Int J Theor Phys (2016) 55:5307–5317
DOI 10.1007/s10773-016-3150-4

Dynamic Multi-Party Quantum Private Comparison Protocol with Single Photons in Both Polarization and Spatial-Mode Degrees of Freedom

Wen Liu[1] · **Yong-Bin Wang**[1]

Received: 8 March 2016 / Accepted: 29 August 2016 / Published online: 5 September 2016

Abstract A dynamic quantum private comparison protocol based on the single photons in both polarization and spatial-mode degrees of freedom is proposed. In this protocol, any two parties of $n(n \geq 4)$ parties can compare their private information with the help of others $n-2$ parties. And any party can join in the protocol to take part in the comparison of n parties. Correctness analysis shows that the proposed protocol can be used to compare their information correctly. Security analysis shows that the proposed protocol can resist the general active attacks from an outside eavesdropper. And it can overcomes the problem of information leakage.

Keywords Dynamic multi-party quantum private comparison protocol · Single photons in both polarization and spatial-mode degrees of freedom · Correctness · Security · Information leakage

1 Introduction

The problem for private comparison of equality is that two parties want to know whether their private information are equal or not without disclosing their private information. It's an important problem in the filed of secure multi-party computation. The problem for private comparison was well-studied in classical cryptography [1–4], but they cannot withstand powerful quantum computers. In 2009, Yang et al. [5] proposed a quantum private comparison protocol(QPC) based on the decoy photon and two-photon entangled Einstein−Podolsky−Rosen (EPR) pairs. In Yang's protocol, a dishonest third party (TP) is introduced. Then, Chen et al. [6] proposed a new QPC protocol to deal with the private comparison of equal information based on the simple single-particle measurement and the

✉ Wen Liu
lw_8206@163.com

[1] School of Computer Science, Communication University of China, Beijing 100024, China

triplet entangled states Greenberger−Horne−Zeilinger (GHZ). In [7], Tseng et al. proposed a QPC protocol using EPR, which provided easier implementation as well as better qubit efficiency than the other quantum private comparison protocols. In [8–12], Liu et al. proposed some QPC protocols based on the triplet W states, GHZ states, $\chi-$type states and Bell entangled states. These protocols all included a semi-honest third party(TP). In [13, 14], Liu et al. studied the extended problem of QPC. With the help of a semi-honest third party (TP), n parties can compare whether their information are equal or not in one execution of the protocol using d-dimensional Bell states as the information carriers.

In this paper, we proposed a dynamic multi-party quantum private comparison(DQPC) protocol with single photons in both polarization and spatial-mode degrees of freedom. The dynamic character of our protocol is reflected in the following two aspects:

(1) We can randomly choose arbitrary two parties of the n parties to compare their private information with the help of $n-2$ parties and don't disclose any information about their private information. And any two party of the n parties can get their comparison result simultaneously.
(2) Any number of new parties, not only one party, can dynamically join the DQPC protocol and take part in the comparison before the single photon state in both polarization and spatial-mode degrees of freedom are measured. The protocol of n parties can be extend to a protocol of $n+n'$ parties.

In [15], Prof. Du, the earliest researchers of secure multi-party computation, pointed out that extending our two-party computation protocol to secure multi-party protocols is not trivial. So in this paper, we study a multi-party protocol, which is not a simple extend protocol of two parties'. Our multi-party protocol can used in some applications, such as multi-keyword ranking, multi-keyword search and personalized search in [16–21]. For example, there are n_1 keywords $w_1, w_2, ..., w_{n_1}$ which are need to research. The keywords of a paper are $w_{n_1+1}, w_{n_1+2}, ..., w_n$. In order to determine whether $w_1, w_2, ..., w_{n_1} \subseteq w_{n_1+1}, w_{n_1+2}, ..., w_n$, we have to use the protocol $n_1(n-n_1)$ times and need to prepare $n_1(n-n_1)L$ single photons to carry information, where L is the length of every keyword in in F_{2^L}. Using our protocol, we can use the protocol one time, need to prepare L single photons to carry information.

The structure of this paper is as follows: we propose a dynamic quantum private comparison(DQPC) protocol with the single photon in both polarization and spatial-mode degrees of freedom in Section 2; and we analyze the security of this protocol in Section 3. A brief discussion and the concluding summary are given in Section 4.

2 The Dynamic Multi-Party Quantum Private Comparison(DMQPC) Protocol with the Single Photon in Both Polarization and Spatial-Mode Degrees of Freedom

Before describing this protocol, we define a single photon state in both polarization and spatial-mode degrees of freedom as follows:

$$|\phi\rangle = |\phi\rangle_P \otimes |\phi\rangle_S \tag{1}$$

where $|\phi\rangle_P$ and $|\phi\rangle_S$ respectively are the single photon states in the polarization and spatial-mode degrees of freedom. $|\phi\rangle_P \in \{|H\rangle, |V\rangle, |S\rangle_P = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle), |A\rangle_P = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)\}$, here H and V respectively denote the horizontal and vertical polarization of single

photons; $|\phi\rangle_P \in \{|a_1\rangle, |a_2\rangle, |s\rangle_P = \frac{1}{\sqrt{2}}(|a_1\rangle + |a_2\rangle), |a\rangle_S = \frac{1}{\sqrt{2}}(|a_1\rangle - |a_2\rangle)\}$, here a_1 and a_2 respectively represent the upper and lower spatial mode of single photons.

Similar to [15, 16], there are two interesting unitary operations in each degree of freedom of single photons. These unitary operations are:

$$\begin{aligned} I_P &= |H\rangle\langle H| + |V\rangle\langle V|, \quad U_P = |V\rangle\langle H| - |H\rangle\langle V|, \\ I_S &= |a_1\rangle\langle a_1| + |a_2\rangle\langle a_2|, \quad U_S = |a_2\rangle\langle a_1| - |a_1\rangle\langle a_2|. \end{aligned} \tag{2}$$

Using these unitary operations, we can get that:

$$\begin{aligned} &I_P|H\rangle = |H\rangle, && U_P|H\rangle = |V\rangle, \\ &I_P|V\rangle = |V\rangle, && U_P|V\rangle = -|H\rangle, \\ &I_P|S\rangle_P = |S\rangle_P, && U_P|S\rangle_P = -|A\rangle_P, \\ &I_P|A\rangle_P = |A\rangle_P, && U_P|A\rangle_P = |S\rangle_P, \\ &I_S|a_1\rangle = |a_1\rangle, && U_P|a_1\rangle = |a_2\rangle, \\ &I_S|a_2\rangle = |a_2\rangle, && U_P|a_2\rangle = -|a_1\rangle, \\ &I_S|s\rangle_S = |s\rangle_S, && U_S|s\rangle_S = -|a\rangle_S, \\ &I_S|a\rangle_S = |a\rangle_S, && U_P|a\rangle_S = |s\rangle_S. \end{aligned} \tag{3}$$

Supposed that there are $n(n \geq 4)$ parties $P_1, P_2, ..., P_n$. Each of them has a private information $M_i (i = 1, 2, ..., n)$. The length of the private information is L. The secret messages M_i in F_{2^L} of P_i is denoted by $m_1^i, m_2^i, ..., m_L^i (i = 1, 2, ..., n)$. In the DQPC protocol, arbitrary two parties of the n party can compare their private information with the help of others $n-2$ parties and don't disclose any information about their private information. And n' parties can dynamically join in the protocol and take part in the comparison before the states are measured. $P_1, P_2, ..., P_n$ agree that $I_P(I_S)$ encodes 0; $U_P(U_S)$ encodes 1; they also agree that $|H\rangle, |S\rangle_P, |a_1\rangle, |s\rangle_S$ encode 0; $|V\rangle, |A\rangle_P, |a_2\rangle, |a\rangle_S$ encode 1. In our protocol, we introduce a semi-honest third party TP. TP executes the protocol loyally, keeps a record of all its intermediate computations and may try to steal the others parties' private inputs from the record, but he cannot be corrupted by the adversary.

The dynamic multi-party quantum private comparison(DMQPC) protocol with the single photon in both polarization and spatial-mode degrees of freedom is divided into sub-protocol 1 and sub-protocol 2. Sub-protocol 1 describes how n paries compare their private information secretly; Sub-protocol 2 describes how n' additional parties take part in the comparison protocol.

Sub-protocol 1 is as follow:

(1) For $i = 1, 2, ..., n$, P_i divides his binary representation of M_i into $\lceil \frac{L}{2} \rceil$ groups $G_1^i, G_2^i, ..., G_{\lceil \frac{L}{2} \rceil}^i$. Each group $G_j^i (j = 1, ..., \lceil \frac{L}{2} \rceil)$ includes two binary bits of M_i. If $L \mod 2 = 1$, P_i adds one 0 into the last group $G_{\lceil \frac{L}{2} \rceil}^i$.

(2) TP prepares a sequence Sq_{TP} of $\lceil \frac{L}{2} \rceil$ single photons. TP also prepares L' single photons. Each photon is in one of the 8 quantum states $|\phi\rangle = |\phi\rangle_P \otimes |\phi\rangle_S, |\phi\rangle_P \in \{|H\rangle, |V\rangle\}, |\phi\rangle_S \in \{|a_1\rangle, |a_2\rangle\}$ or $|\psi\rangle = |\psi\rangle_P \otimes |\psi\rangle_S, |\psi\rangle_P \in \{|S\rangle_P, |A\rangle_P\}, |\psi\rangle_S \in \{|s\rangle_S, |a\rangle_S\}$. TP also records the coding of Sq_{TP} and the coding sequence is denoted by $Iv_1^1 Iv_1^2, ..., Iv_{\lceil \frac{L}{2} \rceil}^1 Iv_{\lceil \frac{L}{2} \rceil}^2$. And TP inserts L' single photons into Sq_{TP} and gets Sq'_{TP}. TP records the insert positions Po_{TP} and sends Sq'_{TP}, Po_{TP} to P_1.

(3) After receiving $Sq^{'}_{TP}$, Po_{TP}, P_1 chooses $L^{'}$ single photons from Sq_{TP} according to Po_{TP} and measures them with one of 8 bases $|H\rangle \otimes |a_1\rangle, |H\rangle \otimes |a_2\rangle, |V\rangle \otimes |a_1\rangle, |V\rangle \otimes |a_2\rangle, |S\rangle_P \otimes |s\rangle_S, |S\rangle_P \otimes |a\rangle_S, |A\rangle_P \otimes |s\rangle_S, |A\rangle_P \otimes |a\rangle_S$. P_1 publishes his measurement results. TP can determine the error rate according to the measurement and initial states in step(1). If the error rate is smaller than the prior threshold determined by the channel noise, P_1 proceeds to the next step; otherwise P_1 aborts the communication and repeat the step (1).

(4) P_1 discards the measured $L^{'}$ photons and the rest photons of $Sq^{'}_{TP}$ form a sequence Sq_{TP}. P_1 performs $U^1_P \otimes U^2_S (U^1_P \in \{I_P, U_P\}, U^2_S \in \{I_S, U_S\})$ on the jth photon of Sq_{TP} according to G^1_j. These operated photons form a new sequence denoted by Sq_{P_1}. P_1 prepares $L^{'}$ single photons which is the same as the step (2). Each photon is one of the 8 quantum states $|\phi\rangle = |\phi\rangle_P \otimes |\phi\rangle_S$. P_1 inserts $L^{'}$ single photons into Sq_{P_1} and also records the insert position Po_1. P_1 sends the new sequence $Sq^{'}_{P_1}$ and Po_1 to P_2.

(5) For $i = 2, ...n-1, n$

(5.1) After P_i gets $Sq^{'}_{P_{i-1}}$, P_i chooses $L^{'}$ single photons from $Sq^{'}_{P_{i-1}}$ according to Po_{i-1} and measures them with one of 8 bases $|H\rangle \otimes |a_1\rangle, |H\rangle \otimes |a_2\rangle, |V\rangle \otimes |a_1\rangle, |V\rangle \otimes |a_2\rangle, |S\rangle_P \otimes |s\rangle_S, |S\rangle_P \otimes |a\rangle_S, |A\rangle_P \otimes |s\rangle_S, |A\rangle_P \otimes |a\rangle_S$. P_i publishes his measurement results and P_{i-1} can determine the error rate according to the measurements. If the error rate is smaller than the prior threshold determined by the channel noise, P_i proceeds to the next step (5.1); otherwise P_i aborts the communication.

(5.2) P_i discards the measured $L^{'}$ photons and the rest photons of $Sq^{'}_{P_{i-1}}$ form a sequence $Sq_{P_{i-1}}$. P_i performs $U^1_P \otimes U^2_S (U^1_P \in \{I_P, U_P\}, U^2_S \in \{I_S, U_S\})$ on the jth photon of $Sq_{P_{i-1}}$ according to G^i_j, $j = 1, 2, ..., L$. These operated photons form a new sequence denoted by Sq_{P_i}. P_i prepares $L^{'}$ single photons which is the same as the step (2). Each photon is one of the 8 quantum states $|\phi\rangle = |\phi\rangle_P \otimes |\phi\rangle_S$. P_i inserts $L^{'}$ single photons into Sq_{P_i} and also records the insert position Po_i. P_i sends the new sequence $Sq^{'}_{P_i}$ and Po_i to P_{i+1}. If $i = n$, P_n sends the new sequence $Sq^{'}_{P_n}$ and Po_n to TP.

The step(5) will continue until $i = n$

(6) After TP gets $Sq^{'}_{P_n}$, TP and P_n use the same method as step (5.1) to check whether the transmission is secure or not. If the transmission is secure, TP can use the correct base according to the single-photon state in step (1) and get the result denoted by R. The binary representations of R are $r^1_1 r^2_1 ... r^1_{\lceil \frac{L}{2} \rceil} r^2_{\lceil \frac{L}{2} \rceil}$

(7) With the help of TP and others $n-2$ parties, any $P_k (k \in \{1, 2, ..., n\})$ can respectively compare his private information with $P_h (h = 1, 2, ..., k-1, k+1, .., n))$.

For $k = 1, 2, ..., n$, For $h = 1, 2, ..., k-1, k+1, .., n$:

TP sends R to $P_j (j \in \{1, 2, ..., n\}, j \neq k, h)$. The $n-2$ parties calculates

$$
\begin{aligned}
& r^{1'}_{1(kh)} r^{2'}_{1(kh)} = r^1_1 r^2_1 \oplus \bigoplus_{j \in \{1,2,...,n\}, j \neq k,h} G^j_1, \\
& ... \\
& r^{1'}_{\lceil \frac{L}{2} \rceil (kh)} r^{2'}_{\lceil \frac{L}{2} \rceil (kh)} = r^1_{\lceil \frac{L}{2} \rceil} r^2_{\lceil \frac{L}{2} \rceil} \oplus \bigoplus_{j \in \{1,2,...,n\}, j \neq k,h} G^j_{\lceil \frac{L}{2} \rceil}.
\end{aligned} \tag{4}
$$

They also send $r^{1'}_{1(kh)} r^{2'}_{1(kh)}, ..., r^{1'}_{\lceil \frac{L}{2} \rceil (kh)} r^{2'}_{\lceil \frac{L}{2} \rceil (kh)}$ to TP.

TP calculates

$$\begin{aligned} & R^1_{kh} = r^{1'}_{1(kh)} r^{2'}_{1(kh)} \oplus I v^{1'}_1 I v^{2'}_1, \\ & ... \\ & R^{\lceil \frac{L}{2} \rceil}_{kh} = r^{1'}_{\lceil \frac{L}{2} \rceil (kh)} r^{2'}_{\lceil \frac{L}{2} \rceil (kh)} \oplus I v^{1'}_{\lceil \frac{L}{2} \rceil} I v^{2'}_{\lceil \frac{L}{2} \rceil}. \end{aligned} \tag{5}$$

For $k = 1, 2, ..., n$,
For $h = 1, 2, ..., k-1, k+1, .., n$:

$R^1_{kh} =, ..., = R^{\lceil \frac{L}{2} \rceil}_{kh} = 00$, TP can know the private information $M_k = M_h$; otherwise $M_k \neq M_h$.

Sub-protocol 2 is as follow:

Before TP measured Sq'_{P_n}, n' parties can join in the protocol, where n' can be arbitrary integer.

(1) For $i = 1, ..., n'$: P_{n+i} divides his binary representation of X_{n+i} into $\lceil \frac{L}{2} \rceil$ groups $G^{n+i}_1, G^{n+i}_2, ..., G^{n+i}_{\lceil \frac{L}{2} \rceil}$. Each group $G^{n+i}_j (j = 1, ..., \lceil \frac{L}{2} \rceil)$ includes two binary bits in X_{n+i}. If $L \mod 2 = 1$, P_{n+i} adds one 0 into the last group $G^{n+i}_{\lceil \frac{L}{2} \rceil}$.

(2) P_n can send Sq'_{P_n} and Po_n to P_{n+1}. The same as the step (5) of sub-protocol 1, P_{n+1} checks whether the transmission between P_n and him is secure or not. And he performs $U^1_P \otimes U^2_S (U^1_P \in \{I_P, U_P\}, U^2_S \in \{I_S, U_S\})$ on the jth photon of Sq_{P_n} according to G^{n+1}_j, $j = 1, 2, ..., L$. These operated photons form a new sequence denoted by $Sq_{P_{n+1}}$.

(3) For $i = 1, ..., n' - 1$: P_{n+i} sends $Sq_{P_{n+i}}$ to P_{n+i+1}. The same as the step (5) of sub-protocol 1, P_{n+i+1} checks whether the transmission between P_{n+i} and him is secure or not. And he performs $U^1_P \otimes U^2_S (U^1_P \in \{I_P, U_P\}, U^2_S \in \{I_S, U_S\})$ on the jth photon of $Sq_{P_{n+i}}$ according to G^{n+i+1}_j, $j = 1, 2, ..., L$. These operated photons form a new sequence denoted by $Sq_{P_{n+i+1}}$.

(4) $P_{n+n'}$ sends $Sq_{P_{n+n'}}$ to TP. The same as the step (5) of sub-protocol 1, TP checks whether the transmission between $P_{n+n'}$ and him is secure or not.

(5) With the help of TP and others $n+n'-2$ parties, any $P_k (k \in \{1, 2, ..., n, n+1, ..., n+n'\})$ can respectively compare his private information with $P_h (h = 1, 2, ..., k-1, k+1, .., n, n+1, ..., n+n'\})$.

For $k = 1, 2, ..., n, n+1, ..., n+n'\}$, For $h = 1, 2, ..., k-1, k+1, .., n, n+1, ..., n+n'\}$:

TP sends R to $P_j (j \in \{1, 2, ..., n, n+1, ..., n+n'\}\}, j \neq k, h)$. The $n-2$ parties calculates

$$\begin{aligned} & r^{1\prime}_{1(kh)} r^{2'}_{1(kh)} = r^1_1 r^2_1 \oplus \bigoplus_{j \in \{1,2,...,n\}, j \neq k,h} G^j_1, \\ & ... \\ & r^{1'}_{\lceil \frac{L}{2} \rceil (kh)} r^{2\prime}_{\lceil \frac{L}{2} \rceil (kh)} = r^1_{\lceil \frac{L}{2} \rceil} r^2_{\lceil \frac{L}{2} \rceil} \oplus \bigoplus_{j \in \{1,2,...,n\}, j \neq k,h} G^j_{\lceil \frac{L}{2} \rceil}. \end{aligned} \tag{6}$$

They also send $r^{1'}_{1(kh)} r^{2'}_{1(kh)}$, ..., $r^{1'}_{\left\lceil \frac{L}{2} \right\rceil (kh)} r^{2'}_{\left\lceil \frac{L}{2} \right\rceil (kh)}$ to TP.

TP calculates

$$\begin{aligned} R^1_{kh} &= r^{1'}_{1(kh)} r^{2'}_{1(kh)} \oplus I v_1^{1'} I v_1^{2'}, \\ &\cdots \\ R^{\left\lceil \frac{L}{2} \right\rceil}_{kh} &= r^{1'}_{\left\lceil \frac{L}{2} \right\rceil (kh)} r^{2'}_{\left\lceil \frac{L}{2} \right\rceil (kh)} \oplus I v^{1'}_{\left\lceil \frac{L}{2} \right\rceil} I v^{2'}_{\left\lceil \frac{L}{2} \right\rceil}. \end{aligned} \tag{7}$$

For $k = 1, 2, ..., n, n+1, ..., n+n^{'}\}$,
For $h = 1, 2, ..., k-1, k+1, .., n, n+1, ..., n+n^{'}\}$:

$R^1_{kh} =, ..., = R^{\left\lceil \frac{L}{2} \right\rceil}_{kh} = 00$, TP can know the private information $M_k = M_h$; otherwise $M_k \neq M_h$.

3 Analysis

3.1 Correctness Analysis

In this section, we choose 8 cases to show that the output of four-party protocol is correct in Table 1. There are four parties, P_1, P_2, P_3, P_4. Each of them has a private information $M_i, i = 1, 2, 3, 4$. For $i = 1, 2, 3, 4$, P_i divides his binary representation of M_i into $\left\lceil \frac{L}{2} \right\rceil$ groups and each groups includes two bits denoted by G^i_j. The initial states of TP are denoted by $I v^1_j I v^2_j (j = 1, 2, ..., \left\lceil \frac{L}{2} \right\rceil)$. P_1, P_2, P_3, P_4 agree that $I_P (I_S)$ encodes 0; $U_P (U_S)$ encodes 1; they also agree that $|H\rangle, |S\rangle_P, |a_1\rangle, |s\rangle_S$ encode 0; $|V\rangle, |A\rangle_P, |a_2\rangle, |a\rangle_S$ encode 1. In the Table 1, we suppose that the initial state is $|H\rangle |a_2\rangle$ and the initial state is encode by 01. P_1, P_2, P_3, P_4 perform the unitary operations on the initial state and get new state. The measurement of new state is encode by $r^1_j r^2_j$. The comparison result of P_1, P_2's private information G^1_j, G^2_j is denoted by R^{12}_j, where $R^{12}_j = r^1_j r^2_j \oplus G^3_j \oplus G^4_j \oplus 01$; The comparison result of P_1, P_3's private information G^1_j, G^3_j is denoted by R^{13}_j, where $R^{13}_j = r^1_j r^2_j \oplus G^2_j \oplus G^4_j \oplus 01$; the comparison result of P_2, P_3's private information G^2_j, G^3_j is denoted by R^{23}_i, where $R^{23}_j = r^1_j r^2_j \oplus G^1_j \oplus G^4_j \oplus 01$; The comparison result of P_1, P_4's private information G^1_j, G^4_j is denoted by R^{14}_j, , where $R^{14}_j = r^1_j r^2_j \oplus G^2_j \oplus G^3_j \oplus 01$; the P_2, P_4's private information G^1_j, G^4_j is denoted by R^{24}_j, where $R^{24}_j = r^1_j r^2_j \oplus G^1_j \oplus G^3_j \oplus 01$; the P_3, P_4's private information G^3_j, G^4_j is denoted by R^{34}_j, where $R^{34}_j = r^1_j r^2_j \oplus G^1_j \oplus G^2_j \oplus 01$.

Before TP measures the states, P_5 can join the protocol to compare his private information. The output of five-party protocol is also correct and we choose 4 cases to show that the output of five-party protocol is correct in Table 2. There are five parties, P_1, P_2, P_3, P_4, P_5. Each of them has a private information $M_i, i = 1, 2, 3, 4, 5$. For $i = 1, 2, 3, 4, 5$, P_i divides his binary representation of M_i into $\left\lceil \frac{L}{2} \right\rceil$ groups and each groups includes two bits denoted by G^i_j. The initial states of TP are denoted by $I v^1_j I v^2_j (j = 1, 2, ..., \left\lceil \frac{L}{2} \right\rceil)$. P_1, P_2, P_3, P_4, P_5 agree that $I_P (I_S)$ encodes 0; $U_P (U_S)$ encodes 1; they also agree that $|H\rangle, |S\rangle_P, |a_1\rangle, |s\rangle_S$ encode 0; $|V\rangle, |A\rangle_P, |a_2\rangle, |a\rangle_S$ encode 1. In the Table 2, we suppose

Table 1 P_1, P_2, P_3, P_4

$Initialstate$	G_j^1	G_j^2	G_j^3	G_j^4	$Newstate$	$r_j^1 r_j^2$	R_j^{12}	R_j^{13}	R_j^{23}	R_j^{14}	R_j^{24}	R_j^{34}
$\|H\rangle \|a_2\rangle$	10	11	01	00	$\|H\rangle \|a_2\rangle$	01	01	11	10	10	11	01
	10	11	01	01	$-\|H\rangle \|a_1\rangle$	00	01	11	10	11	10	00
	10	11	01	10	$\|V\rangle \|a_2\rangle$	11	01	11	10	00	01	11
	10	11	01	11	$-\|V\rangle \|a_1\rangle$	10	01	11	10	01	00	10
	10	01	01	00	$\|V\rangle \|a_2\rangle$	11	11	11	00	10	01	01
	10	01	01	01	$-\|V\rangle \|a_1\rangle$	10	11	11	00	11	00	00
	10	01	01	10	$\|H\rangle \|a_2\rangle$	01	11	11	00	00	11	11
	10	01	01	11	$\|V\rangle \|a_1\rangle$	10	11	11	00	01	10	10

Table 2 P_1, P_2, P_3, P_4, P_5

Initialstate	G_j^1	G_j^2	G_j^3	G_j^4	G_j^5	*Newstate*	$r_j^1 r_j^2$	R_j^{12}	R_j^{13}	R_j^{14}	R_j^{15}	R_j^{23}	R_j^{24}	R_j^{25}	R_j^{34}	R_j^{35}	R_j^{45}
$\|H\rangle\|a_2\rangle$	01	00	10	00	11	$\|H\rangle\|a_2\rangle$	01	01	11	01	10	10	00	11	10	01	11
	01	00	10	01	11	$-\|H\rangle\|a_1\rangle$	00	01	11	00	10	10	01	11	11	01	10
	01	00	10	10	11	$\|V\rangle\|a_2\rangle$	11	01	11	11	10	10	10	11	00	01	01
	01	00	10	11	11	$-\|V\rangle\|a_1\rangle$	10	01	11	10	10	10	11	11	01	01	00
	01	00	11	10	01	$-\|H\rangle\|a_1\rangle$	00	01	10	11	00	11	10	01	01	10	11
	01	01	10	01	01	$\|V\rangle\|a_2\rangle$	11	00	11	00	00	11	00	00	11	11	00
	01	10	01	11	10	$\|V\rangle\|a_1\rangle$	10	11	00	10	11	11	01	00	10	11	01
	01	11	00	00	10	$-\|H\rangle\|a_2\rangle$	01	10	01	01	11	11	11	01	00	10	10

that the initial state is $|H\rangle\,|a_2\rangle$ and the initial state is encode by 01. P_1, P_2, P_3, P_4, P_5 perform the unitary operations on the initial state and get new state. The measurement of new state is encode by $r_j^1 r_j^2$. The comparison result of P_1, P_2's private information G_j^1, G_j^2 is denoted by R_j^{12}, where $R_j^{12} = r_j^1 r_j^2 \oplus G_j^3 \oplus G_j^4 \oplus G_j^5 \oplus 01$; The comparison result of P_1, P_3's private information G_j^1, G_j^3 is denoted by R_j^{13}, where $R_j^{13} = r_j^1 r_j^2 \oplus G_j^2 \oplus G_j^4 \oplus G_j^5 \oplus 01$; the comparison result of P_1, P_4's private information G_j^1, G_j^4 is denoted by R_j^{14}, where $R_j^{14} = r_j^1 r_j^2 \oplus G_j^2 \oplus G_j^3 \oplus G_j^5 \oplus 01$; the comparison result of P_1, P_5's private information G_j^1, G_j^5 is denoted by R_j^{15}, where $R_j^{14} = r_j^1 r_j^5 \oplus G_j^2 \oplus G_j^3 \oplus G_j^4 \oplus 01$; the comparison result of P_2, P_3's private information G_j^2, G_j^3 is denoted by R_i^{23}, where $R_j^{23} = r_j^1 r_j^2 \oplus G_j^1 \oplus G_j^4 \oplus G_j^5 \oplus 01$; the P_2, P_4's private information G_j^2, G_j^4 is denoted by R_j^{24}, where $R_j^{24} = r_j^1 r_j^2 \oplus G_j^1 \oplus G_j^3 \oplus G_j^5 \oplus 01$; the P_2, P_5's private information G_j^2, G_j^5 is denoted by R_j^{25}, where $R_j^{25} = r_j^1 r_j^2 \oplus G_j^1 \oplus G_j^3 \oplus G_j^4 \oplus 01$; the P_3, P_4's private information G_j^3, G_j^4 is denoted by R_j^{34}, where $R_j^{34} = r_j^1 r_j^2 \oplus G_j^1 \oplus G_j^2 \oplus G_j^5 \oplus 01$; the P_3, P_5's private information G_j^3, G_j^5 is denoted by R_j^{35}, where $R_j^{35} = r_j^1 r_j^2 \oplus G_j^1 \oplus G_j^2 \oplus G_j^4 \oplus 01$; the P_4, P_5's private information G_j^3, G_j^4 is denoted by R_j^{45}, where $R_j^{45} = r_j^1 r_j^2 \oplus G_j^1 \oplus G_j^2 \oplus G_j^3 \oplus 01$.

3.2 Security Analysis

Firstly, we show that the outside attack is invalid to our protocol. Secondly, we show that the P_1, P_2, P_3, P_4 can not get any information about the private information of each other.

3.2.1 Outside Attack

According to the description of our protocol in Sub-protocol 1, we can know that P_1, .., P_n have to do two times security checking in step (3) and step (5.1)(6). In step (3)((5.1)(6)), the eavesdropper can attack the quantum channel and get the sequence Sq'_{TP}, $(Sq'_{P_{i-1}}, Sq'_{P_n})$, but he does not know the preparing basis, the photon's original states and the unitary operation formed on the particles. So in step (3)((5.1)(6)), we performed eavesdropper checking process and several kinds of outside attacks, such as the intercept-resend attack, the measure-resend attack, the entangle-measure attack, were detected with nonzero probability. Therefore, our process is also secure.

According to the description of our protocol in Sub-protocol 2, we can know that $P_{n'}$, ..., $P_{n+n'}$ have to do two times security checking in step (3) and step (4). In step (3)(4), the eavesdropper can attack the quantum channel and get the sequence $Sq_{P_{n'}}$, ..., $Sq_{P_{n+n'}}$, but he does not know the preparing basis, the photon's original states and the unitary operation formed on the particles. So in step (3)(4), we performed eavesdropper checking process and several kinds of outside attacks, such as the intercept-resend attack, the measure-resend attack, the entangle-measure attack, were detected with nonzero probability. Therefore, our process is also secure.

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. [22] and has attracted much attention in the cryptanalysis of quantum cryptography [23–28]. We analyze the possibility of the three participants to get information about

M_i in our protocol.we suppose that any two parties of P_h, P_k want to know that wether their private information M_h, M_k are equal or not. Because the roles of others $n-1$ parties are the same, firstly analyze the case that $P_i (i = 1, 2, ..., n, n \geq 4)$ wants to learn $P_j (j = 1, 2, ..., n, j \neq i)$'s private information M_j. Secondly, we analyze the case that TP wants to learn the $P_i (i = 1, 2, ..., n, n \geq 4)$'s private information M_i.

Case 1: $P_i (i = 1, 2, ..., n)$ wants to learn $P_h (h = 1, 2, ..., n, j \neq i)$'s private information M_h. In our protocol, P_i only knows $Sq'_{P_{i-1}}, r_1^1 r_1^2 \oplus \underset{j=\{1,...,n\}, j<i, j\neq h,k}{\oplus} G_1^j, ..., r_{\lceil \frac{L}{2} \rceil}^1 r_{\lceil \frac{L}{2} \rceil}^2 \oplus \underset{j=\{1,...,n\}, j<i, j\neq h,k}{\oplus} G_{\lceil \frac{L}{2} \rceil}^j$. P_i doesn't know the initial states Sq_{TP} chosen by TP, so he cannot deduce any information from $Sq'_{P_{i-1}}$. And he also doesn't know the r_i^1, r_i^2 which is the measurement of Sq_{P_n}, so he cannot deduce any information about others parties private information from $r_1^1 r_1^2 \oplus \underset{j=\{1,...,n\}, j<i, j\neq h,k}{\oplus} G_1^j, ..., r_{\lceil \frac{L}{2} \rceil}^1 r_{\lceil \frac{L}{2} \rceil}^2 \oplus \underset{j=\{1,...,n\}, j<i, j\neq h,k}{\oplus} G_{\lceil \frac{L}{2} \rceil}^j$.

Case 2: TP wants to learn $P_i's (i = 1, 2, ..., n, n \geq 4)$ private information M_i. TP can get $Sq_{TP}, Sq_{P_n}, r_1^1 r_1^2 ... r_{\lceil \frac{L}{2} \rceil}^1 r_{\lceil \frac{L}{2} \rceil}^2, r_1^{1'} r_1^{2'}, ..., r_{\lceil \frac{L}{2} \rceil}^{1'} r_{\lceil \frac{L}{2} \rceil}^{2'}$,

From our protocol, we can know that n parties perform U_P^1, U_S^2 on Sq_{TP} according to their private information and get Sq_{P_n}. Because there are n parties, TP cannot infer the private information of every party according Sq_{P_n}, Sq_{TP}.

From the protocol, we can know the relationship between $r_1^1 r_1^2 ... r_{\lceil \frac{L}{2} \rceil}^1 r_{\lceil \frac{L}{2} \rceil}^2$, $r_1^{1'} r_1^{2'}, ..., r_{\lceil \frac{L}{2} \rceil}^{1'} r_{\lceil \frac{L}{2} \rceil}^{2'}$ is that $r_1^{1'} r_1^{2'} = r_1^1 r_1^2 \oplus \underset{j\in\{1,2,...,n\}, j\neq k,h}{\oplus} G_1^j, ... r_{\lceil \frac{L}{2} \rceil}^{1'} r_{\lceil \frac{L}{2} \rceil}^{2'} = r_{\lceil \frac{L}{2} \rceil}^1 r_{\lceil \frac{L}{2} \rceil}^2 \oplus \underset{j\in\{1,2,...,n\}, j\neq k,h}{\oplus} G_{\lceil \frac{L}{2} \rceil}^j$. Because there are n parties and $n \geq 4$, we have to execute exclusive OR operation of 2 parties' private information with $r_k^1 r_k^2$ and gets $r_k^{1'} r_k^{2'}$. TP cannot exactly know the private information of two parties from $r_k^1 r_k^2$ and $r_k^{1'} r_k^{2'}$.

4 Discussion and Conclusions

In summary, we have put forward a dynamic quantum private comparison protocol based on single photons in both polarization and spatial-mode degrees of freedom. The dynamic property of our protocol is reflected in two aspects: one is that two parties can be dynamically chosen from n parties to compare their private information with the help of other $n-2$ parties. The other aspect is that before the particles are measured, n' party can join in the comparison protocol and the n parties' comparison protocol dynamically extend to a $n+n'$ parties' protocol. The proposed protocol uses the single photons in both polarization and spatial-mode degrees of freedom as the information carriers. The proposed protocol can resist the outside attacks using the checking particles. And any one party cannot get others parties' private information.

Acknowledgments This paper is supported by the National Natural Science Foundation of China(Grant No.61502437); Beijing Youth Talent Plan(YETP0592); Engineering Course Programming Project of Communication University of China(Grant No.3132015XNG1524,3132016XNG1609).

References

1. Fagin, R., Naor, M., Winkler, P.: Comparing information without leaking it. Commun. ACM **39**, 77–85 (1996)
2. 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)
3. Fabrice, B., Berry, S., et al.: A fair and e cient solution to the socialist millionaires' problem. Discret. Appl. Math. **111**, 23–36 (2001)
4. Qin, J., Zhang, Z.F., Feng, D.G., Li, B.: A protocol of comparing information without leaking. J. Softw. **15**, 421–427 (2004)
5. 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)
6. 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)
7. Liu, W., Wang, Y.B., Tao, J.Z.: An efficient protocol for the quantum private comparison of equality with w state. Opt. Commun. **284**, 1561–1565 (2011)
8. Liu, W., Wang, Y.B., Tao, J.Z.: An efficient protocol for the quantum private comparison of equality with w state. Opt. Commun. **284**, 1561–1565 (2011)
9. Liu, W., Wang, Y.B., Tao, J.Z., Cao, Y.Z.: A protocol for the quantum private comparison of equality with chi-type state. International Journal of Theoretical Physics. doi:10.1007/s10773-011-0878-8 (2011)
10. Liu, W., Wang, Y.B.: Quantum private comparison based on GHZ entangled states. Int. J. Theor. Phys. **51**, 3596–3604 (2012)
11. Liu, W., Wang, Y.B., Tao, J.Z., Cao, Y.Z., Cui, W.: New Quantum Private Comparison Protocol Using -Type State. International Journal of Theoretical Physics. doi:10.1007/s10773-011-1073-7 (2012)
12. Liu, W., Wang, Y.B., Tao, J.Z., Cui, W.: Quantum private comparison protocol based on bell entangled states. Commun. Theor. Phys. **57**(4), 583–588 (2012)
13. Liu, W., Wang, Y.B., Wang, X.M.: Quantum Multi-party Private Comparison Protocol using d-dimensional Bell States. International Journal of Theoretical Physics. doi:10.1007/ s10773-014-2388-y
14. Liu, W., Wang, Y.B., Wang, X.M.: Multi-party quantum private comparison protocol using d-dimensional basis States without entanglement swapping. Int. J. Theor. Phys. **53**, 1085–1091 (2014)
15. Du, W.L.: A Study of Several Specific Secure Two-party Computation Problems[D]. Department of computer sciences purdue university (2001)
16. Xia, Z., Wang, X., Sun, X., Wang, Q.: A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data. IEEE Trans. Parallel Distrib. Syst. **27**(2), 340–352 (2015)
17. Cao, N., Wang, C., Li, M., Ren, K., Lou, W.: Privacy-preserving multi-keyword Ranked search over encrypted cloud data. IEEE Trans. Parallel Distrib. Syst. **25**(1), 222–223 (2014)
18. Sun, X., Zhou, L., Fu, Z., Wang, J.: Privacy-preserving multi-keyword ranked search over encrypted cloud data supporting dynamic update. Int. J. Secur. Appl. **8**(6), 1–16 (2014)
19. Fu, Z.J., Ren, K., Shu, J.G., Sun, X.M., Huang, F.X.: Enabling Personalized Search over Encrypted Outsourced Data with Efficiency Improvement. IEEE Transactions on Parallel and Distributed Systems. doi:10.1109/TPDS.2015.2506573
20. Fu, Z.J., Sun, X.M., Liu, Q., Zhou, L., Shu, J.G.: Achieving Efficient Cloud Search Services: Multi-keyword Ranked Search over Encrypted Cloud Data Supporting Parallel Computing. IEICE Trans. Commun. **E98-B**(1), 190–200 (2015)
21. Ren, Y., Shen, J., Wang, J., Han, J., Lee, S.: Mutual verifiable provable data auditing in public cloud storage. J. Internet Technol. **16**(2), 317–323 (2015)
22. 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)
23. 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)
24. 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)
25. 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)
26. 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)
27. Song, T.T., Zhang, J., Gao, F., et al.: Participant attack on quantum secret sharing based on entanglement swapping. Chin. Phys. B **18**, 1333 (2009)
28. Guo, F.Z., Qin, S.J., Gao, F., et al.: Participant attack on a kind of MQSS schemes based on entanglement swapping. Eur. Phys. J. D **56**, 445 (2010)