$ sequence. The remaining partner particles in $S_A(S_B)$

$$P^A_0(3), P^A_1(3), \ldots, P^A_{N-1}(3)$$

which is called $S_A^S(S_B^S)$ sequence.

Alice (Bob) performs operation $I$ or $U$ on the particle 3 sequence $S_A^S(S_B^S)$ according to $(x_0, x_1, \ldots, x_{n-1})$, $(y_0, y_1, \ldots, y_{n-1})$.

$$I = |0\rangle\langle 0| + |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$U = |0\rangle\langle 1| + |1\rangle\langle 0| = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

For $i = 0$ to $N-1$ do:

If $x_i(y_i) = 0$, Alice (Bob) performs operation $I$ on $P^A_0(3)$($P^B_0(3)$); If $x_i(y_i) = 1$, Alice (Bob) performs operation $U$ on $P^A_0(3)$($P^B_0(3)$).

Alice (Bob) prepares $N^C$ three-qubit W states, each of which is randomly in one of the two states:

$$|\phi_1\rangle = \frac{1}{\sqrt{3}} (|100\rangle + |010\rangle + |001\rangle)_{123},$$

$$|\phi_2\rangle = \frac{1}{\sqrt{3}} (|10+\rangle + |01+\rangle + |00-\rangle)_{123},$$

where 1, 2 and 3 represent the three particles of W state. We denote the ordered $N^C$ three qubits W states prepared by Alice (Bob) with:

$$P^B_0(1, 2, 3), P^B_1(1, 2, 3), \ldots, P^B_{N-1}(1, 2, 3)$$

(hereafter called $S_B(S_A)$ sequence), where the subscript indicates the order of the state in W sequence. Alice (Bob) takes particles 1 and 2 from each state in $S_A(S_B)$ to form an ordered particle sequence:

$$P^B_0(1, 2), P^B_1(1, 2), \ldots, P^B_{N-1}(1, 2)$$

which is called $S_B^I(S_A^I)$ sequence.

Alice inserts $P^B_0(1, 2, 3)$ of $S_A$ into $S_B$ and sends the insert positions sequence $S_{QB}$ to Bob. This new sequence is denoted by $S_{AB}$. Bob inserts $P^B_0(1, 2, 3)$ of $S_B$ into $S_A$ according to $S_{QB}$. This new sequence is denoted by $S_{BA}$.

Alice (Bob) takes particles 1 and 2 from each state in $S_A(S_B)$ to form an ordered particle sequence:

$$P^B_0(1, 2), P^B_1(1, 2), \ldots, P^B_{N+N-1}(1, 2)$$

which is called $S_B^I(S_A^I)$ sequence. The remaining partner particles in $S_A(S_B)$

$$P^B_0(3), P^B_1(3), \ldots, P^B_{N+N-1}(3)$$

which is called $S_B^S(S_A^S)$ sequence.

After doing these, Alice (Bob) sends $S_B^I(S_A^I)$ to Bob (Alice).

Alice (Bob) announces publicly the initial states $S_A(S_B)$. If the initial state is $|01\rangle$, Bob (Alice) has nothing to do; If the initial state is $|10\rangle$, Bob (Alice) performs Hadamard operation on $S_B^S(S_A^S)$.

Both Alice and Bob make single-particle measurement on $S_A$ in the basis $|0\rangle, |1\rangle$. Alice lets Bob announce his measurement result publicly. The measurement results of the communication parties are completely correlated. If Alice’s result is $|10\rangle$ or $|01\rangle (|00\rangle)$, Bob’s result should be $|01\rangle (|10\rangle)$. Alice can then evaluate the error rate during the transmission of $S_A^S$ sequence. If the error rate exceeds the threshold they preset, they abort the scheme. Otherwise, they continue to the next step.
Using the same method, both Alice and Bob make single-particle measurement on $S_p$ in the basis $\{|0\rangle, |1\rangle\}$. Bob can then evaluate the error rate during the transmission of $S^B_p$ sequence. If the error rate exceeds the threshold they preset, they abort the scheme. Otherwise, they continue to the next step.

(3) Alice (Bob) makes single-particle measurement in the basis $\{|0\rangle, |1\rangle\}$ on the particles sequences $S_1^A, S_2^A, S_1^B, S_2^B$.

For $i = 0$ to $N - 1$:

If Alice (Bob) measures $P_i^A(1,2)(P_i^B(1,2))$ and the outcome $M_i^A(M_i^B)$ is $|0\rangle$ or $|1\rangle$, $C_i^{(A)}(C_i^{(B)}) = 1$; If Alice (Bob) measures $P_i^A(1,2)(P_i^B(1,2))$ and the outcome $M_i^A(M_i^B)$ is $|0\rangle$, $C_i^{(A)}(C_i^{(B)}) = 0$.

If Alice (Bob) measures $P_i^A(3)(P_i^B(3))$ and the outcome $M_i^A(M_i^B)$ is $|1\rangle$, $C_i^{(A)}(C_i^{(B)}) = 1$; If Alice (Bob) measures $P_i^A(3)(P_i^B(3))$ and the outcome $M_i^A(M_i^B)$ is $|0\rangle$, $C_i^{(A)}(C_i^{(B)}) = 0$.

Alice (Bob) calculates $C_i = C_i^{A} @ C_i^{B}$, where the symbol $@$ denotes the module 2 addition.

After doing these, Alice (Bob) gets a binary sequence $C_A = (C_0^A, C_1^A, ..., C_{N-1}^A)$, $C_B = (C_0^B, C_1^B, ..., C_{N-1}^B)$.

(4) Alice (Bob) chooses a $L$-length random sequence $C_{\text{random}}(i) = (C_{i0}^A, C_{i1}^A, ..., C_{iL-1}^B)$ where $C_i^A, C_i^B \in \{0, 1\}$, $i = 0, ..., L - 1$. Alice (Bob) sends $C_{\text{random}}(i)$ to Bob (Alice).

Alice inserts $C_i^B(i = 0, ..., L - 1) = C_i^{B}$ into the binary sequence $C_A$ and gets a new $(N + L)$-length binary sequence denoted by $C_{AB}$. Alice also records the index position and sends the index positions sequence $S_q$ to Bob. Bob inserts $C_i^A(i = 0, ..., L - 1) = C_i^{A}$ into the binary sequence $C_B$ according to $S_q$ and gets a new $(N + L)$-length binary sequence denoted by $C_{AB}$. Alice (Bob) uses quantum-one-time pad and $K_{\text{enc}}(K_{\text{dec}})$ to encrypt the new binary sequence $C_{AB}$ and gets $E(C_{AB})(E(C_{AB}))$. Alice (Bob) sends $E(C_{AB})(E(C_{AB}))$ to the third party, Calvin.

(5) After using $K_{\text{enc}},{K}_{\text{dec}}$ to decrypt $E(C_{AB}), E(C_{AB})$ and getting $C_{AB}$, $C_{AB}$, Calvin calculates:

$$R' = \sum_{i=0}^{N-1} (C_i^A @ C_i^B) + \sum_{i=0}^{L-1} (C_i^A @ C_i^B).$$

Calvin sends $R'$ to Alice and Bob.

(6) After receiving $C_{AB}, C_{AB}, R'$, Alice and Bob calculates:

$$R = R' - \sum_{i=0}^{L-1} (C_i^A @ C_i^B).$$

If $R = 0$, Alice and Bob gets $X = Y$; otherwise $X \neq Y$.

In order to improve the efficiency of the protocol, Alice and Bob can follow some ideas in [34] to deal with their two private information. Alice and Bob divide their binary string $(x_0, x_1, ..., x_{N-1}), (y_0, y_1, ..., y_{N-1})$ by way of $(L > 1)$ bits as a group. These groups are denoted by:

$$\begin{bmatrix} A_1, A_2, ..., A_{\lceil L/2 \rceil} \times L \end{bmatrix} \begin{bmatrix} B_1, B_2, ..., B_{\lceil L/2 \rceil} \times L \end{bmatrix}. \quad \text{(14)}$$

We use our protocol to compare two groups $A, B$ belong to Alice and Bob respectively. If $A_i \neq B_i$, they can terminate the comparison and know $X \neq Y$; otherwise they have to continue to compare other groups.

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 representation of $X$ and $Y$ in $F_2^N$ are $(x_0, x_1, ..., x_{N-1}), (y_0, y_1, ..., y_{N-1})$, where $x, y \in \{0, 1\}$.

$$X = \sum_{i=0}^{N-1} x_i 2^i, Y = \sum_{i=0}^{N-1} y_i 2^i, 2^{N-1} \leq \max(x, y) \leq 2^N.$$ 

For $i = 0$ to $N - 1$, Alice and Bob use $W$ state $P_i^A(1,2), P_i^B(1,2)$ to compare whether $x_i, y_i$ are equal. All different cases of $x_i, y_i$'s values are shown in Table 1. We denotes Alice's measurement outcomes of $P_i^A(1,2), P_i^B(3)$ as $M_i^A, M_i^B$ and Bob's measurement outcomes of $P_i^A(3), P_i^B(1,2)$ as $M_i^B, M_i^A$. The codings of $M_i^A, M_i^B$ are denoted as $C_i^A, C_i^B$ and the codings of $M_i^B, M_i^A$ are denoted as $C_i^B, C_i^A$. The results of $C_i^A @ C_i^B, C_i^B @ C_i^A$ are denoted as $C_i^A, C_i^B$, which are send to Calvin. After doing $C_i^A @ C_i^B$ which is denoted by $C_i$, Calvin gets the result of the comparison between $x_i, y_i$. If $C_i = 0$, then $x_i = y_i$; otherwise $x_i \neq y_i$.

We have to point out that in order not to leak the comparing result $X, Y$ to Calvin, Alice and Bob inserts some random into their sequences of $C_i^A, C_i^B$. After eliminating the effect of these random, Alice and Bob can get the result $R = \sum_{i=0}^{N-1} (C_i^A @ C_i^B)$. If $R = 0$, Alice and Bob gets $X = Y$; otherwise $X \neq Y$.

3.2. Security

Firstly, we show that the outside attack is invalid to our protocol. Secondly, we show that the two dishonest parties, Alice and Bob, cannot get any information about the private information of each other and the semi-honest third party, Calvin, cannot get any information about the private information of Alice and Bob, even about the length of $X, Y$ or the comparison result of $X, Y$.

3.2.1. Outside attack

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

In step 1, 3, and 6, there is not any information to transfer. In step 2, the outside eavesdropper can attack the quantum channel when Alice and Bob share two groups of triplet W states. These two groups of triplet W states are not leaked to an unauthorized user. It was shown in [23] that outside eavesdropper’s several kinds of attacks, such as the intercept-resend attack, the collective attack, were detected with nonzero probability during the security checking process and the protocol was secure with a noise quantum channel. In step 4, Alice and Bob send the new binary sequences $C_{AB}, C_{AB}$ to the third party, Calvin, through the secure channels. The outside eavesdropper can eavesdrop anything from these two channels. In step 5, Calvin sends $R'$ to Alice and Bob. Because there is a part of random in $R'$, outside eavesdropper cannot get the comparing result. So in every step of our protocol, the outside eavesdropper cannot get any information $X$ and $Y$.

3.2.2. Party attack

We analyze the possibility of the three parties to get information about $X$ and $Y$ in our protocol. Because the role of Alice is same as that of Bob, we firstly analyze the case that Alice wants to learn Bob’s private information $Y$. Secondly, we analyze the case that the third party, Calvin, wants to learn the private information $X, Y$.

<table>
<thead>
<tr>
<th>$x_i$, $y_i$</th>
<th>$M_i^A(M_i^B)$</th>
<th>$M_i^B(M_i^A)$</th>
<th>$C_i^A(C_i^B)$</th>
<th>$C_i^B(C_i^A)$</th>
<th>$C_i$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0, 0</td>
<td>0, 0</td>
<td>0, 0</td>
<td>0, 0</td>
<td>0, 0</td>
<td>0, 0</td>
</tr>
<tr>
<td>0, 1</td>
<td>1, 0</td>
<td>0, 1</td>
<td>1, 0</td>
<td>0, 1</td>
<td>1, 0</td>
</tr>
<tr>
<td>1, 0</td>
<td>0, 1</td>
<td>1, 0</td>
<td>0, 1</td>
<td>1, 0</td>
<td>1, 0</td>
</tr>
<tr>
<td>1, 1</td>
<td>1, 1</td>
<td>1, 1</td>
<td>1, 1</td>
<td>1, 1</td>
<td>1, 1</td>
</tr>
</tbody>
</table>

Table 1: All different cases of $x_i, y_i$'s values.
Case 1. Alice wants to learn Bob's private information $Y$.

Alice can only infer Bob's private information from the measurement $M_{\theta}^Y$ of $P_3^Y(3)$ which is in Alice's hand and $C_3^Y$ which is send from Bob to Calvin. $P_3^Y(3)$ is shared by Bob. Bob shares the 3rd triplet W state $P_3^Y(1,2,3)$ and performs operation $I$ or $U$ on the particle 3 $P_3^Y(3)$ according to $y_i$. No matter that $y_i$ is 0 or 1, Alice's measurement outcome of $P_3^Y(3)$ is $|0\rangle$ or $|1\rangle$. Because these measurement results have the same probability which is shown in Table 1, Alice can't infer any information about Bob's private information $y_i$ from the measurement outcome of $P_3^Y(3)$. $C_3^Y$ is send through the secure channels from Bob to Calvin and Alice cannot eavesdrop any information about $C_3^Y$. So she cannot get any information about Bob's private information.

We can use the same method to analyze that Bob cannot learn any information about Alice's private information $X$.

Case 2. Calvin wants to learn the private information $X, Y$.

Calvin can only infer private information $X, Y$ from $C_{x_i}C_{y_i}$. Because Alice and Bob insert some confusion random, Calvin cannot find out which number is related to $X, Y$ in $C_{x_i}C_{y_i}$. So Calvin cannot learn the private information $X, Y$, even about the comparison result of $x_i, y_i$, and the length of $X, Y$.

4. Discussion and conclusions

In summary, we propose a new quantum private comparison protocol based on the triplet W states and the single-particle measurement. With the help of a semi-honest TP, two parties can know whether the private information $X$ and $Y$ are equal or not. Our protocol cannot only withstand outside attacks, but also preserve the privacy of $X$ and $Y$. Alice and Bob cannot learn private information own by each other. And the semi-honest TP also cannot learn any information about the private information $X, Y$.

In our further works, the quantum private comparison protocol with triplet W state can be studied without two single-direction secure channels and the two-party protocol can be extended to the case of multi-party. The quantum protocol for the millionaires problem can be also studied.

Acknowledgments

This paper is supported by Beijing Municipal Special Fund for Cultural and Creative Industries (2009); the Engineering Course Programming Project of Communication University of China, Grant No. XNG0925; the National “211” Development Fund for Key Engineering Programs; and the Beijing Municipal Natural Science Foundation (4112052).

References
