Int J Theor Phys (2013) 52:3212–3219
DOI 10.1007/s10773-013-1616-1

# Quantum Private Comparison Protocol with the Random Rotation

**Wei Zi · Fenzhuo Guo · Yi Luo · Shouhong Cao · Qiaoyan Wen**

Received: 2 February 2013 / Accepted: 9 April 2013 / Published online: 12 May 2013

**Abstract** We proposed a quantum secret comparison protocol for two parties with the random rotation angle, which is under the help of a semi-honest third party. The random rotation angle made it possible for the protocol to be safer and the two parties cannot deduce each other's information by means of their own possessions. The participants' secrets are divided into groups and the third party announced the results by group, which made the protocol more safely and sometimes it can save lots of resources. Moreover, during our protocol process any information of the two parties will not be leaked, even the third party cannot get any participants' secrets.

**Keywords** Quantum cryptography · Quantum private comparison · Random rotation

## 1 Introduction

Various quantum cryptography protocols have been flourished by utilizing quantum mechanics principles, since Bennett and Brassard proposed the first quantum key distribution protocol in 1984 [3], which ensured two remote users can share a common random key securely. Over recent years many classical cryptographic impossibilities and interesting applications can be solved in quantum ways, such as quantum secret sharing (QSS) [10, 14, 16, 17, 19, 27], quantum key distribution (QKD) [2, 13, 15, 22, 28, 30, 34], quantum teleportation [4, 7, 8, 33], etc.

As a fundamental primitive in modern cryptography, secure multiparty computation (SMC) is to enable distrustful parties to jointly compute a function over their inputs, without leaking their respective secrets under the only assumption that some of them will follow the

W. Zi · F. Guo (✉)
School of Science, Beijing University of Posts and Telecommunications, Beijing 100876, China
e-mail: gfenzhuo@bupt.edu.cn

W. Zi · F. Guo · Y. Luo · S. Cao · Q. Wen
State Key Laboratory of Networking and Switching Technology and School of Science, Beijing University of Posts and Telecommunications, Beijing 100876, China

protocol honestly. Recently research on SMC arouses tremendous interests owing to its extensive applications and prospects, including secure multi-party quantum summation [11], secret ballot elections [1], and anonymous voting [6] and so on. Large numbers of natural protocols can be reworded to special cases of multiparty computation problems, so it is significant to design and analyze the special multiparty computation protocols. In the usual secure two-party computation scenario, Alice and Bob have their inputs $x$ and $y$ individually, and both of them wish to compute $f(x, y)$ which is well known to themselves.

Quantum private comparison (QPC) is an important branch of secure multiparty computing, which allows two participants to determine whether their secrets happened to be equal, at the same time their inputs can be kept in secret. The first QPC protocol was proposed by Yang et al. [31, 32], the secrets of two parties can be compared based on the decoy photon and EPR pairs, and its security was guaranteed by one-way hash function, which utilized to encrypt their own secrets by both of the players. In addition to avoid some special attacks in their round trip transmissions, a number of special optical filters are inserted in every round, which decreases the qubit efficiency apparently. Soon after that, Chen et al.proposed a more efficient QPC protocol [9], which utilized the triplet entangled states and the simple single-particle measurement.

By reason that it is proved to be insecure, to construct a secure equality function in a two-party scheme [25], almost all previous QPC protocols have drawn support from a semi-honest third party (Trent). Trent might try to steal the players' private inputs, but he cannot be corrupted by the adversary. Following some ideas of the quantum computation protocols [18, 21, 23, 24, 29], enlightened by Kye et al.'s quantum key distribution protocol [20], we proposed a QPC protocol with random rotation angle, and it is also under the help of Trent. There are several features in our protocol. Firstly, participants share a sequence of secret classical keys in advance, which can prevent Trent and outsiders to steal or analyze their inputs. Secondly, the selected polarization angles $\theta$ and $\theta + \pi$ are not necessary for participants to discuss with each other, as Bob and Alice do not need to know the other's polarization basis. Thirdly, no round-trip transmission exists in the protocol, so that many kinds of attacks are invalid to this protocol.

The structure of this paper is as follows. In Sect. 2, we propose a private comparison protocol with the random rotation. Then, we analyze the security of this protocol in Sect. 3. Finally, a brief discussion and summary are given in Sect. 4.

## 2 Quantum Private Comparison Protocol with the Random Rotation

The case with two distrustful players who want to compare whether their secrets are equal with Trent's help is taken into consideration. Supposed that the two players, Alice and Bob have secrets $a$ and $b$, respectively.

Let $A = \{a_{n-1}, a_{n-2}, \dots, a_0\}$ and $B = \{b_{n-1}, b_{n-2}, \dots, b_0\}$ be the binary representations of $a$ and $b$ in $F_{2^n}$, where $a = \sum_{i=0}^{n-1} a_i 2^i$, $b = \sum_{i=0}^{n-1} b_i 2^i$, with $a_i, b_i \in (0, 1)$, $2^{n-1} \leq \max\{a, b\} \leq 2^n$.

Then Alice divides her classic secrets into $\lceil \frac{n}{m} \rceil$ $(m \geq 2)$ groups, which are

$$A_0 = \{a_0, a_1, \dots, a_{m-1}\}$$

$$A_1 = \{a_m, a_{m+1}, \dots, a_{2m-1}\}$$

$$\dots$$

$$A_{\lceil \frac{n}{m} \rceil - 1} = \{a_{(\lceil \frac{n}{m} \rceil) * m}, a_{(\lceil \frac{n}{m} \rceil) * m + 1}, \dots, a_{n-1}\}.$$

Bob does the same operation as Alice and gets

$$\begin{aligned} B_0 &= \{b_0, b_1, \dots, b_{m-1}\} \\ B_1 &= \{b_m, b_{m+1}, \dots, b_{2m-1}\} \\ &\dots \\ B_{\lceil \frac{n}{m} \rceil - 1} &= \{b_{(\lceil \frac{n}{m} \rceil) * m}, b_{(\lceil \frac{n}{m} \rceil) * m+1}, \dots, b_{n-1}\}. \end{aligned}$$

*Step 1* Alice and Bob share a sequence of secret classical keys $\Theta = \{\theta_0, \theta_1, \dots, \theta_{n-1}\}$ in advance, in which $n$ is the length of secrets and $\theta_i \in \{\frac{\pi}{4}, \frac{\pi}{2}\}(i = 0, 1, \dots, n-1)$. Trent prepares $m$ EPR pairs to form initial sequence $S_T$, every pair is randomly chosen from $\{|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), |\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)\}$, and records the initial states, after that divides these EPR pairs into two sequences, namely $S_A$, $S_B$. The first particles of all EPR pairs are formed to the sequence $S_A$, and the rest are formed to the sequence $S_B$.

*Step 2* Trent prepares two sequences of decoy states $S'_A$ and $S'_B$, randomly in photon states: $|0\rangle, |1\rangle, |+\rangle, |-\rangle$. Then he randomly inserts $S'_A$ in $S_A$ and $S'_B$ in $S_B$ to form new sequences $S''_A$ and $S''_B$. After that Trent sends the sequences $S''_A$ to Alice, $S''_B$ to Bob respectively.

*Step 3* Alice and Bob inform Trent once they have received the quantum sequences $S''_A$ and $S''_B$. Then Trent announces to Alice and Bob respectively the positions and measuring bases ($\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$) of the decoy states $S'_A$ and $S'_B$ for the eavesdropping check. Alice and Bob extract the checking states from $S''_A$ and $S''_B$, and perform the corresponding basis measurements to obtain two sequences of measuring results $r_A$ and $r_B$. Thereafter, they report the results $S'_A$ and $S'_B$ to Trent respectively. If the error rate is limited in a predetermined threshold, Trent announces there is no eavesdropper and the protocol continues, otherwise Trent aborts the protocol and restarts.

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad \sigma_y = i \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

*Step 4* Alice and Bob recover the initial sequences $S_A$ and $S_B$ through discarding the decoy states, individually. Afterwards, they perform the operators $U_y(\theta_a + \theta_i)$ and $U_y(\theta_b - \theta_i)$ on the $i$th particle respectively according to their secrets, where $U_y(\theta) = \cos(\theta)I - i\sin(\theta)\sigma_y$ is the unitary operator which rotates the arbitrary angle along the $y$ axis, and $I$ and $\sigma_y$ are defined as above. If $a_i(b_i) = 0$, Alice (Bob) chooses $\theta_a(\theta_b)$ randomly from $\{0, \pi\}$, otherwise Alice (Bob) chooses $\theta_a(\theta_b)$ randomly from $\{\frac{\pi}{2}, \frac{3\pi}{2}\}$.

*Step 5* After they perform the operators according to selected initial state, the EPR pairs turn to

$$\begin{aligned} &U_y(\theta_a + \theta_i) \otimes U_y(\theta_b - \theta_i)|\phi^+\rangle \\ &\quad = \frac{1}{\sqrt{2}}[\cos(\theta_a - \theta_b + 2\theta_i)(|00\rangle + |11\rangle) - \sin(\theta_a - \theta_b + 2\theta_i)(|01\rangle - |10\rangle)] \end{aligned}$$

or

$$
\begin{aligned}
&U_y(\theta_a+\theta_i)\otimes U_y(\theta_b-\theta_i)|\psi^-\rangle \\
&\quad=\frac{1}{\sqrt{2}}[\sin(\theta_a-\theta_b+2\theta_i)(|00\rangle+|11\rangle)+\cos(\theta_a-\theta_b+2\theta_i)(|01\rangle-|10\rangle)]
\end{aligned}
$$

Thereafter, Alice and Bob use Z basis $(\{|0\rangle,|1\rangle\})$ to measure the particles, and obtain a sequence of results $R_{A_i}=\{ra_{im},ra_{im+1},\dots,ra_{(i+1)m-1}\}$ and $R_{B_i}=\{rb_{im},rb_{im+1},\dots,rb_{(i+1)m-1}\}$. If the measuring result is $|0\rangle$, then $ra_j(rb_j)=0$; if the measuring result is $|1\rangle$, then $ra_j(rb_j)=1$, where $im\le j\le(i+1)m-1$.

Before they simultaneously transfer the results to Trent, the results should be revised and formed to another sequences $C_{A_i}=\{ca_{im},ca_{im+1},\dots,ca_{(i+1)m-1}\}$ and $C_{B_i}=\{cb_{im},cb_{im+1},\dots,cb_{(i+1)m-1}\}$, where $cb_{im}=rb_{im}$, $cb_{im+1}=rb_{im+1},\dots,$ $cb_{(i+1)m-1}=rb_{(i+1)m-1}$. If $\theta_j=\frac{\pi}{4}$, $ca_j=ra_j\oplus 1$, otherwise $ca_j=ra_j$, where $im\le j\le(i+1)m-1$.

*Step 6* Trent calculates the exclusive-OR results $r_i=ca_i\oplus cb_i$. If the initial state is $|\phi^+\rangle=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$, Trent does nothing to the results, and otherwise he/she adds 1 to every exclusive-OR results, then the results change to $t_i$. Now once there exists any $j$ $(im\le j\le(i+1)m-1)$, $t_j=1$ in $i$th group, Trent interrupts the protocol and announces "1" to indicate Alice's and Bob's secrets are not equal, the $(i+1)$th, $(i+2)$th, ... and $(\lceil\frac{n}{m}\rceil)$th group secrets have no need to be compared. Otherwise Trent repeats the protocol until all the information has been compared, if $T=\{t_0,t_1,\dots,t_{\lceil\frac{n}{m}\rceil-1}\}=\mathbf{0}$, he announces "0" to indicate Alice's and Bob's secrets are identical.

Table 1 shows two cases of comparison and the other cases can be proved in the same way.

## 3 Security Analyses

In general, our protocol process is secure, and any information of the two parties will not be leaked. To see that, we will analyze the security of protocol from two main parts (outsider attack and insider attack).

### 3.1 Outsider Attack

Apart from the process of EPR pairs distribution, the rest information is transferred through a classical channel, in which the information is allowed eavesdropping but modifying. Because the information in the classical channel has no relationship with the participants' secrets owing to the shared secret classical keys $\Theta$, the eavesdroppers have no possibility to get the secrets. As a result, the only chance of outsider eavesdropper's attack in this protocol is to attack the quantum channel in the Step 2. However, Trent inserts the decoy states $S'_A$ and $S'_B$ separately into $S_A$ and $S_B$, and before Alice and Bob continue the next step, they will check the existence of eavesdropper. Trent announces respectively the positions and measuring bases $(\{|0\rangle,|1\rangle\}$ or $\{|+\rangle,|-\rangle\})$ of the decoy states $S'_A$ and $S'_B$. Participants should measure the decoy states according to the measurements, which informed by Trent, then they and Trent publish the measuring results and initial decoy states. By discussion they can confirm whether there is an eavesdropper existing in the quantum channel.

Some well known attacks such as intercept-resend attack, measurement-resend attack, entanglement-measure attack and denial-of-service (DOS) attack can be detected with nonzero probability during the decoy checking process. What's more, the Trojan horse at-

**Table 1** Two cases of comparison

| $a_i$ | $b_i$ | $\theta_a$ | $\theta_b$ | $\theta_i$ | $S_{T_i}$ | $ra_i$ | $rb_i$ | $ca_i$ | $cb_i$ | $r_i$ | $t_i$ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | $\pi/4$ | $\vert\phi^+\rangle$ | 1(0) | 0(1) | 0(1) | 0(1) | 0 | 0 |
| | | 0 | $\pi$ | $\pi/4$ | $\vert\phi^+\rangle$ | 1(0) | 0(1) | 0(1) | 0(1) | 0 | 0 |
| | | $\pi$ | 0 | $\pi/4$ | $\vert\phi^+\rangle$ | 1(0) | 0(1) | 0(1) | 0(1) | 0 | 0 |
| | | $\pi$ | $\pi$ | $\pi/4$ | $\vert\phi^+\rangle$ | 1(0) | 0(1) | 0(1) | 0(1) | 0 | 0 |
| | | 0 | 0 | $\pi/2$ | $\vert\phi^+\rangle$ | 0(1) | 0(1) | 0(1) | 0(1) | 0 | 0 |
| | | 0 | $\pi$ | $\pi/2$ | $\vert\phi^+\rangle$ | 0(1) | 0(1) | 0(1) | 0(1) | 0 | 0 |
| | | $\pi$ | 0 | $\pi/2$ | $\vert\phi^+\rangle$ | 0(1) | 0(1) | 0(1) | 0(1) | 0 | 0 |
| | | $\pi$ | $\pi$ | $\pi/2$ | $\vert\phi^+\rangle$ | 0(1) | 0(1) | 0(1) | 0(1) | 0 | 0 |
| | | 0 | 0 | $\pi/4$ | $\vert\psi^-\rangle$ | 1(0) | 1(0) | 0(1) | 1(0) | 1 | 0 |
| | | 0 | $\pi$ | $\pi/4$ | $\vert\psi^-\rangle$ | 1(0) | 1(0) | 0(1) | 1(0) | 1 | 0 |
| | | $\pi$ | 0 | $\pi/4$ | $\vert\psi^-\rangle$ | 1(0) | 1(0) | 0(1) | 1(0) | 1 | 0 |
| | | $\pi$ | $\pi$ | $\pi/4$ | $\vert\psi^-\rangle$ | 1(0) | 1(0) | 0(1) | 1(0) | 1 | 0 |
| | | 0 | 0 | $\pi/2$ | $\vert\psi^-\rangle$ | 1(0) | 0(1) | 0(1) | 1(0) | 1 | 0 |
| | | 0 | $\pi$ | $\pi/2$ | $\vert\psi^-\rangle$ | 0(1) | 1(0) | 0(1) | 1(0) | 1 | 0 |
| | | $\pi$ | 0 | $\pi/2$ | $\vert\psi^-\rangle$ | 0(1) | 1(0) | 0(1) | 1(0) | 1 | 0 |
| | | $\pi$ | $\pi$ | $\pi/2$ | $\vert\psi^-\rangle$ | 0(1) | 1(0) | 0(1) | 1(0) | 1 | 0 |
| 0 | 1 | 0 | $\pi/2$ | $\pi/4$ | $\vert\phi^+\rangle$ | 0(1) | 0(1) | 1(0) | 0(1) | 1 | 1 |
| | | 0 | $3\pi/2$ | $\pi/4$ | $\vert\phi^+\rangle$ | 0(1) | 0(1) | 1(0) | 0(1) | 1 | 1 |
| | | $\pi$ | $\pi/2$ | $\pi/4$ | $\vert\phi^+\rangle$ | 0(1) | 0(1) | 1(0) | 0(1) | 1 | 1 |
| | | $\pi$ | $3\pi/2$ | $\pi/4$ | $\vert\phi^+\rangle$ | 0(1) | 0(1) | 1(0) | 0(1) | 1 | 1 |
| | | 0 | $\pi/2$ | $\pi/2$ | $\vert\phi^+\rangle$ | 0(1) | 1(0) | 0(1) | 1(0) | 1 | 1 |
| | | 0 | $3\pi/2$ | $\pi/2$ | $\vert\phi^+\rangle$ | 0(1) | 1(0) | 0(1) | 1(0) | 1 | 1 |
| | | $\pi$ | $\pi/2$ | $\pi/2$ | $\vert\phi^+\rangle$ | 0(1) | 1(0) | 0(1) | 1(0) | 1 | 1 |
| | | $\pi$ | $3\pi/2$ | $\pi/2$ | $\vert\phi^+\rangle$ | 0(1) | 1(0) | 0(1) | 1(0) | 1 | 1 |
| | | 0 | $\pi/2$ | $\pi/4$ | $\vert\psi^-\rangle$ | 0(1) | 1(0) | 1(0) | 1(0) | 0 | 1 |
| | | 0 | $3\pi/2$ | $\pi/4$ | $\vert\psi^-\rangle$ | 0(1) | 1(0) | 1(0) | 1(0) | 0 | 1 |
| | | $\pi$ | $\pi/2$ | $\pi/4$ | $\vert\psi^-\rangle$ | 0(1) | 1(0) | 1(0) | 1(0) | 0 | 1 |
| | | $\pi$ | $3\pi/2$ | $\pi/4$ | $\vert\psi^-\rangle$ | 0(1) | 1(0) | 1(0) | 1(0) | 0 | 1 |
| | | 0 | $\pi/2$ | $\pi/2$ | $\vert\psi^-\rangle$ | 0(1) | 0(1) | 0(1) | 0(1) | 0 | 1 |
| | | 0 | $3\pi/2$ | $\pi/2$ | $\vert\psi^-\rangle$ | 0(1) | 0(1) | 0(1) | 0(1) | 0 | 1 |
| | | $\pi$ | $\pi/2$ | $\pi/2$ | $\vert\psi^-\rangle$ | 0(1) | 0(1) | 0(1) | 0(1) | 0 | 1 |
| | | $\pi$ | $3\pi/2$ | $\pi/2$ | $\vert\psi^-\rangle$ | 0(1) | 0(1) | 0(1) | 0(1) | 0 | 1 |

Alice and Bob have secrets $a_i$ and $b_i$, respectively, they have shared a sequence of secret classical keys $\theta_i$, the selected rotation angles of Alice and Bob are $\theta_a$ and $\theta_b$. We denote Alice's and Bob's measurement results as $ra_i$ and $rb_i$, the information that transferred to Trent is respectively $ca_i$ and $cb_i$. After the exclusive-OR operation, Trent obtains the results $r_i$, at last Trent gets the final results $t_i$ after the comparison with the initial state. If $r_i = 0$, the secret $a_i$ is equal to $b_i$. Otherwise, the value of $r_i$ is 1

tack can be automatically prevented, since there is no round-trip transmission in the protocol. Thus the outsider attack is invalid to our protocol.

When a qubit of entangled states travels in a noise quantum channel, parts of the initial entanglement might be lost. Fortunately, it has been proven that over any long distance, the reliably shared entanglement can be obtained by using the quantum-repeater technique, containing the entanglement purification [12, 26] and teleportation [7].

## 3.2 Insider Attack

In general, the participants have more advantages to attack the protocol than the outsider eavesdropper, because they can utilize their partial information without being detected legally. Although Alice's role has superiority over Bob's, the limited advantage does not threaten the security of our protocol. So we will consider two following possible cases.

### *3.2.1 Third Party Attack*

As for Trent, what he does is to generate the initial states and calculate the final results. Due to the dishonesty of Trent, he might try to steal the participants' secrets from the protocol.

In the generating process (S1), Trent could replace the initial states with other states, which can get through the decoy detection. However, by reason that the information Alice and Bob give Trent has irrelevance with the secrets they own, the substitution does not have any benefit for all of them in addition to the error. That is also the reason that Trent cannot obtain any information of Alice and Bob except the comparing results in the calculating process (S6). In the other steps, even though Trent is involved in the protocol process, its role has no more privileges than the outsiders. As a result Trent cannot get any secrets.

### *3.2.2 Participants' Attack*

Suppose Bob is a dishonest participant, who attempts to steal Alice's information $a$. For that purpose Bob must get Alice's initial states and the compared results by whatever means, actually it is not likely to succeed. Let alone the transportation in the classical channel cannot be modified in the quantum world, owing to the decoy states of the initial sequences, the probability is less than 50 %. Also, Bob can insert a filter in front of his devices to filter out the photon signal with an illegitimate wavelength, and obtain information by performing IPE Trojan horse attack strategies. However, there is no round-trip transmission in the protocol, so this method cannot make it.

Despite S5, what the two participants do is exactly same. Though it is Alice, who revises the results $ca_i$ based on their sharing classical secret keys, Bob also knows that which qubit should be revised.

Now we will discuss what will happen due to Alice's superiority. However, the superiority is helpless. If she disobeys the protocol, send $ca_i = ra_i(\theta_i = \frac{\pi}{4})$, or $ca_i = ra_i \oplus 1(\theta_i = \frac{\pi}{2})$ according to her needs, the possibility is no higher than it of coin-flipping. Besides, Trent announces the comparing result by group, Alice has no idea whether the disobedience lead to the result. For instance, we suppose that $m = 5$, the initial states is $|\psi^-\rangle$, Alice's secret $a_i$ is 01010, Bob's $b_i$ is 10010, the comparing result is 1, but if Alice disobeys the rules on the first qubit, the result is 1. Therefore Alice cannot obtain any useful information. What's worse, it leads to an inaccuracy that even Alice does not want to face up with this circumstance. In other words, Alice will introduce errors invariably if she wants to steal valuable information. So it suffices to conclude that our scheme is secure for Alice's eavesdropping under an ideal environment. Moreover, if the quantum channels are noisy, the security of our scheme can be guaranteed by performing quantum error correction and privacy amplification [5, 7].

For these reasons, neither Alice nor Bob can get the other's information via their own photons.

## 4 Conclusions

By and large, in this paper a private comparison protocol has been proposed, which utilized random rotation angle and EPR entangled states. The same as the previous protocols [9, 18, 21, 23, 29], our protocol is also under the help of a semi-honest third party and ensures fairness, security and efficiency. First and foremost, the selected polarization angles can efficiently prevent eavesdropping from the Trent and outsiders. At the same time because both of participants do not know each other's selection, the secrets will not be analyzed and disclosed. What's more, participants' secret messages are divided into many groups, the comparison of following data do not need to continue as long as Trent announces the result "1" in a certain round, Alice and Bob both know the final result. Hence, it saves plenty of quantum recourses and time.

## References

1. Benaloh, J.: Verifiable secret-ballot elections. PhD thesis, Yale University (1987)
2. Bennett, C.H.: Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. **68**(21), 3121–3124 (1992)
3. Bennett, C.H., Brassard, G.: In: IEEE International Conference on Computers, Systems and Signal Processing, pp. 175–179. IEEE Press, New York (1984)
4. Bennett, C.H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., Wootters, W.K.: Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Phys. Rev. Lett. **70**, 1895 (1993)
5. Bennett, C.H., DiVincenzo, D.P., Smolin, J.A., Wootters, W.K.: Mixed-state entanglement and quantum error correction. Phys. Rev. A **54**, 3824 (1996)
6. Bonanome, M., Buzěk, V., Hillery, M., Ziman, M.: Toward protocols for quantum-ensured privacy and secure voting. Phys. Rev. A **84**, 022331 (2011)
7. Bouwmeester, D., Pan, J.W., Mattle, K., Eibl, M., Weinfurter, H., Zeilinger, A.: Experimental quantum teleportation. Nature **390**, 575–579 (1997)
8. Chen, X.B., Wen, Q.Y., Zhu, F.C.: Quantum circuits for probabilistic entanglement teleportation via a partially entangled pair. Int. J. Quantum Inf. **5**, 717 (2007)
9. Chen, X.B., Xu, G., Niu, X.X., Wen, Q.Y., Yang, Y.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)
10. Deng, F.G., Long, G.L., Zhou, H.Y.: Multiparty quantum-state sharing of an arbitrary two-particle state with Einstein-Podolsky-Rosen pairs. Phys. Lett. A **337**, 329 (2005)
11. Du, J.Z., Chen, X.B., Wen, Q.Y., Zhu, F.C.: Secure multiparty quantum summation. Acta Phys. Sin. **56**, 6214 (2007)
12. Dür, W., Briegel, H.-J., Ciracl, J.I., Zoller, P.: Quantum repeaters based on entanglement purification. Phys. Rev. A **59**, 169–181 (1999)
13. Ekert, A.K.: Quantum cryptography based on Bell theorem. Phys. Rev. Lett. **67**(6), 661–663 (1991)
14. Guo, G.P., Guo, G.C.: Quantum secret sharing without entanglement. Phys. Lett. A **310**, 247 (2003)
15. 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**(6), 1013–1022 (2010)
16. Han, L.F., Liu, Y.M., Yuan, H., Zhang, Z.J.: Efficient multiparty-to-multiparty quantum secret sharing via continuous variable operations. Phys. Rev. Lett. **24**, 3312 (2007)
17. Hillery, M., Buzěk, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A **59**, 1829–1834 (1999)
18. Jia, H.Y., Wen, Q.Y., Song, T., Gao, F.: Quantum protocol for millionaire problem. Opt. Commun. **284**, 545–549 (2011)
19. Karlsson, A., Koashi, M., Imoto, N.: Quantum entanglement for secret sharing and secret splitting. Phys. Rev. A **59**, 162 (1999)
20. Kye, W.H., Kim, C.M., Kim, M.S., Park, Y.J.: Quantum key distribution with blind polarization bases. Phys. Rev. Lett. **95**, 040501 (2005)
21. Lin, S., Sun, Y., Liu, X.F., Yao, Z.Q.: Quantum private comparison protocol with d-dimensional Bell states. Quantum Inf. Process. (2012). doi:10.1007/s11128-012-0395-6
22. Liu, B., Gao, F., Wen, Q.Y.: Single-photon multiparty quantum cryptographic protocols with collective detection. IEEE J. Quantum Electron. **47**, 1389–1390 (2011)

23. Liu, B., Gao, F., Jia, H.Y., Huang, W., Zhang, W.W., Wen, Q.Y.: Efficient quantum private comparison employing single photons and collective detection. Quantum Inf. Process. (2012). doi:10.1007/s11128-012-0439-y
24. Liu, W., Wang, Y.B., Cui, W.: Quantum private comparison protocol based on Bell entangled states. Commun. Theor. Phys. **57**, 583–588 (2012)
25. Lo, H.K.: Insecurity of quantum secure computations. Phys. Rev. A **56**(2), 1154–1162 (1997)
26. Pan, J.W., Simon, C., Brukner, Č., Zeilinger, A.: Entanglement purification for quantum communication. Nature **410**, 1067–1070 (2001)
27. Qin, S.J., Gao, F., Wen, Q.Y., Zhu, F.C.: Cryptanalysis of the Hillery-Buzěk-Berthiaume quantum secret-sharing protocol. Phys. Rev. A **76**, 062324 (2007)
28. Sun, Y., Wen, Q.Y., Gao, F., Zhu, F.C.: Robust variations of the Bennett-Brassard 1984 protocol against collective noise. Phys. Rev. A **80**, 032321 (2009)
29. Tseng, H.Y., Lin, J., Hwang, T.: New quantum private comparison protocol using EPR pairs. Quantum Inf. Process. **11**, 373–384 (2012)
30. Wang, X.B.: Quantum key distribution with two-qubit quantum codes. Phys. Rev. Lett. **92**, 077902 (2004)
31. 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)
32. Yang, Y.G., Cao, W.F., Wen, Q.Y.: Secure quantum private comparison. Phys. Scr. **80**(6), 065002 (2009)
33. Zhang, Z.J., Liu, Y.M., Man, Z.X.: Many-agent controlled teleportation of multi-qubit quantum information via quantum entanglement swapping. Commun. Theor. Phys. **44**, 847 (2005)
34. Zhang, Q., Yin, J., Chen, T.Y., Lu, S., Zhang, J., Li, X.Q., Yang, T., Wang, X.B., Pan, J.W.: Experimental fault-tolerant quantum cryptography in a decoherence-free subspace. Phys. Rev. A **73**, 020301 (2006)