Int J Theor Phys (2017) 56:3340–3347
DOI 10.1007/s10773-017-3499-z

Quantum Private Comparison Based on χ-Type Entangled States

Pan Hong-Ming[1]

Received: 23 March 2017 / Accepted: 31 July 2017 / Published online: 23 August 2017

Abstract A two-party quantum private comparison (QPC) protocol is constructed with χ-type entangled states in this paper. The proposed protocol employs a semi-honest third party (TP) that is allowed to misbehave on his own but cannot conspire with the adversary. The proposed protocol need perform Bell basis measurements and single-particle measurements but neither unitary operations nor quantum entanglement swapping technology. The proposed protocol possesses good security toward both the outside attack and the participant attack. TP only knows the comparison result of the private information from two parties in the proposed protocol.

Keywords Quantum private comparison (QPC) · χ-type entangled state · Correctness · Security

1 Introduction

After the first quantum cryptography protocol was proposed by Bennett and Brassard [1] in 1984, quantum cryptography quickly aroused the interests of researchers due to its unconditional security and has already obtained a considerable development. Up to now, various kinds of quantum cryptography protocols have been constructed, such as quantum key distribution (QKD) [1–3], quantum secret sharing (QSS) [4–6], quantum secure direct communication (QSDC) [7–9] and so on.

In 2009, Yang and Wen [10] put forward a novel concept for quantum cryptography named quantum private comparison (QPC), which can be used to determine whether two parties' private inputs are equal or not on the basis that their genuine contents are not leaked

✉ Pan Hong-Ming
hmpan@zjgsu.edu.cn

[1] College of Information & Electronic Engineering, Zhejiang Gongshang University, Hangzhou 310018, People's Republic of China

out. Since the first two-party QPC protocol was proposed by Yang et al. [10], quantum private comparison has been intensively studied so that numerous two-party QPC protocols have been suggested, such as those with single particles [11], product states [12, 13], Bell states [10, 14–18], GHZ states [19–21], W states [22, 23], cluster states [24, 25], χ-type entangled states [26–28], five-particle entangled states [29], six-particle entangled states [30]. Besides the two-party QPC, multi-party QPC has also aroused researchers' interests so that several good multi-party QPC protocols [31–37] have been constructed.

In 1997, Lo [38] found out that it is impossible to evaluate the equality function securely in a two-party scenario. Therefore, all the above QPC protocols [10, 37] need to employ a third party (TP). As the role of TP, there are three different definitions. Zhang et al. [18] explained these roles as follows: (1) TP is honest. In this situation, the users only need to send their encrypted private information to TP, then TP compares the decrypted private information and announces the comparison result. However, this situation is too perfect to be impractical. (2) TP is dishonest. In this situation, the users cannot trust TP any more. This situation is useless. (3) TP is semi-honest. There are two kinds of definition here. The first one is first introduced by Chen et al. [19], which means that TP executes the protocol loyally and keeps a record of all its intermediate computations and might try to steal the users' private information from the record, but cannot be corrupted by the adversary. The second one is introduced by Yang et al. [17], which means that TP is allowed to misbehave on his own but cannot conspire with the adversary. Up to now, the second kind definition of semi-honest TP is thought to be the most reasonable.

Based on the above analysis, similar to the QPC protocols of Refs. [26–28], in this paper, we suggest a novel QPC protocol with a semi-honest TP also using χ-type entangled states as the quantum resource. The proposed protocol adopts Yang et al. 's [17] definition for semi-honest TP, who can only know the comparison result of the private information from two parties.

The rest of this paper is organized as follows: in Section 2, a novel QPC protocol with χ-type entangled states is suggested; in Section 3, its correctness and security are investigated; finally, discussion and conclusion are given in Section 4.

2 The Proposed QPC Protocol

Assume that one user named Alice has a secret X and the other user named Bob has a secret Y, where $X = \sum_{j=0}^{N-1} x_j 2^j$, $Y = \sum_{j=0}^{N-1} y_j 2^j$ and $x_j, y_j \in \{0, 1\}$. They want to determine whether X and Y are equal or not with the help of a semi-honest TP, who is allowed to misbehave on his own but cannot conspire with the adversary. Similar to the QPC protocols of Refs. [26–28], the proposed protocol also uses the χ-type entangled states as the quantum resource, which are defined as

$$\begin{aligned} |\chi\rangle_{1234} &= \frac{\sqrt{2}}{4}(|0000\rangle - |0101\rangle + |0011\rangle + |0110\rangle + |1001\rangle + |1010\rangle \\ &\quad + |1100\rangle - |1111\rangle)_{1234} \\ &= \frac{1}{2}\left(|\varphi^+\rangle|00\rangle + |\varphi^-\rangle|11\rangle - |\psi^-\rangle|01\rangle + |\psi^+\rangle|10\rangle\right)_{1234} \\ &= \frac{1}{2}\left(|00\rangle|\varphi^+\rangle + |11\rangle|\varphi^-\rangle - |01\rangle|\psi^-\rangle + |10\rangle|\psi^+\rangle\right)_{1234} \end{aligned} \quad (1)$$

Here, $|\varphi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$ and $|\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$ are four Bell states. There parties, Alice, Bob and TP, agree that $|\varphi^{+}\rangle$ and $|00\rangle$ represent information 00; $|\varphi^{-}\rangle$ and $|11\rangle$ represent information 11; $|\psi^{-}\rangle$and $|01\rangle$ represent information 01; and $|\psi^{+}\rangle$ and $|10\rangle$ represent information 10.

Suppose that Alice and Bob establish one common binary key sequence K_{AB} with length of $\lceil N/2\rceil$between them through one of the good QKD protocols [1–3] beforehand. Similarly, Alice and TP (Bob and TP) also share one common binary key sequence K_{AT} (K_{BT}) with length of $\lceil N/2\rceil$ between them.

The proposed protocol is consisted of the following steps:

Step 1 Alice (Bob) divides her (his) binary representation of X (Y) into $\lceil N/2\rceil$ groups $G_A^1, G_A^2, \ldots, G_A^{\lceil N/2\rceil}$ $\left(G_B^1, G_B^2, \ldots, G_B^{\lceil N/2\rceil}\right)$, where each group contains two binary bits. If $N \bmod 2 = 1$, Alice (Bob) adds one 0 to $G_A^{\lceil N/2\rceil}$ $\left(G_B^{\lceil N/2\rceil}\right)$.

Step 2 TP prepares $\lceil N/2\rceil$ χ-type entangled states shown in formula (1). Then, he arranges these χ-type entangled states into one sequence

$$\left[P_{a_1}^1 P_{a_2}^1 P_{b_1}^1 P_{b_2}^1, P_{a_1}^2 P_{a_2}^2 P_{b_1}^2 P_{b_2}^2, \ldots, P_{a_1}^{\lceil N/2\rceil} P_{a_2}^{\lceil N/2\rceil} P_{b_1}^{\lceil N/2\rceil} P_{b_2}^{\lceil N/2\rceil}\right] \tag{2}$$

(hereafter called sequence P), where the subscripts a_1, a_2, b_1, b_2 represent four particles in one χ-type entangled state and the superscripts $1, 2, \ldots, \lceil N/2\rceil$ indicate the χ-type entangled states in the sequence.

TP takes particles a_1 and a_2 from each χ-type entangled state in P to form an ordered particle sequence P_A, i.e.,

$$P_A = \left[P_{a_1}^1 P_{a_2}^1, P_{a_1}^2 P_{a_2}^2, \ldots, P_{a_1}^{\lceil N/2\rceil} P_{a_2}^{\lceil N/2\rceil}\right]. \tag{3}$$

TP picks particles b_1 and b_2 from each χ-type entangled state in P to form an ordered particle sequenceP_B, i.e.,

$$P_B = \left[P_{b_1}^1 P_{b_2}^1, P_{b_1}^2 P_{b_2}^2, \ldots, P_{b_1}^{\lceil N/2\rceil} P_{b_2}^{\lceil N/2\rceil}\right]. \tag{4}$$

TP prepares two decoy photon sequences randomly in one of the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, and randomly inserts them into P_A and P_B, respectively. The two new sequences are represented as P'_A and P'_B, respectively. Here, $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. Then, TP sends P'_A $\left(P'_B\right)$ to Alice (Bob).

After receiving P'_A $\left(P'_B\right)$, Alice (Bob) performs the security check with TP. TP informs Alice (Bob) of the inserted positions and the preparation bases of decoy photons in P'_A $\left(P'_B\right)$. Then, Alice (Bob) measures the decoy photons in $P'_A(P'_B)$ with TP's preparation base and informs TP of her (his) measurement results. By comparing the prepared states of decoy photons in $P'_A(P'_B)$ with Alice's (Bob's) measurement results, TP can determine whether the transmission of P'_A $\left(P'_B\right)$ was eavesdropped or not. If the error rate is smaller than the threshold, Alice and Bob go on the next step; otherwise, the protocol is terminated.

Step 3 Alice (Bob) discards the decoy photons in P'_A $\left(P'_B\right)$ to get $P_A(P_B)$. Alice performs Bell basis measurement on particles $P_{a_1}^i$ and $P_{a_2}^i$ and obtains the measurement result M_A^i. If $P_{a_1}^i P_{a_2}^i$ is $|\varphi^{+}\rangle/|\varphi^{-}\rangle/|\psi^{-}\rangle/|\psi^{+}\rangle$, then M_A^i is 00 /11 /01 /10. Here, $\left\{|\varphi^{\pm}\rangle, |\psi^{\pm}\rangle\right\}$ is the Bell basis and $i \in \{1, 2, \ldots, \lceil N/2\rceil\}$.

In the meanwhile, Bob performs Z basis measurement on particles $P_{b_1}^i$ and $P_{b_2}^i$ to obtain the measurement result M_B^i. If $P_{b_1}^i P_{b_2}^i$ is $|\,00\,\rangle/|\,01\,\rangle/|\,10\,\rangle/|\,11\,\rangle$, then M_B^i is 00 /01 /10 /11. Here, $\{|\,0\,\rangle, |\,1\,\rangle\}$ is the Z basis and $i \in \{1, 2, \ldots, \lceil N/2 \rceil\}$.

Afterward, Alice (Bob) computes $R_A^i = G_A^i \oplus M_A^i \oplus K_{AT}^i \oplus K_{AB}^i$ $\left(R_B^i = G_B^i \oplus M_B^i \oplus K_{BT}^i \oplus K_{AB}^i\right)$, where $i \in \{1, 2, \ldots, \lceil N/2 \rceil\}$. Finally, Alice (Bob) publishes $R_A(R_B)$ to TP, where $R_A = \left[R_A^1, R_A^2, \ldots, R_A^{\lceil N/2 \rceil}\right]$ $\left(R_B = \left[R_B^1, R_B^2, \ldots, R_B^{\lceil N/2 \rceil}\right]\right)$.

Step 4 After receiving R_A and R_B, TP computes $R^i = R_A^i \oplus R_B^i \oplus K_{AT}^i \oplus K_{BT}^i$. If TP finds out that there is an i where $R^i \neq 00$, he concludes that $X \neq Y$, and terminates the protocol immediately; otherwise, he concludes that $X = Y$. Finally, TP informs Alice and Bob of the comparison result.

3 Analysis

3.1 Correctness

In this section, we verify the correctness of the output of the proposed protocol.

In the proposed protocol, Alice and Bob own $X = \sum_{j=0}^{N-1} x_j 2^j$ and $Y = \sum_{j=0}^{N-1} y_j 2^j$, respectively. They compare the equality of G_A^i and G_B^i with the help of a semi-honest TP. Due to the entanglement correlation of the χ-type entangled state shown in formula (1), it is apparent that $M_A^i \oplus M_B^i = 00$. Accordingly, we have

$$\begin{aligned} R^i &= R_A^i \oplus R_B^i \oplus K_{AT}^i \oplus K_{BT}^i \\ &= \left(G_A^i \oplus M_A^i \oplus K_{AT}^i \oplus K_{AB}^i\right) \\ &\quad \oplus \left(G_B^i \oplus M_B^i \oplus K_{BT}^i \oplus K_{AB}^i\right) \oplus K_{AT}^i \oplus K_{BT}^i \\ &= \left(G_A^i \oplus G_B^i\right) \oplus \left(M_A^i \oplus M_B^i\right) = G_A^i \oplus G_B^i. \end{aligned} \tag{5}$$

According to formula (5), if $R^i = 00$, it can be obtained that $G_A^i = G_B^i$; otherwise, we have $G_A^i \neq G_B^i$. Therefore, the output of our protocol is correct.

3.2 Security

In this section, we first consider the outside eavesdropper's attack, then analyze the participants' attack.

3.2.1 Outside Attack

We investigate the possibility for an outside eavesdropper to obtain X and Y according to each step of the proposed protocol.

In Step 1, there is not any transmission, so an outside eavesdropper has no opportunity to launch an attack.

In Step 2, TP sends P_A' $\left(P_B'\right)$ to Alice (Bob), so an outside eavesdropper can launch an attack during the transmission of P_A' $\left(P_B'\right)$. However, the decoy photon technology [39, 40] is used for security check in this step, which can detect some famous attacks, such as the

intercept-resend attack, the measure-resend attack, the entangle-measure attack, *etc*, with non-zero probability, as shown in Refs. [41, 42]. Moreover, since the qubit transmission is in a single-direction way, the Trojan horse attacks including the invisible photon eavesdropping attack [43] and the delay-photon Trojan horse attack [44], are also invalid. It can be concluded that in this step, an outside eavesdropper cannot obtain something useful about X and Y without being discovered.

In Step 3, Alice encrypts G_A^i with the one-time-pad keys M_A^i, K_{AT}^i and K_{AB}^i, which are unknown to an outside eavesdropper. In the meanwhile, Bob encrypts G_B^i with the one-time-pad keys M_B^i, K_{BT}^i and K_{AB}^i, which are also unknown to an outside eavesdropper. It is apparent that an outside eavesdropper cannot get $G_A^i\left(G_B^i\right)$ when Alice (Bob) publishes $R_A(R_B)$ to TP in this step, since she has no knowledge about these one-time-pad keys.

To sum up, the proposed protocol can successfully resist the outside attack.

3.2.2 Participant Attack

The term "participant attack" means the kind of attacks from dishonest participants, which is generally more powerful and should be paid more attention to, as first pointed out by Gao et al. [45] in 2007. In the following, we investigate three cases of participant attack in detail.

Case 1: Alice wants to know Bob's Private Information Y In Step 3, Alice can deduce Bob's measurement result of $P_{b_1}^i P_{b_2}^i$ from her own measurement result of $P_{a_1}^i P_{a_2}^i$ through the entanglement correlation of the χ-type entangled state shown in formula (1). Thus, in this step, Alice can know M_B^i from M_A^i. Even though Alice may hear R_B when Bob publishes it to TP in this step, she still cannot get G_B^i, because it is encrypted with the one-time-pad key K_{BT}^i. It can be concluded that Alice cannot know Bob's private information Y.

Case 2: Bob wants to know Alice's Private Information X In Step 3, Bob can deduce Alice's measurement result of $P_{a_1}^i P_{a_2}^i$ from his own measurement result of $P_{b_1}^i P_{b_2}^i$ through the entanglement correlation of the χ-type entangled state shown in formula (1). Thus, in this step, Bob can know M_A^i from M_B^i. Even though Bob may hear R_A when Alice publishes it to TP in this step, he still cannot get G_A^i, because it is encrypted with the one-time-pad key K_{AT}^i. It can be concluded that Bob cannot know Alice's private information X.

Case 3: TP wants to know Alice's Private Information X and Bob's Private Information Y The semi-honest TP may try his best to obtain Alice's private information X and Bob's private information$Y$.

In Step 3, TP receives $R_A(R_B)$ from Alice (Bob). However, even though TP may launch the malicious attacks similar to the ones suggested in Refs. [16–18] to obtain $M_A^i\left(M_B^i\right)$, he still cannot get $G_A^i\left(G_B^i\right)$ from $R_A^i\left(R_B^i\right)$, because it is encrypted with the one-time-pad key K_{AB}^i. It can be concluded that TP cannot know X and Y.

It needs to be pointed out that TP knows the comparison result of X and Y.

4 Discussion and Conclusion

As all of the proposed protocol and the QPC protocols in Refs. [26–28] are based on χ-type entangled states, we compare them in detail, as shown in Table 1, without considering the security check processes. The qubit efficiency η here is defined as $\eta = \frac{r_c}{r_q}$, where r_c is the

Table 1 Comparison among the two-party QPC protocols

	Ref. [26]	Ref. [27]	Ref. [28]	The proposed protocol
Initial quantum resource	$\chi-$type entangled states	$\chi-$type entangled states	$\chi-$type entangled states	$\chi-$type entangled states
Quantum measurement	$\chi-$type entangled state measurements	$\chi-$type entangled state measurements	Bell basis measurements and Z basis measurements	Bell basis measurements and Z basis measurements
Need of QKD method	Yes	No	Yes	Yes
Need of unitary operation	No	Yes	Yes	No
Need of entanglement swapping	Yes	No	No	No
TP's knowledge about the comparison result	No	Yes	Yes	Yes
Qubit efficiency η	50%	100%	25%	50%

number of the compared classical bits, and n_q is the number of consumed qubits [6]. In the proposed protocol, one χ-type entangled state can be used to compare two bit of private information from each party, thus its qubit efficiency is 50%.

In addition, it is worth pointing out that there is an alternative choice scheme of measurement basis for Alice and Bob. Concretely, in Step 3, Alice (Bob) chooses Z basis (Bell basis) to measure particle $P^i_{a_1}P^i_{a_2}\left(P^i_{b_1}P^i_{b_2}\right)$ and gets the measurement result $M^i_A\left(M^i_B\right)$. According to the entanglement correlation of the χ-type entangled state shown in formula (1), this alternative choice scheme of measurement basis also guarantees the correctness of the output of the proposed protocol.

To sum up, in this paper, we propose a two-party QPC protocol with a semi-honest TP by using χ-type entangled states. The proposed protocol needs to perform Bell basis measurements and single-particle measurements rather than χ-type entangled state measurements, and does not need to employ unitary operation and quantum entanglement swapping technology.

Compliance with Ethical Standards

Conflict of interests The author declares that he has no conflict of interest.

References

1. Bennett, C.H., Brassard, G.: Quantum cryptography: Public-key distribution and coin tossing. In: Proceeding IEEE international conference computers, systems and signal processing, pp. 175–179 (1984)
2. Ekert, A.K.: Quantum cryptography based on Bell's theorem. Phys. Rev. Lett. **67**(6), 661–663 (1991)
3. Bennett, C.H., Brassard, G., Mermin, N.D.: Quantum cryptography without Bell theorem. Phys. Rev. Lett. **68**, 557–559 (1992)
4. Hillery, M., Buzek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A **59**, 1829–1834 (1999)

5. Karlsson, A., Koashi, M., Imoto, N.: Quantum entanglement for secret sharing and secret splitting. Phys. Rev. A **59**, 162–168 (1999)
6. Chen, J.H., Lee, K.C., Hwang, T.: The enhancement of Zhou et al.'s quantum secret sharing protocol. Int. J. Mod. Phy. C **20**(10), 1531–1535 (1999)
7. Long, G.L., Liu, X.S.: Theoretically efficient high-capacity quantum-key-distribution scheme. Phys. Rev. A **65**, 032302 (2002)
8. Bostrom, K., Felbinger, T.: Deterministic secure direct communication using entanglement. Phys. Rev. Lett. **89**, 187902 (2002)
9. 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)
10. 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)
11. Yang, Y.G., Gao, W.F., Wen, Q.Y.: Secure quantum private comparison. Phys. Scr. **80**, 065002 (2009)
12. Yang, Y.G., Xia, J., Jia, X., Shi, L., Zhang, H.: New quantum private comparison protocol without entanglement. Int. J. Quantum. Inf. **10**, 1250065 (2012)
13. Ye, T.Y.: Quantum private comparison via cavity QED. Commun. Theor. Phys. **67**(2), 147–156 (2017)
14. Liu, W., Wang, Y.B., Cui, W.: Quantum private comparison protocol based on Bell entangled states. Commun. Theor. Phys. **57**, 583–588 (2012)
15. Tseng, H.Y., Lin, J., Hwang, T.: New quantum private comparison protocol using EPR pairs. Quantum. Inf. Process. **11**, 373–384 (2012)
16. Wang, C., Xu, G., Yang, Y.X.: Cryptanalysis and improvements for the quantum private comparison protocol using EPR pairs. Int. J. Quantum. Inf. **11**, 1350039 (2013)
17. Yang, Y.G., Xia, J., Jia, X., Zhang, H.: Comment on quantum private comparison protocols with a semi-honest third party. Quantum. Inf. Process. **12**, 877–885 (2013)
18. Zhang, W.W., Zhang, K.J.: Cryptanalysis and improvement of the quantum private comparison protocol with semi-honest third party. Quantum. Inf. Process. **12**, 1981–1990 (2013)
19. 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 (2010)
20. Lin, J., Tseng, H.Y., Hwang, T.: Intercept-resend attacks on Chen et al.'s quantum private comparison protocol and the improvements. Opt. Commun. **284**, 2412–2414 (2011)
21. Liu, W., Wang, Y.B.: Quantum private comparison based on GHZ entangled states. Int. J. Theor. Phys. **51**, 3596–3604 (2012)
22. Liu, W., Wang, Y.B., Jiang, Z.T.: An efficient protocol for the quantum private comparison of equality with W state. Opt. Commun. **284**, 3160–3163 (2011)
23. Zhang, W.W., Li, D., Li, Y.B.: Quantum private comparison protocol with W States. Int. J. Theor. Phys. **53**(5), 1723–1729 (2014)
24. Xu, G.A., Chen, X.B., Wei, Z.H., Li, M.J., Yang, Y.X.: An efficient protocol for the quantum private comparison of equality with a four-qubit cluster state. Int. J. Quantum. Inf. **10**, 1250045 (2012)
25. Sun, Z.W., Long, D.Y.: Quantum private comparison protocol based on cluster states. Int. J. Theor. Phys. **52**, 212–218 (2013)
26. Liu, W., Wang, Y.B., Jiang, Z.T., Cao, Y.Z.: A protocol for the quantum private comparison of equality with χ-type state. Int. J. Theor. Phys. **51**, 69–77 (2012)
27. Jia, H.Y., Wen, Q.Y., Li, Y.B., Cao, F.: Quantum private comparison using genuine four-particle entangled states. Int. J. Theor. Phys. **51**(4), 1187–1194 (2012)
28. Liu, W., Wang, Y.B., Jiang, Z.T., Cao, Y.Z., Cui, W.: New quantum private comparison protocol using χ-type state. Int. J. Theor. Phys. **51**, 1953–1960 (2012)
29. Ye, T.Y., Ji, Z.X.: Two-party quantum private comparison with five-qubit entangled states. Int. J. Theor. Phys. **56**(5), 1517–1529 (2017)
30. Ji, Z.X., Ye, T.Y.: Quantum private comparison of equal information based on highly entangled six-qubit genuine state. Commun. Theor. Phys. **65**(6), 711–715 (2016)
31. Chang, Y.J., Tsai, C.W., Hwang, T.: Multi-user private comparison protocol using GHZ class states. Quantum. Inf. Process. **12**, 1077–1088 (2013)
32. Wang, Q.L., Sun, H.X., Huang, W.: Multi-party quantum private comparison protocol with n-level entangled states. Quantum. Inf. Process. **13**, 2375–2389 (2014)
33. 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)
34. Liu, W., Wang, Y.B., Wang, X.M.: Quantum multi-party private comparison protocol using d-dimensional Bell states. Int. J. Theor. Phys. **54**, 1830–1839 (2015)

35. Huang, S.L., Hwang, T., Gope, P.: Multi-party quantum private comparison with an almost-dishonest third party. Quantum. Inf. Process. **14**, 4225–4235 (2015)
36. Huang, S.L., Hwang, T., Gope, P.: Multi-party quantum private comparison protocol with an almost-dishonest third party using GHZ states. Int. J. Theor. Phys. **55**, 2969–2976 (2016)
37. Ye, T.Y.: Multi-party quantum private comparison protocol based on entanglement swapping of Bell entangled states. Commun. Theor. Phys. **66**(3), 280–290 (2016)
38. Lo, H.K.: Insecurity of quantum secure computations. Phys. Rev. A **56**(2), 1154–1162 (1997)
39. Li, C.Y., Zhou, H.Y., Wang, Y., Deng, F.G.: Secure quantum key distribution network with Bell states and local unitary operations. Chin. Phys. Lett. **22**(5), 1049 (2005)
40. Li, C.Y., Li, X.H., Deng, F.G., Zhou, P., Liang, Y.J., Zhou, H.Y.: Efficient quantum cryptography network without entanglement and quantum memory. Chin. Phys. Lett. **23**(11), 2896 (2006)
41. Chen, Y., Man, Z.X., Xia, Y.J.: Quantum bidirectional secure direct communication via entanglement swapping. Chin. Phys. Lett. **24**(1), 19 (2007)
42. Ye, T.Y., Jiang, L.Z.: Improvement of controlled bidirectional quantum direct communication using a GHZ state. Chin. Phys. Lett. **30**(4), 040305 (2013)
43. Cai, Q.Y.: Eavesdropping on the two-way quantum communication protocols with invisible photons. Phys. Lett. A **351**(1), 23–25 (2006)
44. Gisin, N., Ribordy, G., Tittel, W., Zbinden, H.: Quantum cryptography. Rev. Mod. Phys. **74**(1), 145 (2002)
45. Gao, F., Qin, S.J., Wen, Q.Y., Zhu, F.C.: A simple participant attack on the Bradler-Dusek protocol. Quantum. Inf. Comput. **7**, 329 (2007)