Int J Theor Phys (2013) 52:2818–2825
DOI 10.1007/s10773-013-1573-8

Fault-Tolerate Quantum Private Comparison Based on GHZ States and ECC

Yan-Bing Li · Tian-Yin Wang · Hui-Yan Chen · Meng-Dong Li · Ya-Tao Yang

Received: 17 January 2013 / Accepted: 15 March 2013 / Published online: 2 April 2013

Abstract There are some quantum private comparison (QPC) schemes proposed previously. In this paper we study these QPC protocols in non-ideal scenario and find that they are not secure there. For resolving the problem, we propose a QPC scheme which could be performed in practical scenario. By the use of Greenberger-Horne-Zeilinger (GHZ) states and error-correcting code (ECC), the scheme has the capability of fault-tolerate.

Keywords Quantum private comparison · Fault-tolerate · GHZ state · Error-correcting code

1 Introduction

With the development of quantum mechanics, quantum cryptography attracts more and more attention, and many secure protocols have been designed for quantum key distribution (QKD) [1–7], quantum secret sharing (QSS) [8–15], quantum secure direct communication (QSDC) [16–19], quantum teleportation (QT) [20–24], and so on. Secure multiparty computation (SMPC) [25, 26] is an important and fundamental cryptographic protocol. Unfortunately, it was shown by Mayers [27] and Lo-Chau [28] that deterministic two-party-setting computation was impossible, even with quantum means. However, if some additional assumptions are introduced, the quantum secure multiparty computation (QSMPC) maybe have higher security than classical SMPC.

Y.-B. Li (✉)
State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China
e-mail: liyanbing1981@gmail.com

Y.-B. Li · H.-Y. Chen · M.-D. Li · Y.-T. Yang
Beijing Electronic Science and Technology Institute, Beijing 100070, China

T.-Y. Wang
School of Mathematical Science, Luoyang Normal University, Luoyang 471022, China

Recently, the quantum private comparison (QPC) became a novel topic in quantum cryptography. To be specific, QPC allows two distrustful parties, Alice and Bob, to determine whether their secret inputs are equal or not without disclosing their own secret to each other. In 2009, QPC was proposed by Yang et al. [29, 30]. After these, some QPC protocols based on different states are proposed [31–38]. Summarily, the QPC schemes presented previously have the following principles.

(1) A Third Party (TP) which is at least semi-honest is required to help the two parties (Alice and Bob) accomplish the comparison. And TP always follows the procedure of the protocol. He/she will take a record of all intermediate computations, and will not be corrupted by an outside eavesdropper. However, TP might try to steal the information from the record.
(2) No matter whether TP will know the positions of different bit value in the compared information or not, he/she will not be able to know the actual bit value of the information.
(3) All outsiders and the two players should only know the result of the comparison (i.e., identical or different), but not the different positions of the information.

These schemes are feasible in the ideal scenario. However, in this paper, we will point that these schemes would not be secure in practical scenario where fault (including noise and error) is existent in the quantum channel and measurement. And we design a new QPC scheme based on Greenberger-Horne-Zeilinger (GHZ) states and error-correcting code (ECC) against noise.

The rest of this paper is constructed as follows. Section 2 analyzes the previously QPC schemes' security in practical scenario. Then a new QPC scheme based on GHZ states and ECC is proposed in Sect. 3. In Sect. 4, we analyzes the protocol's security and the capability of fault-tolerate. Finally, a short conclusion is given in Sect. 5.

2 Analysis of Some QPC Schemes' Security in Practical Scenario

In all the QPC schemes proposed previously, there are two participants, Alice and Bob, and a semi-honest third party, Calvin. Alice has a private information X, Bob has a private information Y. The binary representations of X and Y in F_{2^n} are $(x_0, x_1, \dots, x_{n-1})$, $(y_0, y_1, \dots, y_{n-1})$, where $x_i, y_i \in \{0, 1\}$; $X = \sum_{i=0}^{n-1} x_i \cdot 2^i$, $Y = \sum_{i=0}^{n-1} y_i \cdot 2^i$.

These QPC schemes could be divided into two families, one is based on sharing states, one is based on travelling photons. For simpleness, we give the processes that they compare two bits x_i and y_i. In the first family, without loss of generality, the main steps which removes the steps of detecting cheating could be described as

(1) Calvin, Alice and Bob (or only Alice and Bob) share a entangled state.
(2) After measurements, they have three bits, s_C, s_A and s_B respectively (or only Alice and Bob have two bits, s_A and s_B respectively), where the value of $k = s_C \oplus s_A \oplus s_B$ is known to Calvin (or the value of $k = s_A \oplus s_B$ is known to all of Calvin, Alice and Bob).
(3) Then Alice and Bob announce the values of $s_A \oplus x_i$ and $s_B \oplus y_i$ publicly (or in private) to Calvin.
(4) Calvin could judge whether $x_i = y_i$ or not by comparing $s_A \oplus s_B$ and $(s_A \oplus x_i) \oplus (s_B \oplus y_i)$.

In the second family, without loss of generality, the main steps removes the steps of detecting cheating could be described as

(1) Calvin prepares a photon S and sends it to Alice.

(2) Alice performs an unitary operator I or U_1 on S when $x_i = 0$ or 1, where $\langle s|(U_1|s\rangle) = 0$, $U_1(U_1|s\rangle) = |s\rangle$ and $|s\rangle$ is arbitrary one in all the possible states of photon S. Then she sends S to Bob.
(3) Bob performs an unitary operator I or U_1 on S when $y_i = 0$ or 1. Then he sends S to Calvin.
(4) Calvin measures S in its initial basis. Then he could judge $x_i = y_i$ if the state are not changed, $x_i \neq y_i$ if the state are changed.

Now we analyze them in practical scenario. In the first family, there would be $s_C \oplus s_A \oplus s_B = k$ (or $s_A \oplus s_B = k$) in the ideal scenario. However, in practical scenario where fault (including noise and error) is existent in the quantum channel and measurement, it will be $s_C \oplus s_A \oplus s_B = k \oplus 1$ (or $s_A \oplus s_B = k \oplus 1$) with some probability. For instance, in Chen et al.'s scheme [31], the sharing entangled state $(|000\rangle + |111\rangle)/\sqrt{2}$ would evolve to $(|001\rangle + |110\rangle)/\sqrt{2}$ in practical noise quantum channel which will change the correlation of Calvin, Alice and Bob's measurement outcomes. In the case, Calvin will judge that $x_i = y_i$ (or $x_i \neq y_i$) but in fact $x_i \neq y_i$ (or $x_i = y_i$).

In the second family, the state of photon S does not change in the transmission, and measurement mistakes does not happen in the ideal scenario. However, when channel noise appears and measurement mistakes happens, the state $|s\rangle$ sent by one participant will evolve to $|s \perp\rangle$ with some probability when it arrives another participant, where $\langle s|s \perp\rangle = 0$. For instance, in Yang et al.'s scheme [30], the state $|0\rangle$ sent by Calvin (denoted as TP in Ref. [30]) would evolve to $|1\rangle$ when it arrives Alice (denoted as Bob in Ref. [30]). In the case, Calvin will judge that $x_i = y_i$ (or $x_i \neq y_i$) but in fact $x_i \neq y_i$ (or $x_i = y_i$).

Consequently, using the above schemes to compare two n bits private information X and Y, Calvin will output $X = Y$ (or $X \neq Y$) incorrectly but in fact $X \neq Y$ (or $X = Y$) with some probability.

From above, we conclude that QPC schemes are very sensitive of fault, special in the case of $X = Y$. There even one error bit appears in the quantum channel and measurement will lead an absolute incorrect result. In some other quantum protocols, such as QKD and QSS, some technologies, such as privacy amplification [39] have been added to overcome limited error. Similarly, some technologies should be added in QPC to overcome noise and error. Next, we will give an example to solve the problem.

3 QPC Based on Error-Correcting Code

It has been shown that when the rate of error is below a certain threshold, fault tolerant quantum information manipulation is possible by using some strategies, such as classical error-correcting code (ECC) [40], quantum error correction [41–43], and quantum error rejection [44]. Specially, ECC is a special form of QECC, and it is easier to implement than other QECC.

In this section, we will give a QPC scheme in the first QPC family based on GHZ states and ECC for fault-tolerate which is not achieved in the previously schemes. The specific steps of the scheme are described as follows.

1. Alice, Bob and Calvin prepare a $[m, n]$ error-correcting code which uses m bits codeword to encode n bits word and can correct l error bits in codeword with the error-correcting function $D(x^m)$ according to the fault rate of the noise scenario. We suppose the error-correcting code's generator matrix is G, check matrix is H. Then they

encode $X=(x_0,x_1,\dots,x_{N-1})$ and $Y=(y_0,y_1,\dots,y_{N-1})$ to $X'=(x'_0,x'_1,\dots,x'_{N-1})$ and $Y'=(y'_0,y'_1,\dots,y'_{m-1})$ with the generator matrix G, respectively. There are

$$X'=X\cdot G, \tag{1}$$

$$Y'=Y\cdot G. \tag{2}$$

2. Calvin prepares m triplet GHZ states all in

$$\begin{aligned}|\Psi\rangle &= \frac{1}{\sqrt{2}}\big(|000\rangle+|111\rangle\big)\\ &= \frac{1}{2}\big(|+++\rangle+|+--\rangle+|-+-\rangle+|--+\rangle\big),\end{aligned} \tag{3}$$

   where $|0\rangle$ and $|1\rangle$ are measured in Z basis, $|+\rangle$ and $|-\rangle$ are measured in X basis, and $|\pm\rangle=\frac{1}{\sqrt{2}}(|0\rangle\pm|1\rangle)$. Then Calvin divides these m GHZ states into three sequences S_A, S_B and S_C, which includes the first, the second, and the third particles of all GHZ states, respectively.
3. Calvin prepares some decoy photons prepared in states $\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$ in random. He inserts these decoy photons in S_A and S_B at random positions to form sequences S_A^* and S_B^* respectively. Then Calvin retains the quantum sequence S_C and sends the sequence S_A^* to Alice, S_B^* to Bob.
4. When Alice and Bob arrive S_A^* and S_B^*, Calvin announces the decoy photons' positions and measurement base. Then Alice and Bob measure them in the base and announce their outcome. If the error rate exceeds a rational threshold, Calvin aborts the protocol and restarts from Step 1. Otherwise, there is no eavesdropper, and the protocol continues to the next step.
5. Alice and Bob recover S_A and S_B respectively by discarding the decoy photons. Then Alice, Bob and Calvin measure S_A , S_B and S_C in X basis, respectively. If the measurement result is $|+\rangle$ ($|-\rangle$), then they encode it as the classical bit 0 (1). Thus, each of Alice, Bob and Calvin will obtain m bits from S_A, S_B and S_C, respectively. We denote each of them as k_i^A , k_i^B and k_i^C ($i=0,1,\dots,m-1$).
6. Alice and Bob calculate $x'_i=k_i^A\oplus x_i$ and $y'_i=k_i^B\oplus y_i$ respectively. They announce $X'=(x'_0,x'_1,\dots,x'_{m-1})$ and $Y'=(y'_0,y'_1,\dots,y'_{m-1})$ to Calvin.
7. Calvin calculates $c'_i=k_i^C\oplus x'_i\oplus y'_i$ to form m bits sequence $C'=(c'_0,c'_1,\dots,c'_{m-1})$.
8. Then Calvin uses the check matrix H to check whether the number of error bits exceeds the threshold l. If it does, Calvin aborts the protocol and restarts from Step 1. Otherwise, he arrives n bits sequence C by decoding C' with error-correcting function $D(C')$. If there is at least *one* bit 0 in C, Calvin announces $X\neq Y$. Otherwise, he announces $X=Y$.

4 Analysis

4.1 Correctness

In the scheme, the GHZ state $|\Psi\rangle$ will collapse to one of the states $\{|+++\rangle,|+--\rangle,|-+-\rangle,|--+\rangle\}$, therefore, there always have $k_i^A\oplus k_i^B\oplus k_i^C=0$. According to $x'_i=k_i^A\oplus x_i$, $y'_i=k_i^B\oplus y_i$ and $c'_i=k_i^C\oplus x'_i\oplus y'_i$, we know that $c'_i=x'_i\oplus y'_i$.

Based on Eqs. (1) and (2), there should be that

$$C'=C\cdot G, \tag{4}$$

where $C' = (x_0 \oplus y_0, x_1 \oplus y_1, \ldots, x_{n-1} \oplus y_{n-1})$. Namely, C' is the codeword of $C = (x_0 \oplus y_0, x_1 \oplus y_1, \ldots, x_{n-1} \oplus y_{n-1})$ decoded with the $[m, n]$ error-correcting code. Therefore, C' could be checked by the check matrix H, and C could be recoded with the error-correcting function $D(C')$.

If there is at least *one* bit 1 in C', it indicates that at least one set of (x_i, y_i) are different, i.e., $X \neq Y$. Otherwise, if all the bits are 0 in C', it indicates that all the sets of (x_i, y_i) are same, i.e., $X = Y$. So the presented scheme is correctness.

4.2 Security

In this sub-section, we will analyze the outsider attack and participant attack respectively.

4.2.1 Outsider Attack

After Alice and Bob received the quantum sequences S_A^* and S_B^* respectively, they and Calvin will start their public discussion to check for the existence of an eavesdropper. Calvin announces the positions and the measurement bases of all decoy photons. Later, both of Alice and Bob publish the measurement results. They can discuss the public results to determine whether an eavesdropper exists or not. Since the eavesdropper (say Eve) does not know the positions, and the measuring bases of all decoy photons before Calvin announces them, some well known attacks such as intercept-resend attack, measurement-resend attack, and entanglement-measure attack can be detected via the checking mechanism [29, 30]. For example, if Eve measures a X-basis decoy photon with Z basis, she will have a probability of $\frac{1}{2}$ to be detected. Obviously, Eve has a probability of $\frac{1}{2}$ to choose the wrong basis for measurement. Therefore, the detection rate for each decoy photon is $\frac{1}{2} \times \frac{1}{2} = \frac{1}{4}$. For t decoy photons, the detection rate is $1 - (\frac{3}{4})^t$, which is close to 1 if t is large enough. Furthermore, since no round-trip transmission strategy is used in the protocol, the Trojan horse attack can be automatically prevented. Therefore, the proposed protocol can resist all well known outsider attacks.

4.2.2 Participant Attack

In QPC, every participant has more resources than outsider. With these resources, a dishonest participant has more strategies to cheat besides the strategies which outsider can perform. So the term participant attack, which emphasizes that the attacks from dishonest users are generally more powerful and should be paid more attention to, is first proposed by Gao et al. in Ref. [45] and has attracted much attention in the cryptanalysis of quantum cryptography [46–52]. From the conclusions of QSMPC, we know that it should be insecure when less than a half of participants are honest [53–58]. Since QPC is a instance of QSMPC, it can only guarantee the secure when there is only one dishonest participant. So we will only analyze the attacks performed by Alice, Bob, and Calvin respectively, but not two colluded participants.

The first case discusses the possibility that a participant obtains the other participant's information. The second case discusses the possibility that the TP Calvin obtains Alice or Bob's private information.

Case 1 Alice and Bob want to learn the other's information.

Suppose Bob is a dishonest participant who attempts to obtain the other participant's (Alice's) information. One possible way for Bob is to use the photons (i.e., the second article of all GHZ states in S_B) sent to him.

When Alice and Calvin have not measured their photons, the reduced density operator of Bob's photon is

$$\rho_B = \mathrm{tr}_{AC}\left(\frac{|000\rangle + |111\rangle}{\sqrt{2}} \frac{\langle 000| + \langle 111|}{\sqrt{2}}\right) \\ = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{bmatrix}. \tag{5}$$

After Alice and Calvin's measurements in basis X , Bob's photons will collapse to $|+\rangle$ and $|-\rangle$ with probability 50 % respectively. If it collapses to $|+\rangle$, Alice and Calvin's measurement outcomes should be one of $\{|{+}{+}\rangle, |{+}{-}\rangle, |{-}{+}\rangle, |{-}{-}\rangle\}$ with probability $1/4$. Namely, Alice's outcome should be $|+\rangle$ and $|-\rangle$ with equal probability. Consequently, Bob cannot obtain the information of k_i^A. In fact, he only can obtain the information of $k_i^A \oplus k_i^C$ by measuring his ith photon. Since k_i^C is hold by Calvin and cannot be known by Bob, Bob could know nothing about k_i^A. Therefore, he could not obtain x_i even he can decode the value of $x_i \oplus k_i^A$. Namely, he cannot get any information about Alice's private information.

Case 2 Calvin wants to learn the private information X, Y.

In the scheme, Calvin is a semi-honest TP. He always follows the processes of the scheme. Such as, he will prepare GHZ states as an honest party. He will take a record of all intermediate computations, and will not be corrupted by an outside eavesdropper. So he only can use his measurement outcome and the announcements of Alice and Bob to cheat.

Same to a dishonest Bob, Calvin only can obtain the information of $k_i^A \oplus k_i^B$ when he measures his ith photon. He only could obtain $x_i \oplus y_i$ (but not x_i or y_i) even he can decode the value of $k_i^A \oplus x_i$ and $k_i^B \oplus y_i$. Namely, he cannot get any information about Alice and Bob's private information.

4.3 The Capability of Fault-Tolerate

In the presented scheme, error-correcting code is used for correcting the fault appears both in practical quantum channel and measurement. Since error-correcting code's capability of error-correcting is limited, the protocol's capability of error-correcting is limited too. In the protocol, the total fault rate must be less than l/m, otherwise, it would lead to restart the scheme. Then Alice, Bob and Calvin must prepare another error-correcting code which has higher error-correcting capability to utilize in the scheme.

We must point out that there are some computer power needed for utilizing error-correcting code. In the scheme, the participants might have not enough computer power to utilize the $[m, n]$ error-correcting code when n is very large. For solving the problem, they can select a suitable value of n' to split the n private information to $[N/L]$ groups where $[N/L]$ is the maximal integer which is less than N/L, then fill up the last group with some 0. After this, they can arrive the comparison result by comparing every groups using the presented scheme until Calvin announce $X \neq Y$ at one group or announce $X = Y$ all the time.

5 Conclusion

In this paper, we point out that the previously QPC schemes are not secure in practical scenario where fault (including noise and error) is existent in the quantum channel and measurement. Then we propose a QPC scheme using GHZ states and error-correcting code. The analysis indicates that the scheme is secure and has the capability of fault-tolerate. In future, with the error-correcting code, we also can design other QPC schemes using other quantum resources in practical scenario.

Acknowledgements We are grateful to the anonymous reviewer for helpful comments. This work is supported by NSFC (Grant Nos. 61272057, 61202434, 61170270, 61100203, 61003286, 61121061, 61202317, and 61103210), NCET (Grant No. NCET-10-0260), Beijing Natural Science Foundation (Grant Nos. 4112040, 4122054), the Fundamental Research Funds for the Central Universities (Grant Nos. 2012RC0612, 2011YB01).

References

1. Bennett, C.H., Brassard, G.: Quantum cryptography: public-key distribution and coin tossing. In: Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing, Bangalore, India, p. 175. IEEE Press, New York (1984)
2. Bennett, C.H.: Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. **68**, 3121 (1992)
3. Wang, X.B.: Quantum key distribution with two-qubit quantum codes. Phys. Rev. Lett. **92**, 077902 (2004)
4. 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)
5. 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)
6. Tan, Y.G., Cai, Q.Y.: Practical decoy state quantum key distribution with finite resource. Eur. Phys. J. D **56**, 449 (2010)
7. Wei, T., Tsai, C.W., Hwang, T.: Comment on quantum key distribution and quantum authentication based on entangled state. Int. J. Theor. Phys. **50**, 2703–2707 (2011)
8. Karlsson, A., Koashi, M., Imoto, N.: Quantum entanglement for secret sharing and secret splitting. Phys. Rev. A **59**, 162 (1999)
9. Hillery, M., Bužek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A **59**, 1829 (1999)
10. Qin, S.J., Gao, F., Wen, Q.Y., Zhu, F.C.: Cryptanalysis of the Hillery-Buek-Berthiaume quantum secret-sharing protocol. Phys. Rev. A **76**, 062324 (2007)
11. 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 **65**, 373 (2008)
12. Guo, F.Z., Qin, S.J., Gao, F., Lin, S., Wen, Q.Y., Zhu, F.C.: Participant attack on a kind of MQSS schemes based on entanglement swapping. Eur. Phys. J. D **56**, 445 (2010)
13. Wang, T.Y., Wen, Q.Y.: Security of a kind of quantum secret sharing with single photons. Quantum Inf. Comput. **11**(5–6), 0434 (2011)
14. Hwang, T., Hwang, C.C., Yang, C.W., Li, C.M.: Revisiting Deng et al.'s multiparty quantum secret sharing protocol. Int. J. Theor. Phys. **50**, 2790–2798 (2011)
15. Shi, R., Huang, L.S., Yang, W., Zhong, H.: Efficient symmetric five-party quantum state sharing of an arbitrary m-qubit state. Int. J. Theor. Phys. **50**, 3329–3336 (2011)
16. Bostroem, K., Felbinger, T.: Deterministic secure direct communication using entanglement. Phys. Rev. Lett. **89**, 187902 (2002)
17. 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)
18. Lin, S., Wen, Q.Y., Gao, F., Zhu, F.C.: Quantum secure direct communication with χ-type entangled states. Phys. Rev. A **78**, 064304 (2008)
19. Tsai, C.W., Hsieh, C.R., Hwanga, T.: Dense coding using cluster states and its application on deterministic secure quantum communication. Eur. Phys. J. D **61**, 779 (2011)
20. 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)
21. Bouwmeester, D., Pan, J.W., Mattle, K., Eibl, M., Weinfurter, H., Zeilinger, A.: Experimental quantum teleportation. Nature (London) **390**, 575 (1997)
22. 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)
23. 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)
24. Cao, H.J., Wang, H.S., Li, P.F., Song, H.S.: Teleportation of a 3-dimensional GHZ state. Int. J. Theor. Phys. **51**, 1448–1452 (2012)
25. Yao, A.C.: Protocols for secure computation. In: Proceedings of the 23rd Annual IEEE Symposium on Foundations of Computer Science, p. 160. IEEE Comput. Soc., Washington (1982)
26. Goldreich, O., Micali, S., Wigderson, A.: How to play a mental game. In: Annual ACM Symposium on Theory of Computing, p. 218. ACM, New York (1987)

27. Mayers, D.: Unconditional secure quantum bit commitment is impossible. Phys. Rev. Lett. **78**, 3414 (1997)
28. Lo, H.K., Chau, H.F.: Is quantum bit commitment really possible? Phys. Rev. Lett. **78**, 3410 (1997)
29. 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)
30. Yang, Y.G., Cao, W.F., Wen, Q.Y.: Secure quantum private comparison. Phys. Scr. **80**, 065002 (2009)
31. 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)
32. 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 (2011)
33. 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 (2011)
34. Tseng, H.Y., Lin, J., Hwang, T.: New quantum private comparison protocol using EPR pairs. Quantum Inf. Process. **11**(2), 373 (2012)
35. 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**, 1187 (2012)
36. 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**, 110 (2012)
37. 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 (2012)
38. Liu, W., Wang, Y.B., Cui, W.: Quantum private comparison protocol based on bell entangled states. Commun. Theor. Phys. **57**, 583 (2012)
39. Deutsch, D., Ekert, A., Jozsa, R., Macchiavello, C., Popescu, S., Sanpera, A.: Phys. Rev. Lett. **77**(13), 2818–2821 (1996)
40. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. North-Holland, Amsterdam (1977)
41. Shor, P.W.: Scheme for reducing decoherence in quantum computer memory. Phys. Rev. A **52**, R2493 (1995)
42. Laflamme, R., Miquel, C., Paz, J.P., Zurek, W.H.: Perfect quantum error correcting code. Phys. Rev. Lett. **77**, 198 (1996)
43. Steane, A.M.: Error correcting codes in quantum theory. Phys. Rev. Lett. **77**, 793 (1996)
44. Wang, X.B.: Quantum error-rejection code with spontaneous parametric down-conversion. Phys. Rev. A **69**, 022320 (2004)
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)
46. Qin, S.J., Gao, F., Wen, Q.Y., Zhu, F.C.: Cryptanalysis of the Hillery-Buzek-Berthiaume quantum secret-sharing protocol. Phys. Rev. A **76**, 062324 (2007)
47. Gao, F., Wen, Q.Y., Zhu, F.C.: Comment on: "Quantum exam" [Phys. Lett. A 350 (2006) 174]. Phys. Lett. A **360**, 748 (2007)
48. Gao, F., Qin, S.J., Wen, Q.Y.: Cryptanalysis of multiparty controlled quantum secure direct communication using Greenberger-Horne-Zeilinger state. Opt. Commun. **283**, 192 (2010)
49. 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)
50. Song, T.T., Zhang, J., Gao, F., Wen, Q.Y., Zhu, F.C.: Participant attack on quantum secret sharing based on entanglement swapping. Chin. Phys. B **18**, 1333 (2009)
51. Guo, F.Z., Qin, S.J., Gao, F., Zhu, F.C.: Participant attack on a kind of MQSS schemes based on entanglement swapping. Eur. Phys. J. D **56**, 445 (2010)
52. Lin, S., Gao, F., Guo, F.Z., Zhu, F.C.: Comment on "Multiparty quantum secret sharing of classical messages based on entanglement swapping". Phys. Rev. A **76**, 036301 (2007)
53. Damgård, I., Nielsen, J.B.: Scalable and unconditionally secure multiparty computation. In: Lecture Notes in Computer Science, vol. 4622, pp. 572–590. Springer, Berlin (2007)
54. Anders, J., Browne, D.E.: Computational power of correlations. Phys. Rev. Lett. **102**, 050502 (2009)
55. Loukopoulos, K., Browne, D.E.: Secure multiparty computation with a dishonest majority via quantum means. Phys. Rev. A **81**, 062336 (2010)
56. Li, Y.B., Wen, Q.Y., Qin, S.J.: Comment on secure multiparty computation with a dishonest majority via quantum means. Phys. Rev. A **84**, 016301 (2011)
57. Yang, Y.G., Zhou, Z., Teng, Y.W., Wen, Q.Y.: Arbitrated quantum signature with an untrusted arbitrator. Eur. Phys. J. D **61**, 773 (2011)
58. Li, Y.B., Wen, Q.Y., Qin, S.J.: Improved secure multiparty computation with a dishonest majority via quantum means. Int. J. Theor. Phys. **52**, 199 (2013)