Quantum Inf Process (2015) 14:4593–4600
DOI 10.1007/s11128-015-1145-3

Cryptanalysis and improvement of quantum private comparison of equality protocol without a third party

Bo Zhang[1] · **Xingtong Liu**[1] · **Jian Wang**[1] · **Chaojing Tang**[1]

Received: 27 May 2015 / Accepted: 3 October 2015 / Published online: 19 October 2015

Abstract Recently, Lin et al. proposed a novel quantum private comparison protocol without a third party (Quantum Inf. Process. 13:239–247, 2014). This paper points out two security loopholes in Lin et al.'s protocol, in which one dishonest party can disclose the other's private information without being detected and the comparison result can be manipulated completely by either party. In addition, improvements are proposed to avoid these loopholes.

Keywords Quantum cryptography · Quantum private comparison · Entanglement swapping · Security

1 Introduction

The original characteristics of quantum mechanics such as superposition and entanglement play an important role in quantum cryptography. Utilizing these properties, numerous applications in quantum cryptography, such as quantum key distribution [1–3], quantum secret sharing [4], quantum secure direct communication [5–7], and quantum authentication and signature [8–11], have been proposed. Recently, quantum private comparison (QPC) has gained a great deal of attention and become an important branch of quantum cryptography. Based on the principles of quantum mechanics, the QPC protocol can be used to privately compare the equality of players' secret without any complex computation.

✉ Bo Zhang
yumingsec@sina.com

[1] College of Electronic Science and Engineering, National University of Defense Technology, Changsha 410073, China

In fact, the private comparison concept originated in secure multiparty computation which has long been an important subject in classical cryptography. In [12,13], Yao proposed a protocol to solve the millionaires' problem, in which two millionaires wish to determine who is richer without knowing their actual worth. Thereafter, Boudot et al. [14] proposed a protocol to decide whether the two millionaires are equally rich. However, Lo [15] in 1997 pointed out that it is impossible to construct a secure equality function in a two-party scenario. Thus, some additional assumptions, i.e., a semi-honest third party (TP), should be considered in QPC protocols.

The earliest two QPC protocols were proposed by Yang et al. [16,17] in 2009, utilizing two-photon entangled Einstein–Podolsky–Rosen (EPR) pairs and polarized single photons, respectively. Since then, the development of QPC techniques has mainly fallen into three paradigms [18]: "the quantum cryptography QPC [19,20], the superdense coding QPC [16,17,21–25], and the entanglement swapping QPC [26–28]."

Cryptanalysis is a very important part of cryptography. It finds potential loopholes from an eavesdropper's viewpoint and improves the protocol's security level. As pointed out by Lo and Ko, breaking cryptographic systems is as important as building them [29]. With the development of quantum cryptography, various attack strategies have been proposed, such as intercept-resend attacks [30], entanglement swapping attacks [31,32], teleportation attacks [33], dense coding attacks [34–36], channel-loss attacks [37,38], denial-of-service attacks [39,40], correlation-extractability attacks [41–45], Trojan horse attacks [46,47], and participant attacks [32,36]. Understanding these attacks is helpful for designing new protocols with high security.

Recently, Lin et al. [48] proposed a novel two-party QPC protocol based on the entanglement swapping of two EPR pairs without the help of a TP, and this protocol has been claimed to be unconditionally secure. Clearly, a contradiction exists between Lin et al.'s "secure" QPC protocol without a TP and Lo's result [15]. This contradiction needs to be clarified. In this paper, we show that Lin et al.'s protocol is not as secure as claimed. We find two security loopholes in Lin et al.'s protocol. First, a dishonest party can disclose the other's private information without being detected. The proposed attack exploits the fact that the one-time-pad key encryption can be broken by manipulating the transmission of quantum sequences between two users. As far as we know, this is a new participant attack scenario that has not yet been addressed in the existing literature. Second, the comparison result can be manipulated completely by either party. Finally, improvements are proposed to avoid these loopholes.

The rest of this paper is organized as follows. Section 2 reviews Lin et al.'s two-party QPC protocol. Section 3 points out two security loopholes in Lin et al.'s protocol and proposes our improvements. Section 4 concludes the paper.

2 Review of Lin et al.'s QPC protocol

Let Alice and Bob be the two parties who want to compare the equality of their M-bit secret messages, M_A and M_B, respectively. They agree that four Bell states $\{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$ represent the classical bits $\{00, 01, 10, 11\}$, respectively. Lin et al.'s QPC protocol proceeds by the following steps:

Step 1 Alice (Bob) prepares a sequence of EPR pairs S_A (S_B) according to each of the two bits of M_A (M_B), each randomly in the following states,

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

Alice (Bob) then divides them into two ordered sequences S_{A_1} and S_{A_2} (S_{B_1} and S_{B_2}) composed of the 1_{st} and 2_{nd} particles of each EPR pair, respectively. Alice (Bob) then randomly inserts some decoy photons D_A (D_B) into S_{A_1} (S_{B_1}) to form a new sequence $S^{'}_{A_1}$ $(S^{'}_{B_1})$, with each decoy photon randomly in $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Finally, Alice (Bob) sends $S^{'}_{A_1}$ $(S^{'}_{B_1})$ to Bob (Alice).

Step 2 To guarantee the transmission security, after confirming that Bob has received $S^{'}_{A_1}$, Alice publishes the positions and measurement bases of D_A. Bob then performs the corresponding measurements on those decoy photons and publishes the measurement results. Alice then checks for the existence of an eavesdropper. In the same way, after confirming that Alice has received $S^{'}_{B_1}$, Bob publishes the information for D_B. Alice then performs measurements on D_B and publishes the measurement results. If there is no eavesdropper, the protocol continues. Otherwise, they abort the communication and restart from Step 1.

Step 3 Alice (Bob) performs a Bell measurement on $S^i_{B_1}$, $S^i_{A_2}$ ($S^i_{A_1}$,$S^i_{B_2}$), where i represents the i_{th} set of EPR pairs. Thereafter, Alice (Bob) obtains an M-bit measurement result C_A (C_B). They then employ the hash function [49], i.e., $H : \{0, 1\}^N \rightarrow \{0, 1\}^M$, on their secret message (M_A and M_B) to obtain two hash codes, $H(M_A)$ and $H(M_B)$, each of M bits in length. Finally, Alice (Bob) computes the exclusive-OR result R_A (R_B) of C_A and $H(M_A)$ (C_B and $H(M_B)$), i.e., $R_A = C_A \oplus H(M_A)$ and $R_B = C_B \oplus H(M_B)$.

Step 4 Alice (Bob) publishes R_A (R_B). If $R_A = R_B$, Alice's and Bob's secret messages are regarded as equal. Otherwise, their secret messages are regarded as different.

We now explain the basic concepts of Lin et al.'s QPC protocol. The outcome collections of entanglement swapping between any two Bell states are listed in Table 1. If the two initial Bell states are identical, then the two measurement results after entanglement swapping will also be the same, i.e., $|\psi^-\rangle_{A_1A_2}|\psi^-\rangle_{B_1B_2} = \frac{1}{2}(|\phi^+\rangle|\phi^+\rangle - |\phi^-\rangle|\phi^-\rangle - |\psi^+\rangle|\psi^+\rangle + |\psi^-\rangle|\psi^-\rangle)_{B_1A_2A_1B_2}$. This feature is used in Step 4. If $M_A = M_B$, then $C_A = C_B$ and $R_A = R_B$. Furthermore, the measurement results after entanglement swapping will cover the secret message with a one-time-pad key, so one party (say Alice) will not be able to deduce the other party's (Bob's) secret message M_B from C_A, M_A, and $R_B = C_B \oplus H(M_B)$. However, we find that Lin et al.'s QPC protocol is not as secure as expected. Details are explained in the next section.

Table 1 Entanglement swapping results

	$\lvert\phi^+\rangle_{B_1B_2}$	$\lvert\phi^-\rangle_{B_1B_2}$	$\lvert\psi^+\rangle_{B_1B_2}$	$\lvert\psi^-\rangle_{B_1B_2}$
$\lvert\phi^+\rangle_{A_1A_2}$	C_0	C_1	C_2	C_3
$\lvert\phi^-\rangle_{A_1A_2}$	C_1	C_0	C_3	C_2
$\lvert\psi^+\rangle_{A_1A_2}$	C_2	C_3	C_0	C_1
$\lvert\psi^-\rangle_{A_1A_2}$	C_3	C_2	C_1	C_0

Four collections composed by different outcome combinations of B_1A_2 and A_1B_2 are labeled as C_0, C_1, C_2, and C_3, where $C_0 = \{|\phi^+\rangle_{B_1A_2}|\phi^+\rangle_{A_1B_2}, |\phi^-\rangle_{B_1A_2}|\phi^-\rangle_{A_1B_2}, |\psi^+\rangle_{B_1A_2}|\psi^+\rangle_{A_1B_2}, |\psi^-\rangle_{B_1A_2}|\psi^-\rangle_{A_1B_2}\}$, $C_1 = \{|\phi^-\rangle_{B_1A_2}|\phi^+\rangle_{A_1B_2}, |\phi^+\rangle_{B_1A_2}|\phi^-\rangle_{A_1B_2}, |\psi^+\rangle_{B_1A_2}|\psi^-\rangle_{A_1B_2}, |\psi^-\rangle_{B_1A_2}|\psi^+\rangle_{A_1B_2}\}$, $C_2 = \{|\phi^+\rangle_{B_1A_2}|\psi^+\rangle_{A_1B_2}, |\phi^-\rangle_{B_1A_2}|\psi^-\rangle_{A_1B_2}, |\psi^+\rangle_{B_1A_2}|\phi^+\rangle_{A_1B_2}, |\psi^-\rangle_{B_1A_2}|\phi^-\rangle_{A_1B_2}\}$, $C_3 = \{|\phi^-\rangle_{B_1A_2}|\psi^+\rangle_{A_1B_2}, |\phi^+\rangle_{B_1A_2}|\psi^-\rangle_{A_1B_2}, |\psi^-\rangle_{B_1A_2}|\phi^+\rangle_{A_1B_2}, |\psi^+\rangle_{B_1A_2}|\phi^-\rangle_{A_1B_2}\}$

3 Loopholes and improvements

A QPC protocol should ensure privacy and fairness [18]. Privacy means that outside parties can not learn players' secret information nor deduce it from the comparison result. Moreover, one player cannot know the other's secret. Fairness means that one party knows the sound result of a private comparison if and only if the other party knows the sound result. In this section, we point out two security loopholes in Lin et al.'s protocol. The first loophole concerns privacy, and the second one concerns fairness. Correspondingly, improvements to address both loopholes are proposed.

3.1 Loophole I

This subsection shows that Lin et al.'s QPC protocol cannot ensure privacy. A dishonest party (say Bob) can obtain the other party's (Alice's) secret without being detected. The detailed processes are as follows.

In Step 1, Bob prepares nothing and just waits for Alice.

In Step 2, after confirming that Bob has received S'_{A_1}, Alice publishes the positions and measurement bases of D_A. Bob then performs the corresponding measurements on those decoy photons and publishes the measurement results. Alice then checks for the existence of an eavesdropper. At this point, Bob has recovered original sequence S_{A_1} from disturbed sequence S'_{A_1}. Bob then inserts some decoy photons D_B into S_{A_1} to form a new sequence S''_{A_1} and sends it to Alice. After confirming that Alice has received S''_{A_1}, Alice and Bob check for the existence of an eavesdropper, as described above. Alice then recovers original sequence S_{A_1} from disturbed sequence S''_{A_1}.

In Step 3, Alice performs Bell measurements on $(S^i_{A_1}, S^i_{A_2})$, which is actually the EPR pair she prepared. Thus, Alice's measurement result C_A equals M_A. Finally, Alice computes $R_A = C_A \oplus H(M_A) = M_A \oplus H(M_A)$, which means that the original one-time-pad encryption no longer exists.

In Step 4, after Alice publishes R_A, Bob will obtain Alice's secret message M_A from $R_A = M_A \oplus H(M_A)$ without being detected. More precisely, Bob only needs at most 2^M hash computations together with exclusive-OR computations to determine the exact M_A from R_A. For large M, this is a difficult task in classical cryptography using current technology, but it is not difficult for an adversary in quantum cryptography, who is assumed to have infinite resources and computation power.

3.2 Loophole II

This subsection shows that Lin et al.'s QPC protocol cannot ensure fairness. The comparison result can be manipulated completely by either party because it is fully determined by the classical information published by both parties in Step 4. Thus, the latter party who publishes the exclusive-OR result in Step 4 can manipulate the comparison result completely. For example, after Alice publishes R_A, Bob knows the true comparison result immediately. Bob can then publish R_B ($R_B = R_A$) to make Alice believe their secret messages are the same or publish another R_B ($R_B \neq R_A$) to make Alice believe their secret messages are different. Of course, one could argue that in a QPC protocol with a TP, either party (Alice or Bob) can tell lies to affect the final comparison result. However, it should be noted that in such a protocol, the comparison result will not be manipulated completely by either party (Alice or Bob), because there are some key parameters on the TP's site that cannot be accessed by the parties. More specifically, neither party (Alice nor Bob) can determine the exact operations to manipulate the final comparison result. As a result, most QPC protocols with a TP congenitally ensure fairness. In some cases, users may only care about the privacy of secure multiparty computation and fairness could be neglected [50]. However, it should be noted that fairness cannot be neglected in some cases that require a high security level, e.g., a QPC protocol that compares not only the equality but also the relative size (which is the larger/smaller) of users' secrets [51].

3.3 Improvements of Lin et al.'s protocol

To avoid the privacy loophole described in Sect. 3.1, a possible countermeasure is that the two parties do not publish the decoy photon information until both of them have received the quantum sequence in Step 2. Thereafter, Bob cannot replace $S^{'}_{B_1}$ with $S^{''}_{A_1}$ and then obtain Alice's secret message M_A from R_A.

As described in Sect. 3.2, fairness may be neglected sometimes, but it cannot be neglected if the protocol requires a high security level in some cases. To avoid the fairness loophole described in Sect. 3.2, a semi-honest TP should be introduced with only a simple modification. A semi-honest TP is allowed to misbehave on its own, but cannot conspire with either of two parties [52]. The modified protocol proceeds according to the following steps:

*Step 1** Alice (Bob, the TP) prepares a sequence of EPR pairs S_A (S_B, S_T) according to each of the two bits of M_A (M_B, M_T), each randomly in one of the Bell states $|\phi^{\pm}\rangle, |\psi^{\pm}\rangle$, where M_T denotes the TP's random number. Alice (Bob, the TP) then divides them into two ordered sequences S_{A_1} and S_{A_2} (S_{B_1} and S_{B_2}, S_{T_1}, and S_{T_2}), which is composed by the 1_{st} and 2_{nd} particles of each EPR pair, respectively. Alice (the TP) then randomly inserts some decoy photons D_A (D_T) into S_{A_2} (S_{T_2}) to form a new sequence S'_{A_2} (S'_{T_2}), with each decoy photon randomly in $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Finally, Alice (the TP) sends S'_{A_2} (S'_{T_2}) to the TP (Alice).

*Step 2** Alice and the TP do not publish the decoy photon information until both of them have received the quantum sequence. They then check the security of the Alice-TP channel, as in Step 2. At this point, Alice (the TP) can obtain the sequences S_{A_1} and S_{T_2} (S_{T_1} and S_{A_2}). Alice measures each pair in (S_{A_1}, S_{T_2}) using Bell basis and obtains result C_A. Bob (the TP) prepares some decoy photons D_B (D'_T) to protect the transmission of S_{B_2} (S_{A_2}), as described above.

*Step 3** Bob measures each pair in (S_{B_1}, S_{A_2}) using Bell basis and obtains result C_B. The TP also measures each pair in (S_{T_1}, S_{B_2}) using Bell basis and obtains result C_T. Alice and Bob then, respectively, calculate $R_A = C_A \oplus H(M_A)$ and $R_B = C_B \oplus H(M_B)$.

*Step 4** Alice (Bob) publishes R_A (R_B) to the TP. The TP calculates $R = R_A \oplus R_B \oplus M_T \oplus C_T$. If $R = 0$, Alice's and Bob's secret messages are regarded as equal. Otherwise, their secret messages are regarded as different.

Clearly, the comparison result is not fully determined by the classical information published by both parties anymore, so the fairness loophole has been fixed. We now consider the correctness and security of the modified protocol above.

According to Table 1, we can see that $IS_1 \oplus MR_1 = IS_2 \oplus MR_2$, where $\{IS_1, IS_2\}$ are the two-bit codes of the two initial Bell states and $\{MR_1, MR_2\}$ are the two-bit codes of the two measured Bell states after entanglement swapping. If $M_A = M_B$, the responding measurement results C_A, C_B, and C_T satisfy the following equation:

$$C_B \oplus C_T = C_A \oplus M_T. \tag{1}$$

Thus, if $M_A = M_B$, then $R = R_A \oplus R_B \oplus M_T \oplus C_T = H(M_A) \oplus H(M_B) = 0$. The correctness of the modified protocol is guaranteed by Eq.(1).

In our second improvement, the measurement results after entanglement swapping will cover the secret with a one-time-pad key. More specifically, the TP cannot infer M_A (M_B) from C_T, M_T, and $R_A = C_A \oplus H(M_A)$ ($R_B = C_B \oplus H(M_B)$) because the initial state M_A (M_B) is unknown to him/her, and hence he/she cannot deduce the measurement result C_A (C_B) through the principle of entanglement swapping. A dishonest party (say Bob) cannot infer Alice's secret from $R_A = C_A \oplus H(M_A)$ and $R_B = C_B \oplus H(M_B)$ because M_T and C_T are unknown to him. Due to the use of decoy photons, it is secure against outside attackers. Similar results can also be found in [27,53,54].

4 Conclusion

In this paper, we described two security loopholes in Lin et al.'s two-party QPC protocol. In this protocol, a dishonest party can obtain the other's secret messages without being detected. In addition, the comparison procedure without the help of a TP directly leads to the fact that the comparison result can be manipulated completely by either party. We also propose two improvements to avoid these loopholes.

References

1. Bennett, C.H., Brassard, G.: Quantum cryptography: public-key distribution and coin tossing. In: IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, IEEE, New York, pp. 175–179 (1984)
2. Ekert, A.K.: Quantum cryptography based on Bell theorem. Phys. Rev. Lett. **67**(6), 661–663 (1991)
3. Bennett, C.H.: Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. **68**(21), 3121–3124 (1992)
4. Hillery, M., Buzěk, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A **59**, 1829–1834 (1999)
5. Beige, A., Englert, B., Kurtsiefer, C., Weinfurter, H.: Secure communication with a publicly known key. Acta Phys. Pol. A **101**, 901 (2002)
6. Boström, K., Felbinger, T.: Deterministic secure direct communication using entanglement. Phys. Rev. Lett. **89**, 187902 (2002)
7. 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)
8. Dušek, M., Haderka, O., Hendrych, M.: Quantum identification system. Phys. Rev. A **60**, 149–156 (1999)
9. Curty, M., Santos, D.J.: Quantum authentication of classical messages. Phys. Rev. A **64**, 062309 (2001)
10. Ljunggren, D., Bourennane, M., Karlsson, A.: Authority-based user authentication in quantum key distribution. Phys. Rev. A **62**, 022305 (2000)
11. Yang, Y.G., Zhou, Z., Teng, Y.W., Wen, Q.Y.: Arbitrated quantum signature with an untrusted arbitrator. Eur. Phys. J. D **61**(3), 773–778 (2011)
12. Yao, A.C.: Protocols for secure computations. In: Proceedings of the 23rd Annual Symposium on Foundations of Computer Science (1982)
13. Yao, A.C.: How to generate and exchange secrets. In: Proceedings of the 27th Annual Symposium on Foundations of Computer Science (1986)
14. Boudot, F., Schoenmakers, B., Traoré, J.: A fair and efficient solution to the socialist millionaires' problem. Discret Appl. Math. **111**(1–2), 23–36 (2001)
15. Lo, H.K.: Insecurity of quantum secure computations. Phys. Rev. A **56**(2), 1154–1162 (1997)
16. 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)
17. Yang, Y.G., Cao, W.F., Wen, Q.Y.: Secure quantum private comparison. Phys. Scr. **80**(6), 065002 (2009)
18. Liu, W.J., Liu, C., Wang, H.B., Jia, T.T.: Quantum private comparison: a review. IETE Tech. Rev. **30**(5), 439–445 (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**(7), 1561–1565 (2010)
20. Tseng, H.Y., Lin, J., Hwang, T.: New quantum private comparison protocol using EPR pairs. Quantum Inf. Process. **11**(2), 373–384 (2012)
21. 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. **12**(2), 887–897 (2013)
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**(12), 3160–3163 (2011)
23. Li, Y.B., Wen, Q.Y., Gao, F., Jia, H.Y., Sun, Y.: Information leak in Liu et al'.s quantum private comparison and a new protocol. Eur. Phys. J. D **66**(4), 110 (2012)
24. Jia, H.Y., Wen, Q.Y., Li, Y.B., Gao, F.: Quantum private comparison using genuine four particle entangled states. Int. J. Theor. Phys. **51**(4), 1187–1194 (2012)
25. 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**(6), 1953–1960 (2012)
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**(1), 69–77 (2012)
27. Liu, W., Wang, Y.B., Cui, W.: Quantum private comparison protocol based on Bell entangled states. Commun. Theor. Phys. **57**(4), 583–588 (2012)
28. Liu, W., Wang, Y.B.: Quantum private comparison based on GHZ entangled states. Int. J. Theor. Phys. **51**(11), 3596–3604 (2012)
29. Lo, H., Ko, T.: Some attacks on quantum-based cryptographic protocols. Quantum Inf. Comput. **5**, 41 (2005)

30. Gao, F., Guo, F.Z., Wen, Q.Y., Zhu, F.C.: Comment on "Experimental demonstration of a quantum protocol for byzantine agreement and liar detection". Phys. Rev. Lett. **101**, 208901 (2008)
31. Zhang, Y.S., Li, C.F., Guo, G.C.: Comment on "Quantum key distribution without alternative measurements". Phys. Rev. A **63**, 036301 (2001)
32. Gao, F., Qin, S., Wen, Q.Y., Zhu, F.C.: A simple participant attack on the Bradler-Dusek protocol. Quantum Inf. Comput. **7**, 329–334 (2007)
33. Gao, F., Wen, Q.Y., Zhu, F.C.: Teleportation attack on the QSDC protocol with a random basis and order. Chin. Phys. B **17**, 3189–3193 (2008)
34. Gao, F., Qin, S., Guo, F.Z., Wen, Q.Y.: Dense-coding attack on three-party quantum key distribution protocols. IEEE J. Quantum Electron. **47**, 630–635 (2011)
35. Hao, L., Li, J.L., Long, G.L.: Eavesdropping in a quantum secret sharing protocol based on Grover algorithm and its solution. Sci. China Phys. Mech. Astron. **53**, 491–495 (2010)
36. Qin, S., Gao, F., Wen, Q.Y., Zhu, F.C.: Improving the security of multiparty quantum secret sharing against an attack with a fake signal. Phys. Lett. A **357**, 101–103 (2006)
37. Wójcik, A.: Eavesdropping on the "Ping-Pong" quantum communication protocol. Phys. Rev. Lett. **90**, 157901 (2003)
38. Wójcik, A.: Comment on "Quantum dense key distribution". Phys. Rev. A **71**, 016301 (2005)
39. Cai, Q.Y.: The "Ping-Pong" protocol can be attacked without eavesdropping. Phys. Rev. Lett. **91**, 109801 (2003)
40. Gao, F., Guo, F.Z., Wen, Q.Y., Zhu, F.C.: Consistency of shared reference frames should be reexamined. Phys. Rev. A **77**, 014302 (2008)
41. Gao, F., Wen, Q.Y., Zhu, F.C.: Comment on: "Quantum exam". Phys. Lett. A **360**, 748–750 (2007)
42. Gao, F., Lin, S., Wen, Q.Y., Zhu, F.C.: A special eavesdropping on one-ender versus N-receiver QSDC protocol. Chin. Phys. Lett. **25**, 1561–1563 (2008)
43. Gao, F., Qin, S., Wen, Q., Zhu, F.C.: Cryptanalysis of multiparty controlled quantum secure direct communication using Greenberger–Horne–Zeilinger state. Opt. Commun. **283**, 192–195 (2010)
44. Yang, Y.G., Naseri, M., Wen, Q.Y.: Improved secure quantum sealed-bid auction. Opt. Commun. **282**(20), 4167–4170 (2009)
45. Yang, Y.G., Teng, Y.W., Chai, H.P., Wen, Q.Y.: Revisiting the security of secure direct communication based on ping-pong protocol. Quantum Inf. Process. **10**(3), 317–323 (2011)
46. Gisin, N., Fasel, S., Kraus, B., Zbinden, H., Ribordy, G.: Trojan-horse attacks on quantum-key-distribution systems. Phys. Rev. A **73**, 022320 (2006)
47. Deng, F.G., Li, X.H., Zhou, H.Y., Zhang, Z.J.: Improving the security of multiparty quantum secret sharing against Trojan horse attack. Phys. Rev. A **72**, 044302 (2005)
48. Lin, J., Yang, C.W., Hwang, T.: Quantum private comparison of equality protocol without a third party. Quantum Inf. Process. **13**, 239–247 (2014)
49. Damgard, I.B.: A design principle for hash functions. Adv. Cryptol. **89**(435), 416–427 (1990)
50. Zhang, C., Sun, Z.W., Huang, X., Long, D.Y.: Three-party quantum summation without a trusted third party. Int. J. Quantum Inf. **13**, 1550011 (2015)
51. Zhang, W.W., Li, D., Zhang, K.J., Zuo, H.J.: A quantum protocol for millionaire problem with Bell states. Quantum Inf. Process. **12**, 2241–2249 (2013)
52. 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)
53. Chen, Y.T., Hwang, T.: Comment on the "Quantum private comparison protocol based on Bell entangled states". Int. J. Theor. Phys. **53**, 837–840 (2014)
54. Liu, W.J., Liu, C., Chen, H.W., Li, Z.Q., Liu, Z.H.: Cryptanalysis and improvement of quantum private comparison protocol based on Bell entangled states. Commun. Theor. Phys. **62**, 210–214 (2014)