Int J Theor Phys (2012) 51:69–77
DOI 10.1007/s10773-011-0878-8

A Protocol for the Quantum Private Comparison of Equality with χ-Type State

Wen Liu · Yong-Bin Wang · Zheng-Tao Jiang · Yi-Zhen Cao

Received: 30 March 2011 / Accepted: 28 June 2011 / Published online: 19 July 2011

Abstract We present a new quantum protocol for comparing the equal information with the help of a semi-honest third party (TP). Different from previous protocols, we utilize the four-particle χ-type states as the information carriers. Various kinds of outside attacks and participant attacks are discussed in detail. One party cannot learn 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.

Keywords Quantum private comparison · χ-Type state · Correctness · Security

1 Introduction

With the development of quantum mechanics, quantum information has attracted a lot of attention and many protocols of quantum information have been developed for quantum key distribution (QKD) [1–7], quantum secret sharing (QSS) [8–11], quantum secure direction communication (QSDC) [12–17], quantum teleportation (QT) [18, 19], and so on. Now, secure multiparty computation (SMC) has been discussed in the quantum field. Many special SMC problems have been solved in quantum setting, for instance, secure multiparty quantum summation [20, 21], quantum protocol for anonymous voting and surveying [22, 23], quantum protocol for millionaire problem [24], etc.

The problem for private comparison of equality or socialist millionaires' problem [25] is an important special SMC problem, in which two millionaires want to know whether they happen to be equally rich without disclosing any information about their riches to each other. It's an extended problem of the millionaire's problem. The millionaire's problem introduced by Yao [26, 27] was the origin of SMC. The problem for private comparison of equality was well-studied based on classical cryptography [28–31], but they cannot withstand powerful

W. Liu (✉) · Y.-B. Wang · Z.-T. Jiang · Y.-Z. Cao
School of Computer Science, Communication University of China, Beijing 100024, China
e-mail: lw8206@gmail.com

quantum computers. Recently, Yang et al. [32] 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. Then, Chen et al. [33] 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. Then, Liu et al. [34] proposed a new protocol for dealing with the private comparison of equal information based on the triplet W states and the single-particle measurement. This protocol included a semi-honest TP.

Enlightened by the works of [32–34], we proposed a new protocol for dealing with the private comparison of equal information based on χ-type genuine four-particle entangled state [35], which is a new state. The χ-type state is different from four-particle GHZ or W state under stochastic local operations and classical communication (SLOCC), and optimally violates a new Bell inequality [36]. Employed it, a two-particle arbitrary state can be teleported. Moreover, it is not reducible to two EPR pairs. So it may be a genuine four-particle entangled state similar to an EPR state. Based on its peculiar construction, it can realize some special communication functions, whereas the four-particle GHZ or W states may be incapable of realizing. In this paper, using χ-type state to solve the problem for private comparison of equality is a new application of χ-type state. Similar to some previous protocols [32–34], our protocol includes a semi-honest third party, i.e., TP. The role of TP is to execute the protocol loyally and record all the results of its intermediate computations. But 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 idea of the block transmission method to send qubits in a batch by batch way in our protocol, which was proposed in [12].

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

2 The Quantum Private Comparison of Equal Information

Before describing this protocol, similar to [35–38], let us define sixteen χ-type states as follows:

$$\begin{aligned}|\chi^{00}\rangle_{abcd} &= \frac{\sqrt{2}}{4}(|0000\rangle - |0101\rangle + |0011\rangle + |0110\rangle \\ &\quad + |1001\rangle + |1010\rangle + |1100\rangle - |1111\rangle)_{abcd} \\ &= \frac{1}{2}(|\phi^+\rangle|00\rangle + |\phi^-\rangle|11\rangle - |\psi^-\rangle|01\rangle + |\psi^+\rangle|10\rangle) \\ &= \frac{1}{2}(|00\rangle|\phi^+\rangle + |11\rangle|\phi^-\rangle - |01\rangle|\psi^-\rangle + |10\rangle|\psi^+\rangle),\end{aligned} \tag{1}$$

where $|\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle|10\rangle)$, $|\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$.

The other fifteen χ-type states can be obtained by the following way:

$$|\chi^{ij}\rangle_{abcd} = \sigma_a^i \sigma_c^j |\chi^{00}\rangle_{abcd} \quad (i, j = 0, 1, 2, 3). \tag{2}$$

Where, σ^i belongs to one of four Pauli operators: $\sigma^0 = I = |0\rangle\langle 0| + |1\rangle\langle 1|$, $\sigma^1 = \sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|$, $\sigma^2 = \sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|$, $\sigma^3 = \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$.

For simplicity, we consider that there are two parties, Alice and Bob. Alice has a private information X, Bob has a private information Y. The binary representations

of X and Y in F_{2^N} are $(x_0, x_1, \ldots, x_{N-1})$ and $(y_0, y_1, \ldots, y_{N-1})$, where $x_i, y_i \in \{0, 1\}$; $X = \sum_{i=0}^{N-1} x_i 2^i$, $Y = \sum_{i=0}^{N-1} y_i 2^i$; $2^{N-1} \leq \max\{x, y\} \leq 2^N$. They want to determine whether their private information X and Y are equal with a help of the semi-honest third party Calvin, but except the result Bob learns nothing about X and Alice learns nothing about Y.

Supposed that two parties, Alice and Bob, use a QKD protocol to establish three common secret keys K_A, K_B, K_{AB}, 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}

The protocol for quantum private comparison of equal information is described as follow:

(1) Alice (Bob) divides her(his) binary representation of $X(Y)$ into $\lceil \frac{N}{4} \rceil$ groups $G_1^A, G_2^A, \ldots, G_{\lceil \frac{N}{4} \rceil}^A (G_1^B, G_2^B, \ldots, G_{\lceil \frac{N}{4} \rceil}^B)$. Each group $G_i^A (G_i^B)$ $(i = 1, \ldots, \lceil \frac{N}{4} \rceil)$ includes four binary bits in $X(Y)$. If $N \mod 4 = n$ $(n \neq 0)$, Alice (Bob) adds n 0 into the last group $G_{\lceil \frac{N}{4} \rceil}^A (G_{\lceil \frac{N}{4} \rceil}^B)$.

(2) Alice prepares a group of four-particle χ-type states $|\chi^{00}\rangle_{abcd}$. Whereafter, she arranges these χ-type states into one sequence

$$[P_1^{a1}, P_1^{b1}, P_1^{c1}, P_1^{d1}, P_2^{a1}, P_2^{b1}, P_2^{c1}, P_2^{d1}, \ldots, P_{2\lceil \frac{N}{4} \rceil}^{a\lceil \frac{N}{4} \rceil}, P_{2\lceil \frac{N}{4} \rceil}^{b\lceil \frac{N}{4} \rceil}, P_{2\lceil \frac{N}{4} \rceil}^{c\lceil \frac{N}{4} \rceil}, P_{2\lceil \frac{N}{4} \rceil}^{d\lceil \frac{N}{4} \rceil}] \quad (3)$$

(hereafter called sequence S_A), where the a, b, c, d represent four particles in one χ-type state and the subscripts $1, 2, 3, \ldots, 2\lceil \frac{N}{4} \rceil$ indicate the χ-type state in the sequence.

Alice prepares another group of χ-type states $|\chi^{00}\rangle_{abcd}$. She arranges these χ-type states into one sequence

$$[P_1^{a'}, P_1^{b'}, P_1^{c'}, P_1^{d'}, P_2^{a'}, P_2^{b'}, P_2^{c'}, P_2^{d'}, \ldots, P_L^{a'}, P_L^{b'}, P_L^{c'}, P_L^{d'}] \quad (4)$$

(hereafter called checking sequence $S_A^{'}$), where the a, b, c, d represent four particles in one χ-type state and the subscripts $1, 2, 3, \ldots, L$ indicate the χ-type state in the sequence. The checking sequence $S_A^{'}$ is used to check the security of quantum channel.

Alice inserts the χ-type states of $S_A^{'}$ into S_A and records the insert positions sequence Sq. This new sequence is denoted by $S_A^{''}$.

Alice takes a, b particles from each χ-type state in $S_A^{''}$ to form an ordered sequence

$$[P_1^{a1}, P_1^{b1}, \ldots, P_1^{a'}, P_1^{b'}, \ldots, P_k^{ah}, P_k^{bh}, \ldots, P_j^{a'}, P_j^{b'}, \ldots, P_L^{a'}, P_L^{b'}, \ldots, P_{2\lceil \frac{N}{4} \rceil}^{a\lceil \frac{N}{4} \rceil}, P_{2\lceil \frac{N}{4} \rceil}^{b\lceil \frac{N}{4} \rceil}], \quad (5)$$

which is called $S_A^{ab''}$

The remaining partner c, d particles form another ordered sequence

$$[P_1^{c1}, P_1^{d1}, \ldots, P_1^{c'}, P_1^{d'}, \ldots, P_k^{ch}, P_k^{dh}, \ldots, P_j^{c'}, P_j^{d'}, \ldots, P_L^{c'}, P_L^{d'}, \ldots, P_{2\lceil \frac{N}{4} \rceil}^{c\lceil \frac{N}{4} \rceil}, P_{2\lceil \frac{N}{4} \rceil}^{d\lceil \frac{N}{4} \rceil}], \quad (6)$$

which is called $S_A^{cd''}$.

Alice sends $S_A^{cd''}$ to Bob and remains $S_A^{ab''}$ herself.

(3) After receiving $S_A^{cd''}$, Alice sends Sq to Bob. According to Sq, Bob performs measurements on the particles $P_i^{c'}, P_i^{d'} (i = 1, 2, \ldots, L)$ using the basis $\{|0\rangle, |1\rangle\}$ or Bell-basis $\{|\phi^{\pm}\rangle, |\psi^{\pm}\rangle\}$ randomly. Finishing measurement, Bob tells Alice his measurement results and his measurement bases.

After receiving Bob's measurement results and his measurement bases, Alice performs the measurement according to Sq using the appropriate bases. If Bob's measurement basis is $\{|0\rangle, |1\rangle\}$, Alice selects Bell-basis; If Bob's measurement basis is Bell-basis, Alice selects $\{|0\rangle, |1\rangle\}$. Alice can then evaluate the error rate during the transmission of sequence $S_A^{cd''}$ according to their measurement results. The measurement outcomes should be correlative perfectly according to (1). If the error rate exceeds the threshold they preset, they abort the scheme. Otherwise, they continue to the next step.

(4) Alice and Bob discard the χ-type states which is used to check eavesdropping. Then they divide remaining χ-type states into some groups. There are two χ-type states including four particles in each group. The group owned by Alice (Bob) is denoted by $(P_k^{ah}, P_k^{bh}, P_{k+1}^{ah}, P_{k+1}^{bh})((P_k^{ch}, P_k^{dh}, P_{k+1}^{ch}, P_{k+1}^{dh}))$, where $k = 1, 3, \ldots, 2\lceil \frac{N}{4} \rceil - 1; h = 1, 2, \ldots, \lceil \frac{N}{4} \rceil$. Both Alice and Bob make χ-type state measurements on four particles in their hands. Obviously, this is the entanglement swapping of χ-type state and the states of particles (a, b, c, d, a, b, c, d) can be denoted as follows:

$$\begin{aligned}
|\chi^{00}\rangle_{abab}|\chi^{00}\rangle_{cdcd} = \frac{1}{4}(&|\chi^{00}\rangle_{abab}|\chi^{00}\rangle_{cdcd} + |\chi^{01}\rangle_{abab}|\chi^{12}\rangle_{cdcd} \\
&+ |\chi^{02}\rangle_{abab}|\chi^{11}\rangle_{cdcd} + |\chi^{03}\rangle_{abab}|\chi^{03}\rangle_{cdcd} \\
&+ |\chi^{10}\rangle_{abab}|\chi^{10}\rangle_{cdcd} + |\chi^{11}\rangle_{abab}|\chi^{02}\rangle_{cdcd} \\
&+ |\chi^{12}\rangle_{abab}|\chi^{01}\rangle_{cdcd} + |\chi^{13}\rangle_{abab}|\chi^{13}\rangle_{cdcd} \\
&+ |\chi^{20}\rangle_{abab}|\chi^{33}\rangle_{cdcd} + |\chi^{21}\rangle_{abab}|\chi^{21}\rangle_{cdcd} \\
&+ |\chi^{22}\rangle_{abab}|\chi^{22}\rangle_{cdcd} + |\chi^{23}\rangle_{abab}|\chi^{30}\rangle_{cdcd} \\
&+ |\chi^{30}\rangle_{abab}|\chi^{23}\rangle_{cdcd} + |\chi^{31}\rangle_{abab}|\chi^{31}\rangle_{cdcd} \\
&+ |\chi^{32}\rangle_{abab}|\chi^{32}\rangle_{cdcd} + |\chi^{33}\rangle_{abab}|\chi^{20}\rangle_{cdcd}).
\end{aligned} \tag{7}$$

(5) The measurement result of $(P_k^{ah}, P_k^{bh}, P_{k+1}^{ah}, P_{k+1}^{bh})((P_k^{ch}, P_k^{dh}, P_{k+1}^{ch}, P_{k+1}^{dh}))$ is $|\chi^{i_h^A j_h^A}\rangle_{abab}(|\chi^{i_h^B j_h^B}\rangle_{cdcd})$, where $i_h^A, j_h^A, i_h^B, j_h^B = 0, 1, 2, 3; h = 1, 2, \ldots, \lceil \frac{N}{4} \rceil$. The binary representation of $i_h^A j_h^A (i_h^B j_h^B)$ is denoted by $G_h^{A'} = (r_1^{Ah} r_2^{Ah} r_3^{Ah} r_4^{Ah})$ $(G_h^{B'} = (r_1^{Bh} r_2^{Bh} r_3^{Bh} r_4^{Bh}))$, where $h = 1, 2, \ldots, \lceil \frac{N}{4} \rceil$.

If $|\chi^{i_h^A j_h^A}\rangle_{abab} = |\chi^{00}\rangle_{abab}$ or $|\chi^{03}\rangle_{abab}$ or $|\chi^{10}\rangle_{abab}$ or $|\chi^{13}\rangle_{abab}$ or $|\chi^{21}\rangle_{abab}$ or $|\chi^{22}\rangle_{abab}$ or $|\chi^{31}\rangle_{abab}$ or $|\chi^{32}\rangle_{abab}$, Alice sets $R_h^{AB} = (R_1^{ABh} R_2^{ABh} R_3^{ABh} R_4^{ABh}) = (0000)$; Otherwise Alice sets $R_h^{AB} = (R_1^{ABh} R_2^{ABh} R_3^{ABh} R_4^{ABh}) = (0111)$.

Alice calculates $R_h^A = G_h^A \oplus G_h^{A'} \oplus R_h^{AB} = R_1^{Ah} R_2^{Ah} R_3^{Ah} R_4^{Ah}$; Bob calculates $R_h^B = G_h^B \oplus G_h^{B'} = R_1^{Bh} R_2^{Bh} R_3^{Bh} R_4^{Bh}$, where the symbol $\oplus$ denotes the bitwise XOR operation.

Alice (Bob) chooses L random quads $R_1^{A'}, R_2^{A'}, \ldots, R_L^{A'} (R_1^{B'}, R_2^{B'}, \ldots, R_L^{B'})$, where $R_h^{A'} = (R_1^{Ah'} R_2^{Ah'} R_3^{Ah'} R_4^{Ah'})(R_h^{B'} = (R_1^{Bh'} R_2^{Bh'} R_3^{Bh'} R_4^{Bh'}))$ and $R_1^{Ah'}, R_2^{Ah'}, R_3^{Ah'}, R_4^{Ah'}, R_1^{Bh'}, R_2^{Bh'}, R_3^{Bh'}, R_4^{Bh'} \in \{0, 1\}, h = 1, \ldots, L$. Alice (Bob) uses quantum-one-time pad and $K_A(K_B)$ to encrypt $R_1^{A'}, R_2^{A'}, \ldots, R_L^{A'} (R_1^{B'}, R_2^{B'}, \ldots, R_L^{B'})$ and sends the result $E_{K_A}(R_1^{A'}, R_2^{A'}, \ldots, R_L^{A'})(E_{K_B}(R_1^{B'}, R_2^{B'}, \ldots, R_L^{B'}))$ to Bob. Alice (Bob) uses $K_A(K_B)$ to decrypt $E_{K_B}(R_1^{B'}, R_2^{B'}, \ldots, R_L^{B'})(E_{K_A}(R_1^{A'}, R_2^{A'}, \ldots, R_L^{A'}))$ and gets $R_1^{B'}, R_2^{B'}, \ldots, R_L^{B'}$ $(R_1^{A'}, R_2^{A'}, \ldots, R_L^{A'})$.

Alice inserts $R_h^{A'}(h=1,\ldots,L)$ into the sequence $R_1^A, R_2^A, \ldots, R_{\lceil \frac{N}{4} \rceil}^A$ and gets a new $(\lceil \frac{N}{4} \rceil + L)$-length quads sequence denoted by $R_1^{A''}, R_2^{A''}, \ldots, R_{\lceil \frac{N}{4} \rceil + L}^{A''}$. Alice also records the insert positions sequence Sq and insert several 0 into Sq to form a new sequence Sq'. Alice uses quantum-one-time pad and K_{AB} to encrypt Sq' and sends the result $E_{K_{AB}}(Sq')$ to Bob.

Bob uses K_{AB} to decrypt $E_{K_{AB}}(Sq')$, deletes the 0 which is inserted in Sq' and gets Sq. Bob inserts $R_h^{B'}(h=1,\ldots,L)$ into the sequence $R_1^B, R_2^B, \ldots, R_{\lceil \frac{N}{4} \rceil}^B$ according to Sq and gets a new $(\lceil \frac{N}{4} \rceil + L)$-length quads sequence denoted by $R_1^{B''}, R_2^{B''}, \ldots, R_{\lceil \frac{N}{4} \rceil + L}^{B''}$.

Alice (Bob) uses quantum-one-time pad and $K_{AC}(K_{BC})$ to encrypt the new quads sequence $R_1^{A''}, R_2^{A''}, \ldots, R_{\lceil \frac{N}{4} \rceil + L}^{A''}(R_1^{B''}, R_2^{B''}, \ldots, R_{\lceil \frac{N}{4} \rceil + L}^{B''})$ and gets $E_{K_{AC}}(R_h^{A''})(E_{K_{BC}}(R_h^{B''}))$, where $h = 1, 2, \ldots, \lceil \frac{N}{4} \rceil + L$. Alice (Bob) sends $E_{K_{AC}}(R_h^{A''})(E_{K_{BC}}(R_h^{B''}))$ $(h = 1, 2, \ldots, \lceil \frac{N}{4} \rceil + L)$ to the third party, Calvin.

(6) After using K_{AC}, K_{BC} to decrypt $E_{K_{AC}}(R_h^{A''})$, $E_{K_{BC}}(R_h^{B''})$ and getting $R_h^{A''}, R_h^{B''}$, where $h = 1, 2, \ldots, \lceil \frac{N}{4} \rceil + L$.

Calvin calculates

$$R' = \sum_{h=1}^{\lceil \frac{N}{4} \rceil} \{(R_1^{Ah''} \oplus R_1^{Bh''}) + (R_2^{Ah''} \oplus R_2^{Bh''}) + (R_3^{Ah''} \oplus R_3^{Bh''}) + (R_4^{Ah''} \oplus R_4^{Bh''})\} \tag{8}$$

Calvin sends R' to Alice and Bob.

(7) After receiving $R', R_h^{A'}, R_h^{B'}(h=1,\ldots,L)$, Alice and Bob calculate

$$R = R' - \sum_{h=1}^{L} \{(R_1^{Ah'} \oplus R_1^{Bh'}) + (R_2^{Ah'} \oplus R_2^{Bh'}) + (R_3^{Ah'} \oplus R_3^{Bh'}) + (R_4^{Ah'} \oplus R_4^{Bh'})\} \tag{9}$$

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

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_{2^N} are $(x_0, x_1, \ldots, x_{N-1}), (y_0, y_1, \ldots, y_{N-1})$, where $x_i, y_i \in \{0, 1\}$; $X = \sum_{i=0}^{N-1} x_i 2^i, Y = \sum_{i=0}^{N-1} y_i 2^i$; $2^{N-1} \leq \max\{x, y\} \leq 2^N$. Alice and Bob divide their binary representations of X and Y into $\lceil \frac{N}{4} \rceil$ groups, $G_1^A, \ldots, G_{\lceil \frac{N}{4} \rceil}^A$ and $G_1^B, \ldots, G_{\lceil \frac{N}{4} \rceil}^B$.

For $h = 1$ to $\lceil \frac{N}{4} \rceil$, Alice and Bob use two χ-type states $[P_k^{ah}, P_k^{bh}, P_k^{ch}, P_k^{dh}, P_{k+1}^{ah}, P_{k+1}^{bh}, P_{k+1}^{ch}, P_{k+1}^{dh}]$ to compare whether G_h^A, G_h^B are equal. For simplicity, two cases of G_h^A, G_h^B's values are shown in Table 1 and other cases can use the same way to get. We denotes Alice's measurement outcome of $P_k^{ah}, P_k^{bh}, P_{k+1}^{ah}$, P_{k+1}^{bh} as M_h^A and Bob's measurement outcome of $P_k^{ch}, P_k^{dh}, P_{k+1}^{ch}, P_{k+1}^{dh}$ as M_h^B. The represents of M_h^A, M_h^B are denoted as $G_h^{A'}, G_h^{B'}$. The results of $G_h^A \oplus G_h^{A'}, G_h^B \oplus G_h^{B'}$ are denoted as R_h^A, R_h^B, which are send to Calvin. The represent of auxiliary data is denoted as R_h^{AB},

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

G_h^A	G_h^B	M_h^A	M_h^B	$G_h^{A'}$	$G_h^{B'}$	R_h^A	R_h^B	R_h^{AB}	R_h
0000	0000	$\|\chi^{00}\rangle_{abab}$	$\|\chi^{00}\rangle_{cdcd}$	0000	0000	$0000 \oplus 0000$	$0000 \oplus 0000$	0000	0
		$\|\chi^{01}\rangle_{abab}$	$\|\chi^{12}\rangle_{cdcd}$	0001	0110	$0000 \oplus 0001$	$0000 \oplus 0110$	0111	0
		$\|\chi^{02}\rangle_{abab}$	$\|\chi^{11}\rangle_{cdcd}$	0010	0101	$0000 \oplus 0010$	$0000 \oplus 0101$	0111	0
		$\|\chi^{03}\rangle_{abab}$	$\|\chi^{03}\rangle_{cdcd}$	0011	0011	$0000 \oplus 0011$	$0000 \oplus 0011$	0000	0
		$\|\chi^{10}\rangle_{abab}$	$\|\chi^{10}\rangle_{cdcd}$	0100	0100	$0000 \oplus 0100$	$0000 \oplus 0100$	0000	0
		$\|\chi^{11}\rangle_{abab}$	$\|\chi^{02}\rangle_{cdcd}$	0101	0010	$0000 \oplus 0101$	$0000 \oplus 0010$	0111	0
		$\|\chi^{12}\rangle_{abab}$	$\|\chi^{01}\rangle_{cdcd}$	0110	0001	$0000 \oplus 0110$	$0000 \oplus 0001$	0111	0
		$\|\chi^{13}\rangle_{abab}$	$\|\chi^{13}\rangle_{cdcd}$	0111	0111	$0000 \oplus 0111$	$0000 \oplus 0111$	0000	0
		$\|\chi^{20}\rangle_{abab}$	$\|\chi^{33}\rangle_{cdcd}$	1000	1111	$0000 \oplus 1000$	$0000 \oplus 1111$	0111	0
		$\|\chi^{21}\rangle_{abab}$	$\|\chi^{21}\rangle_{cdcd}$	1001	1001	$0000 \oplus 1001$	$0000 \oplus 1001$	0000	0
		$\|\chi^{22}\rangle_{abab}$	$\|\chi^{22}\rangle_{cdcd}$	1010	1010	$0000 \oplus 1010$	$0000 \oplus 1010$	0000	0
		$\|\chi^{23}\rangle_{abab}$	$\|\chi^{30}\rangle_{cdcd}$	1011	1100	$0000 \oplus 1011$	$0000 \oplus 1100$	0111	0
		$\|\chi^{30}\rangle_{abab}$	$\|\chi^{23}\rangle_{cdcd}$	1100	1011	$0000 \oplus 1100$	$0000 \oplus 1011$	0111	0
		$\|\chi^{31}\rangle_{abab}$	$\|\chi^{31}\rangle_{cdcd}$	1101	1101	$0000 \oplus 1101$	$0000 \oplus 1101$	0000	0
		$\|\chi^{32}\rangle_{abab}$	$\|\chi^{32}\rangle_{cdcd}$	1110	1110	$0000 \oplus 1110$	$0000 \oplus 1110$	0000	0
		$\|\chi^{33}\rangle_{abab}$	$\|\chi^{20}\rangle_{cdcd}$	1111	1000	$0000 \oplus 1111$	$0000 \oplus 1000$	0111	0
0011	1100	$\|\chi^{00}\rangle_{abab}$	$\|\chi^{00}\rangle_{cdcd}$	0000	0000	$0011 \oplus 0000$	$1100 \oplus 0000$	0000	4
		$\|\chi^{01}\rangle_{abab}$	$\|\chi^{12}\rangle_{cdcd}$	0001	0110	$0011 \oplus 0001$	$1100 \oplus 0110$	0111	4
		$\|\chi^{02}\rangle_{abab}$	$\|\chi^{11}\rangle_{cdcd}$	0010	0101	$1100 \oplus 0010$	$0011 \oplus 0101$	0111	4
		$\|\chi^{03}\rangle_{abab}$	$\|\chi^{03}\rangle_{cdcd}$	0011	0011	$0011 \oplus 0011$	$1100 \oplus 0011$	0000	4
		$\|\chi^{10}\rangle_{abab}$	$\|\chi^{10}\rangle_{cdcd}$	0100	0100	$0011 \oplus 0100$	$1100 \oplus 0100$	0000	4
		$\|\chi^{11}\rangle_{abab}$	$\|\chi^{02}\rangle_{cdcd}$	0101	0010	$0011 \oplus 0101$	$1100 \oplus 0010$	0111	4
		$\|\chi^{12}\rangle_{abab}$	$\|\chi^{01}\rangle_{cdcd}$	0110	0001	$0011 \oplus 0110$	$1100 \oplus 0001$	0111	4
		$\|\chi^{13}\rangle_{abab}$	$\|\chi^{13}\rangle_{cdcd}$	0111	0111	$0011 \oplus 0111$	$1100 \oplus 0111$	0000	4
		$\|\chi^{20}\rangle_{abab}$	$\|\chi^{33}\rangle_{cdcd}$	1000	1111	$0011 \oplus 1000$	$1100 \oplus 1111$	0111	4
		$\|\chi^{21}\rangle_{abab}$	$\|\chi^{21}\rangle_{cdcd}$	1001	1001	$0011 \oplus 1001$	$1100 \oplus 1001$	0000	4
		$\|\chi^{22}\rangle_{abab}$	$\|\chi^{22}\rangle_{cdcd}$	1010	1010	$0011 \oplus 1010$	$1100 \oplus 1010$	0000	4
		$\|\chi^{23}\rangle_{abab}$	$\|\chi^{30}\rangle_{cdcd}$	1011	1100	$0011 \oplus 1011$	$1100 \oplus 1100$	0111	4
		$\|\chi^{30}\rangle_{abab}$	$\|\chi^{23}\rangle_{cdcd}$	1100	1011	$0011 \oplus 1100$	$1100 \oplus 1011$	0111	4
		$\|\chi^{31}\rangle_{abab}$	$\|\chi^{31}\rangle_{cdcd}$	1101	1101	$0000 \oplus 1101$	$0000 \oplus 1101$	0000	4
		$\|\chi^{32}\rangle_{abab}$	$\|\chi^{32}\rangle_{cdcd}$	1110	1110	$0011 \oplus 1110$	$1100 \oplus 1110$	0000	4
		$\|\chi^{33}\rangle_{abab}$	$\|\chi^{20}\rangle_{cdcd}$	1111	1000	$0011 \oplus 1111$	$1100 \oplus 1000$	0111	4

which is also send to Calvin. After doing $R_h = \sum_{i=1}^{4} R_i^{Ah} \oplus R_i^{Bh} \oplus R_i^{ABh}$, Calvin gets the result of the comparison between G_h^A, G_h^B. If $R_h = 0$, then $G_h^A = G_h^B$; otherwise $G_h^A \neq G_h^B$.

We have to point out that in order not to leak the comparing result of X, Y to Calvin, Alice and Bob inserts some random into their sequences of $R_h^{A'}, R_h^{B'}, R_h^{AB'} (h = 1, 2, \ldots, \lceil \frac{N}{4} \rceil)$. After eliminating the effect of these random quads, Alice and Bob can get the result $R = \sum_{h=1}^{\lceil \frac{N}{4} \rceil} (\sum_{i=1}^{4} R_i^{Ah} \oplus R_i^{Bh} \oplus R_i^{ABh})$. 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, can not get any information about the private informa-

tion of each other and the semi-honest third party, Calvin, can not 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, 4, 7, there is not any information to transfer. In step 2, the outside eavesdropper can attack the quantum channel when Alice and Bob share a group of four-particle χ-type states. These four-particle χ-type states are not leaked to an unauthorized user. It was shown in [37, 38] that outside eavesdropper's several kinds of attacks, such as the intercept-resend attack, the measure-resend attack, the entangle-measure attack,were detected with nonzero probability during the security checking process and the protocol was secure with a noise quantum channel. In step 5, Alice and Bob send the new quads sequences $R_h^{A''}, R_h^{B''}, R_h^{AB''} (h = 1, 2, \ldots, \lceil \frac{N}{4} \rceil + L)$ to the third party, Calvin, using the quantum-one-time pad. The outside eavesdropper cannot eavesdrop anything. In step 6, 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 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. [39] and has attracted much attention in the cryptanalysis of quantum cryptography [40–45]. We analyze the possibility of the three participants 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.

Case 1: Alice wants to learn Bob's private information Y.

Alice can only infer Bob's private information from the measurement result M_h^A of $P_k^{ah}, P_k^{bh}, P_{k+1}^{ah}, P_{k+1}^{bh}$ which are in Alice's hand and R_h^B which is send from Bob to Calvin. $P_k^{ah}, P_k^{bh}, P_{k+1}^{ah}, P_{k+1}^{bh}$ are the two particles of two χ-type states. According to the (7), Alice can infer the measurement result M_h^B of $P_k^{ch}, P_k^{dh}, P_{k+1}^{ch}, P_{k+1}^{dh}$ which are in Bob's hand. Because these measurement results have the same probability which is shown in Table 1, Alice cannot infer any information about Bob's private information G_h^B from the measurement outcome of M_h^B. R_h^B is send using the quantum-one-time pad from Bob to Calvin and Alice also cannot eavesdrop any information about R_h^B. 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 $R_h^{A''}, R_h^{B''}, R_h^{AB''}$. Because Alice and Bob insert some confusion random, Calvin cannot find out which number is related to X, Y in $R_h^{A''}, R_h^{B''}, R_h^{AB''}$. So Calvin cannot learn the private information X, Y, even about the comparison result of G_h^A, G_h^B and the length of X, Y.

3.3 Discussion and Conclusions

We present a quantum protocol which can be used to solve private comparison problem. Our protocol is based on the χ-type states. It's a new application of the χ-type states. With the help of a semi-honest TP, two parties can know whether the private information X and Y are equal or not. The security of the protocol relies on the laws of quantum mechanics. And various kinds of outside attacks and participant attacks are discussed. The advantage of our protocol is that it can 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 can be studied without the help of the third party and the two-party protocol can be extend to the case of multi-party. The quantum protocols for the millionaire's problem and multi-party sorting problem can be also studied.

Acknowledgements 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

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. 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)
6. 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)
7. Gao, F., Guo, F.Z., Wen, Q.Y., Zhu, F.C.: Quantum key distribution by construction nonorthogonal states with Bell states. Int. J. Mod. Phys. B **24**, 4611–4618 (2010)
8. Karlsson, A., Koashi, M., Imoto, N.: Quantum entanglement for secret sharing and secret splitting. Phys. Rev. A **59**, 052307 (1999)
9. Xiao, L., Long, G.L., Deng, F.G., Pan, J.W.: Efficient multiparty quantum-secret-sharing schemes. Phys. Rev. A **69**, 162–168 (2004)
10. 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)
11. 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)
12. 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)
13. Deng, F.G., Long, G.L.: Secure direct communication with a quantum one-time pad. Phys. Rev. A **69**, 052319 (2004)
14. 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)
15. Wang, J., Zhang, Q., Tang, C.J.: Quantum secure communication scheme with w state. Commun. Theor. Phys. **48**, 637–640 (2007)
16. Lin, S., Wen, Q.Y., Gao, F., Zhu, F.C.: Quantum secure direct communication with chi-type entangled states. Phys. Rev. A **78**, 064304 (2008)
17. 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)

18. 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)
19. Bouwmeester, D., Pan, J.W., et al.: Experimental quantum teleportation. Nature **390**, 575–579 (1997)
20. Du, J.Z., Chen, X.B., Wen, Q.Y., Zhu, F.C.: Secure multi-party quantum summation. Acta Phys. Sin. **56**, 6214 (2007)
21. Chen, X.B., Xu, G., Yang, Y.X., Wen, Q.Y.: An efficient protocol for the secure multi-party quantum summation. Int. J. Theor. Phys. **49**, 2793–2804 (2010)
22. Vaccaro, J.A., Spring, J., Chefles, A.: Quantum protocols for anonymous voting and surveying. Phys. Rev. A **75**, 012333 (2007)
23. Li, Y., Zeng, G.H.: Opt. Rev. **15**, 219 (2008)
24. Jia, H.Y., Wen, Q.Y., Song, T.T., Gao, F.: Quantum protocol for millionaire problem. Opt. Commun. **284**, 545–549 (2011)
25. Markus, J., Moti, Y.: Proving without knowing: on oblivious, agnostic and blindfolded provers. In: Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology, pp. 186–200 (1996)
26. Yao, A.: Protocols for secure computations. In: Proc. 23rd IEEE Symposium on Foundations of Computer Science, pp. 160–164 (1982)
27. Yao, A.: How to generate and exchange secrets. In: Proceedings of the 27th Annual Symposium on Foundations of Computer Science, pp. 162–167 (1986)
28. Fagin, R., Naor, M., Winkler, P.: Comparing information without leaking it. Commun. ACM **39**, 77–85 (1996)
29. Cachin, C.: Efficient private bidding and auctions with an oblivious third party. In: Proceedings of the 6th ACM Conference on Computer and Communications Security, pp. 120–127 (1999)
30. Fabrice, B., Berry, S., et al.: A fair and efficient solution to the socialist millionaires' problem. Discrete Appl. Math. **111**, 23–36 (2001)
31. Qin, J., Zhang, Z.F., Feng, D.G., Li, B.: A protocol of comparing information without leaking. J. Softw. **15**, 421–427 (2004)
32. 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)
33. 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)
34. Liu, W., Wang, Y.B., Jiang, Z.T.: An efficient protocol for the quantum private comparison of equality with W state. Opt. Commun. (2011). doi:10.1016/j.optcom.2011.02.017
35. Yeo, Y., Chua, W.K.: Teleportation and dense coding with genuine multipartite entanglement. Phys. Rev. Lett. **96**, 060502 (2006)
36. Wu, C., Yeo, Y., Kwek, L., Oh, C.: Phys. Rev. A **75**, 032332 (2007)
37. Gao, G., Wang, L.P.: A protocol for bidirectional quantum secure communication based on genuine four-particle entangled states. Commun. Theor. Phys. **75**, 447–451 (2010)
38. Xiu, X.M., Dong, H.K., Dong, L., Gao, Y.J., Chi, F.: Deterministic secure quantum communication using four-particle genuine entangled state and entanglement swapping. Opt. Commun. **282**, 2457–2459 (2009)
39. 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)
40. Qin, S.J., Gao, F., Wen, Q.Y., et al.: Cryptanalysis of the Hillery–Buzek–Berthiaume quantum secret-sharing protocol. Phys. Rev. A **76**, 062324 (2007)
41. 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)
42. 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)
43. 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)
44. Song, T.T., Zhang, J., Gao, F., et al.: Participant attack on quantum secret sharing based on entanglement swapping. Chinese. Physics B **18**, 1333 (2009)
45. 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. A **56**, 445 (2010)