Quantum Inf Process (2013) 12:877–885
DOI 10.1007/s11128-012-0433-4

Comment on quantum private comparison protocols with a semi-honest third party

Yu-Guang Yang · Juan Xia · Xin Jia · Hua Zhang

Received: 26 March 2012 / Accepted: 11 June 2012 / Published online: 22 June 2012

Abstract As an important branch of quantum cryptography, quantum private comparison (QPC) has recently received a lot of attention. In this paper we study the security of previous QPC protocols with a semi-honest third party (TP) from the viewpoint of secure multi-party computation and show that the assumption of a semi-honest TP is unreasonable. Without the unreasonable assumption of a semi-honest TP, one can easily find that the QPC protocol (Tseng et al. in Quantum Inf Process, 2011, doi:10.1007/s11128-011-0251-0) has an obvious security flaw. Some suggestions about the design of QPC protocols are also given.

Keywords Secure multiparty computation · Quantum private comparison · Security

1 Introduction

As we know, the security of most classical cryptosystems is based on the assumption of computational complexity so that it is conditionally secure. Different from its classical counterpart, quantum cryptography can attain unconditional security because the security is ensured by physical principles such as the Heisenberg uncertainty principle and the quantum no-cloning theorem. Hence quantum cryptography has attracted a

Y.-G. Yang (✉) · J. Xia · X. Jia
College of Computer Science and Technology, Beijing University of Technology, Beijing 100124, China
e-mail: yangyang7357@bjut.edu.cn

Y.-G. Yang
State Key Laboratory of Integrated Services Network, Xidian University, Xi'an 710071, China

H. Zhang
State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China

lot of attention. Many quantum cryptography protocols are designed for quantum key distribution (QKD) [1–3], quantum secure direct communication (QSDC) [4–9], quantum secret sharing (QSS) [10–27], quantum authentication and signature [28–34] and so on.

Secure multi-party computation (SMC) are fundamental primitives in modern cryptography, allowing a group of mutually distrustful players to perform correct, distributed computations without leaking their respective secret inputs. SMC can be applied extensively to many applications including secret voting, private querying of database, oblivious negotiation, playing mental poker, etc..

As a fundamental primitive in secure multi-party quantum computation, verifiable quantum secret sharing (VQSS) also attracts some attention [35,36]. Based on Lagrange interpolation formula and the post-verification mechanism, Yang et al. [35] first constructed a verifiable quantum (k, n)-threshold secret key sharing scheme. Then they also showed how to construct a verifiable quantum (k, n)-threshold scheme by combining a qubit authentication process [36].

In the traditional secure two-party computation scenario [37,38], Alice has secret input x, Bob has secret input y, and both of them wish to compute $f(x, y)$ which is well-known to the two parties; the usual example is that of Yao's millionaires' problem where two millionaires wish to know who is richer; however, they do not want to find out inadvertently any additional information about each other's wealth [38]. Based on Yao's millionaires' problem, Boudot et al. [39] subsequently proposed a protocol to decide whether two millionaires are equally rich. However, Lo [40] pointed out that the equality function cannot be securely evaluated with a two-party scenario. Therefore, an additional assumption with a TP is necessary to reach the goal of private comparison.

Now, private comparison for equality problem has been discussed and generalized to the quantum cryptographic scenario [41–48]. Yang et al. [41,42] first discussed this issue and proposed a QPC protocol based on the decoy photons and two-photon entangled Einstein–Podolsky–Rosen (EPR) pairs and another QPC protocol with polarized single photons respectively. Then, Chen et al. [43] proposed a protocol for dealing with the private comparison of equal information based on the triplet Greenberger–Horne–Zeilinger (GHZ) entangled states. In ref. [44], Tseng et al. proposed a QPC protocol using EPR pairs. In refs. [45–47], Liu et al. proposed three QPC protocols based on the triplet W states and χ-type genuine four-particle entangled states respectively. In ref. [48], Jia et al. [49] proposed another QPC protocol based on χ-type genuine four-particle entangled states. They also proposed a more difficult quantum solution for millionaire problem.

The design and the cryptanalysis are two important parts of quantum cryptography. Cryptanalysis is aimed to find potential loopholes in the quantum cryptography protocols and try to overcome them. In the study of quantum cryptography, quite a few effective attack strategies have been proposed, such as intercept-resend attacks [50], entanglement swapping attacks [51,52], teleportation attacks [53], dense coding attacks [54–56], channel-loss attacks [57,58], denial-of-service attacks [59,60], correlation-extractability attacks [61–65], Trojan horse attacks [66,67], participant attacks [52,56], fake-particle attack [56,68], man-in-the-middle attack [69]. Understanding those attacks will be helpful for us to design new schemes with high security.

After analyzing the QPC protocols for equality problem [43–48], we find that in all these protocols there is an assumption that the TP is semi-honest. They assumed that the semi-honest TP executes the protocol loyally and records all the results of its intermediate computations but he might try to steal the information from the record. However, we show that the assumption of a semi-honest TP is unreasonable. The reasons are as follows. First, from the viewpoint of secure multi-party computation, a group of players should be mutually distrustful and try to eavesdrop other players' secret inputs without leaking their respective secret inputs. Second, from another viewpoint of quantum cryptography, the aim of a quantum cryptography protocol is to attain unconditional security so that it should not have any assumption different from its classical counterpart, where the security of most classical cryptosystems is based on the assumption of computational complexity so that it is conditionally secure. At last, in real situations, the TP will surely try to eavesdrop the secret information of Alice and Bob by means of various attack ways and he never simply executes the protocol loyally, records all the results of its intermediate computations and tries to steal the information from the record. Obviously we cannot say a user, who is trying to steal the secrets, can only perform some limited operations but cannot do others. This kind of assumption is meaningless. If we can do that, we had better assume that the eavesdropper can only do classical operations, where all quantum protocols might be secure. This is also obvious without any doubt. Hence, the semi-honest TP's assumption is impractical and unreasonable.

When we analyze the security of a QPC protocol, we should pay attention to an important security requirement for QPC; i.e., although the QPC task is implemented with the help of a TP, the TP cannot learn any information about the players' respective private inputs by means of various active and passive attacks. In fact the attack from TP is a kind of "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. [52].

Without the unreasonable assumption of a semi-honest TP, one can easily find that the QPC protocol [44] has an obvious security flaw. The analysis process is described in detail. In addition, we make a simple comparison of the security of the QPC protocols with a semi-honest TP [43–48] and some suggestions about the design of QPC protocols are given.

The rest of this paper is organized as follows. In Sect. 2 we analyze the security of QPC protocol in ref. [44], where the protocol is briefly recalled and analyzed. And Sect. 3 is our discussion and conclusion.

2 Analysis of the QPC protocol with Bell states

In this section we first recall the QPC protocol briefly and our security analysis follows.

2.1 The QPC protocol with Bell states

The QPC protocol with Bell states [44] is as follows.

Step 1. TP prepares N EPR pairs randomly chosen from four Bell states $\left|\phi^{+}\right\rangle$, $\left|\phi^{-}\right\rangle$, $\left|\psi^{+}\right\rangle$ and $\left|\psi^{-}\right\rangle$, which can be expressed in the form as shown in Eq. (1). TP divides these EPR pairs into two quantum sequences, namely S_A and S_B. The first particles and the second particles of all EPR pairs are in S_A and S_B respectively.

$$\begin{aligned}
\left|\phi^{+}\right\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) = \frac{1}{\sqrt{2}}\left(|{+}{+}\rangle + |{-}{-}\rangle\right) \\
\left|\phi^{-}\right\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right) = \frac{1}{\sqrt{2}}\left(|{-}{+}\rangle - |{+}{-}\rangle\right) \\
\left|\psi^{+}\right\rangle &= \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right) = \frac{1}{\sqrt{2}}\left(|{+}{+}\rangle - |{-}{-}\rangle\right) \\
\left|\psi^{-}\right\rangle &= \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right) = \frac{1}{\sqrt{2}}\left(|{-}{+}\rangle - |{+}{-}\rangle\right)
\end{aligned} \tag{1}$$

Step 2. TP prepares two sets of decoy photons D_A and D_B randomly in photon states: $|0\rangle$, $|1\rangle$, $|+\rangle$ $(= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle))$, and $|-\rangle$ $(= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle))$. TP randomly inserts D_A in S_A (D_B in S_B) to form two new sequences S_A^* and S_B^*, respectively. Later, he/she sends the quantum sequence S_A^* to Alice, S_B^* to Bob.

Step 3. After the quantum sequences have been received by Alice and Bob, they will each store the received photons. For the eavesdropping check, TP will announce the positions and the measuring bases (Z basis or X basis) of D_A and D_B. Then Alice and Bob will extract the particles in D_A and D_B, respectively, and perform the corresponding basis measurement to obtain two sequences of measuring results (R_A and R_B). Afterwards, Alice and Bob report the measuring results R_A and R_B to TP, respectively. They can check the existence of an eavesdropper by a predetermined threshold of error rate. If there is no eavesdropper, then the protocol can continue to the next step. Otherwise, TP aborts the protocol and restarts from Step 1.

Step 4. Alice and Bob can recover S_A and S_B respectively by discarding the decoy photons (D_A and D_B). They use Z basis to measure the photons in S_A and S_B, respectively. If the measurement result is $|0\rangle$ ($|1\rangle$), then encode it as the classical bit '0' ('1'). Thus, Alice and Bob individually will obtain a key bit string, which are denoted as K_A and K_B, respectively.

Step 5. Alice and Bob orderly pick up a portion of their information, which is denoted as bit strings M_A and M_B, respectively. Later, Alice encrypts M_A with K_A by using an exclusive-OR operation to obtain C_A. Meanwhile, Bob encrypts M_B with K_B by using the same operation to obtain C_B. In order to reduce the transmission cost, Alice and Bob may also collaborate together to compute the exclusive-OR result C of C_A and C_B, and then send the result of C to TP via a public channel.

Step 6. TP transforms those Bell states (S_A, S_B) in Step 1, for the particles that have been received by Alice and Bob, into a classical bit string C_T by their initial states in Step 1. Here, i represents the ith particle of S_A and S_B, and the ith bit of C_T.

Step 7. After extracting C_T, TP computes the exclusive-OR result R_C of C and C_T. If there is a bit '1' in R_C, then TP terminates the protocol, and publishes '1' indicating that Alice's and Bob's information are different. Otherwise, TP repeats the protocol from Step 1 to Step 7 until all parts of information have been completely compared, and then TP announces that the two parties' information are identical.

2.2 Cryptanalysis of the QPC protocol with Bell states

Now we analyze the above protocol. Obviously in the first three steps the role of TP is to distribute EPR pairs to two players, i.e., Alice and Bob, and check eavesdropping in the quantum channels between TP and Alice, and between TP and Bob by adopting decoy photon techniques respectively. If there is no eavesdropper, then in Step 4 Alice and Bob can obtain their respective one-time-pad key K_A and K_B by using Z basis to measure the photons in S_A and S_B, respectively. Note that in Step 4 the aim of Alice and Bob's doing so is to expect to obtain a "one-time-pad" key K_A and K_B respectively so that the randomness of K_A and K_B can ensure the privacy of their secret information, i.e., M_A and M_B. However, are K_A and K_B true one-time-pad? The matter is not so simple because of TP's little trick. Instead of preparing EPR pairs, TP prepares two sets of polarized single photons randomly in photon states: $|0\rangle, |1\rangle$. In Step 5 Alice(Bob) encrypts $M_A(M_B)$ with $K_A(K_B)$ by using an exclusive-OR operation to obtain $C_A(C_B)$. If Alice(Bob) sends the result $C_A(C_B)$ to TP via a public channel, TP recovers M_A and M_B very easily. Of course, if Alice and Bob collaborate together to compute the exclusive-OR result C of C_A and C_B, and then send the result of C to TP via a public channel in order to reduce the transmission cost, TP's little trick will be invalid because he only obtains the collective result of M_A and M_B, not M_A and M_B individually. Hence, there is a security loophole in the protocol in ref. [44].

To solve the security drawback, it is a key to check the validity of the EPR pairs in S_A and S_B. The security check of EPR entangled state can be completed with the following procedures. (1) Alice tells TP and Bob the sample particles that she has chosen at random, and Bob pick out the corresponding particles from S_B. (2) Bob randomly chooses the basis $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$ to measure the chosen particles. (3) Bob tells Alice the corresponding measurement basis (MBs) he has chosen for the particles. (4) Alice uses the same MBs as Bob to measure the corresponding particles. (5) TP first publicly announces the initial EPR entangled states, then Alice the second, and Bob the last publicly announces their measurement outcomes. When no eavesdropping exists, their outcomes should be completely correlated. If there is no eavesdropping or the probability for being eavesdropped is lower than a suitable threshold, the procedure of the protocol can go on.

This additional step of checking the validity of the EPR pairs in S_A and S_B has two functions: (i) it can check whether TP is honest; (ii) it can also check the security in the quantum lines between TP and Alice, between TP and Bob respectively. Therefore, the preparation of decoy photons for eavesdropping check can be omitted in the protocol.

3 Discussions and conclusions

Now let us make a simple comparison of previous QPC protocols with a semi-honest TP [43–48]. Different from the protocol in ref. [44], those in refs. [43,45–48] are secure against the TP, where the security is ensured by some additional steps: (i) either an additional step for verifying the true entanglement of the information carriers for private comparison; (ii) or some secret information shared by the two players of private comparison unknown to the TP. Therefore, although the assumption in refs. [43,45–48] is unreasonable, the additional security strategies ensure the security of the protocols. Now let us review the protocol in ref. [44], where the protocol security is ensured by so called one-time-pad key K_A and K_B. In fact, the randomness of so called one-time-pad key K_A and K_B is difficult to ensure unless the true entanglement of the EPR pairs is verified. However, Tseng et al. neglected the verification process. Under the assumption with a semi-honest TP in ref. [44] it is not a loophole. However we have showed that the assumption is unreasonable, so the QPC protocol in ref. [44] is insecure.

From a general view of point, any quantum cryptographic protocol is a special example of secure multi-party quantum computation protocols. Therefore the techniques used in quantum multiparty computation [70,71] may be exploited to propose QPC schemes where less than half of the participants are not required to play honestly during the private comparison phase. This thought shall build a bridge between quantum cryptographic protocols and quantum multiparty computation. How to utilize them comprehensively will be the further work.

In conclusion, we study the security of previous QPC protocols with a semi-honest TP from the viewpoint of secure multi-party computation. We show that in these protocols the assumption that a TP is semi-honest is unreasonable which directly causes the protocols to be invalid. The analysis process is described in detail and some discussions about the design of the QPC protocols are given.

Acknowledgments This work is supported by the National Natural Science Foundation of China (Grant Nos. 61170270, 61003290); The Specialized Research Fund for the Doctoral Program of Higher Education (Grant Nos. 20091103120014, 20090005110010); Beijing Natural Science Foundation (Grant Nos. 4122008, 1102004); the ISN open Foundation.

References

1. Bennett, C.H., Brassard, G.: Quantum cryptography: public-key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, pp. 175–179. IEEE, New York (1984)
2. Ekert, A.: Quantum cryptography based on Bell's theorem. Phys. Rev. Lett. **67**, 661–664 (1991)
3. Bennett, C.H.: Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. **68**, 3121–3124 (1992)
4. Boström, K., Felbinger, T.: Deterministic secure direct communication using entanglement. Phys. Rev. Lett. **89**, 187902 (2002)
5. 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)
6. Lin, S., Wen, Q.Y., Gao, F., Zhu, F.C.: Quantum secure direct communication with chi-type entangled states. Phys. Rev. A **78**, 064304 (2008)

7. Wang, T.-Y., Wen, Q.-Y., Zhu, F.-C.: Multiparty controlled quantum secure direct communication with phase encryption. Int. J. Quant. Inform. **9**(2), 801–807 (2011)
8. Yang, Y.-G., Wen, Q.-Y.: Threshold quantum secure direct communication without entanglement. Sci. Chin. Ser. G Phys. Astron. **51**(2), 176–183 (2008)
9. Cao, W.-F., Yang, Y.-G., Wen, Q.-Y.: Quantum secure direct communication with cluster states. Sci. Chin. Ser. G Phys. Astron. **53**(7), 1271–1275 (2010)
10. Hillery, M., Bužek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A **59**, 1829–1834 (1999)
11. Karlsson, A., Koashi, M., Imoto, N.: Quantum entanglement for secret sharing and secret splitting. Phys. Rev. A **59**, 162–168 (1999)
12. Guo, G.P., Guo, G.C.: Quantum secret sharing without entanglement. Phys. Lett. A **310**, 247–251 (2003)
13. Zhang, Z.J., Man, Z.X.: Multiparty quantum secret sharing of classical messages based on entanglement swapping. Phys. Rev. A **72**, 022303 (2005)
14. Lin, S., Wen, Q.Y., Qin, S.J.: Multiparty quantum secret sharing with collective eavesdropping-check. Opt. Commun. **282**, 4455–4459 (2009)
15. Wang, T.Y., Wen, Q.Y., Gao, F., Lin, S., Zhu, F.C.: Cryptanalysis and improvement of multiparty quantum secret sharing schemes. Phys. Lett. A **373**, 65–68 (2008)
16. Li, B.-K., Yang, Y.-G., Wen, Q.-Y.: Threshold quantum secret sharing of secure direct communication. Chin. Phys. Lett. **26**(1), 010302 (2009)
17. Yang, Y.-G., Wang, Y., Chai, H.-P., Teng, Y.-W., Zhang, H.: Member expansion in quantum (t,n) threshold secret sharing schemes. Opt. Commun. **284**(13), 3479–3482 (2011)
18. Yang, Y.-G., Wang, Y., Teng, Y.-W., Wen, Q.-Y.: Universal three-party quantum secret sharing against collective noise. Commun. Theor. Phys. **55**(4), 589–593 (2011)
19. Yang, Y.-G., Chai, H.-P., Wang, Y., Teng, Y.-W., Wen, Q.-Y.: Fault tolerant quantum secret sharing against collective-amplitude-damping noise. Sci. Chin. Ser. G Phys. Astron. **54**(9), 1619–1624 (2011)
20. Yang, Y.-G., Teng, Y.-W., Chai, H.-P., Wen, Q.-Y.: Verifiable quantum (k,n)-threshold secret key sharing. Int. J. Theor. Phys. **50**(3), 792–798 (2011)
21. Yang, Y.-G., Teng, Y.-W., Chai, H.-P., Wen, Q.-Y.: Fault tolerant quantum secret sharing against collective noise. Phys. Scr. **83**(2), 025003 (2011)
22. Yang, Y.-G., Wen, Q.-Y.: Comment on: "Efficient high-capacity quantum secret sharing with two-photon entanglement". Phys. Lett. A **373**(3), 396–398 [Phys. Lett. A **372**, 1957 (2008)] (2009)
23. Yang, Y.-G., Wen, Q.-Y.: Threshold multiparty quantum-information splitting via quantum channel encryption. Int. J. Quantum Inf. **7**(6), 1249–1254 (2009)
24. Sun, Y., Wen, Q.Y., Zhu, F.C.: Improving the multiparty quantum secret sharing over two collective-noise channels against insider attack. Opt. Commun. **283**, 181–183 (2010)
25. Lin, S., Wen, Q.Y., Gao, F., Qin, S.J.: Improving the security of multiparty quantum secret sharing based on the improved Bostrom-Felbinger protocol. Opt. Commun. **281**, 4553–4554 (2008)
26. Qin, S.J., Gao, F., Wen, Q.Y., Zhu, F.C.: A special attack on the multiparty quantum secret sharing of secure direct communication using single photons. Opt. Commun. **281**, 5472–5474 (2008)
27. Sun, Y., Wen, Q.Y., Gao, F.: Multiparty quantum secret sharing based on Bell measurement. Opt. Commun. **282**, 3647–3651 (2009)
28. Dušek, M., Haderka, O., Hendrych, M.: Quantum identification system. Phys. Rev. A **60**, 149–156 (1999)
29. Curty, M., Santos, D.J.: Quantum authentication of classical messages. Phys. Rev. A **64**, 062309 (2001)
30. Ljunggren, D., Bourennane, M., Karlsson, A.: Authority-based user authentication in quantum key distribution. Phys. Rev. A **62**, 022305 (2000)
31. 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)
32. Yang, Y.-G., Wen, Q.-Y.: Arbitrated quantum signature of classical messages against collective amplitude damping noise. Opt. Commun. **283**(16), 3198–3201 (2010)
33. Yang, Y.-G., Wang, Y., Wen, Q.-Y.: Scalable arbitrated quantum signature of classical messages with multi-signers. Commun. Theor. Phys. (Beijing, China) **54**(1), 84–88 (2010)
34. Yang, Y.-G., Wen, Q.-Y.: Economical multiparty simultaneous quantum identity authentication based on Greenberger-Horne-Zeilinger states. Chin. Phys. B **18**(8), 3233–3236 (2009)
35. Yang, Y.-G., Teng, Y.W., Chai, H.P., Wen, Q.-Y.: Verifiable quantum (k,n)-threshold secret key sharing. Int. J. Theor. Phys. **50**(3), 792–798 (2011)
36. Yang, Y.-G., Jia, X., Wang, H. Y., Zhang, H.: Verifiable quantum (k, n)-threshold secret sharing. Quantum Inf. Process. (2012). doi:10.1007/s11128-011-0323-1

37. Abadi, M., Feigenbaum, J.: A simple protocol for secure circuit evaluation. LNCS **294**, 264–272 (1987)
38. Yao, A.C.: Protocols for secure computations. In: Proceedings of 23rd IEEE Symposium on Foundations of Computer Science (FOCS' 82), p. 160. Washington, DC, USA (1982)
39. Boudot, F., Schoenmakers, B., Traor'e, J.: A fair and efficient solution to the socialist millionaires' problem. Discr. Appl. Math. (Special Issue on Coding and Cryptology) **111**(1–2), 23–36 (2001)
40. Lo, H.K.: Insecurity of quantum secure computations. Phys. Rev. A **56**(2), 1154–1162 (1997)
41. 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**(5), 055305 (2009)
42. Yang, Y.G., Cao, W.F., Wen, Q.Y.: Secure quantum private comparison. Phys. Scr. **80**(6), 065002 (2009)
43. 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)
44. Tseng, H.-Y., Lin, J., Hwang, T.: New quantum private comparison protocol using EPR pairs. Quantum Inf. Process. **11**(2), 373–384 (2012)
45. 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)
46. Liu, W., Wang, Y.B., Tao, J.Z., Cao, Y.Z.: A protocol for the quantum private comparison of equality with χ-type state. Int. J. Theor. Phys. **51**, 69–77 (2012)
47. 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)
48. 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)
49. Jia, H.Y., Wen, Q.Y., Song, T.T., Gao, F.: Quantum protocol for millionaire problem. Opt. Commun. **284**, 545–549 (2011)
50. 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)
51. Zhang, Y.S., Li, C.F., Guo, G.C.: Comment on "Quantum key distribution without alternative measurements". Phys. Rev. A **63**, 036301 [Phys. Rev. A **61**, 052312 (2000)] (2001)
52. Gao, F., Qin, S., Wen, Q., Zhu, F.: A simple participant attack on the Bradler-Dusek protocol. Quantum Inf. Comput. **7**, 329–334 (2007)
53. Gao, F., Wen, Q., Zhu, F.: Teleportation attack on the QSDC protocol with a random basis and order. Chin. Phys. B **17**, 3189–3193 (2008)
54. Gao, F., Qin, S., Guo, F., Wen, Q.: Dense-Coding Attack on Three-Party Quantum Key Distribution Protocols. IEEE J. Quantum Electron. **47**, 630–635 (2011)
55. 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)
56. Qin, S., Gao, F., Wen, Q., Zhu, F.: Improving the security of multiparty quantum secret sharing against an attack with a fake signal. Phys. Lett. A **357**, 101–103 (2006)
57. Wójcik, A.: Eavesdropping on the "Ping-Pong" quantum communication protocol. Phys. Rev. Lett. **90**, 157901 (2003)
58. Wójcik, A.: Comment on "Quantum dense key distribution". Phys. Rev. A **71**, 016301 (2005)
59. Cai, Q.Y.: The "Ping-Pong" protocol can be attacked without eavesdropping. Phys. Rev. Lett. **91**, 109801 (2003)
60. 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)
61. Gao, F., Wen, Q.Y., Zhu, F.C.: Comment on: "Quantum exam". Phys. Lett. A **360**, 748–750 [Phys. Lett. A **350** (2006) 174] (2007)
62. Gao, F., Lin, S., Wen, Q.Y., Zhu, F.: A special eavesdropping on one-sender versus N-receiver QSDC protocol. Chin. Phys. Lett. **25**, 1561–1563 (2008)
63. Gao, F., Qin, S., Wen, Q., Zhu, F.: Cryptanalysis of multiparty controlled quantum secure direct communication using Greenberger-Horne-Zeilinger state. Opt. Commun. **283**, 192–195 (2010)
64. Yang, Y.-G., Naseri, M., Wen, Q.-Y.: Improved secure quantum sealed-bid auction. Opt. Commun. **282**(20), 4167–4170 (2009)
65. 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 [Quantum Inf. Process. **8**, 347 (2009)] (2011)

66. Gisin, N., Fasel, S., Kraus, B., Zbinden, H., Ribordy, G.: Trojan-horse attacks on quantum-key-distribution systems. Phys. Rev. A **73**, 022320 (2006)
67. 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)
68. Yang, Y.-G., Chai, H.-P., Teng, Y.-W., Wen, Q.-Y.: Improving the security of controlled quantum secure direct communication by using four particle cluster states against an attack with fake entangled particles. Int. J. Theor. Phys. **50**, 395–400 (2011)
69. Gao, F., Qin, S.-J., Guo, F.Z., Wen, Q.-Y.: Cryptanalysis of quantum secure direct communication and authentication scheme via Bell states. Chin. Phys. Lett. **28**, 020303 (2011)
70. Crépeau, C., Gottesman, D., Smith, A.: Secure multi-party quantum computation. In: Proceedings of the 34th Annual ACM Symposium on Theory of Computing, pp. 643–652. ACM, New York (2002)
71. Ben-Or, M., Crépeau, C., Gottesman, D., Hassidim, A., Smith, A.: Secure multiparty quantum computation with (only) a strict honest majority. In: Proceedings of 47th Annual IEEE Symposium on the Foundations of Computer Science, pp. 249–260. IEEE, Los Alamitos (2006)