Front. Phys. 10, 100303 (2015)
DOI 10.1007/s11467-015-0460-6

RESEARCH ARTICLE

# Twice-Hadamard-CNOT attack on Li *et al.*'s fault-tolerant quantum private comparison and the improved scheme

**Sai Ji** (季赛)[1,2], **Fang Wang** (王芳)[2], **Wen-Jie Liu** (刘文杰)[1,2,†], **Xiao-Min Yuan** (袁晓敏)[2]

[1] *Jiangsu Engineering Center of Network Monitoring, Nanjing University of Information Science & Technology, Nanjing 210044, China*

[2] *School of Computer and Software, Nanjing University of Information Science & Technology, Nanjing 210044, China*

*Corresponding author. E-mail:* [†] *wenjiel@163.com*

*Received July 20, 2014; accepted October 10, 2014*

Recently, Li *et al.* presented a two-party quantum private comparison scheme using Greenberger–Horne–Zeilinger (GHZ) states and error-correcting code (ECC) [*Int. J. Theor. Phys.* 52, 2818 (2013)], claiming it is fault-tolerant and could be performed in a non-ideal scenario. However, there exists a fatal loophole in their private comparison scheme under a special attack, namely the twice-Hadamard-CNOT attack. Specifically, a malicious party may intercept the other party's particles and execute Hadamard operations on the intercepted particles as well as on his or her own particles. Then, the malicious party could sequentially perform a controlled-NOT (CNOT) operation between intercepted particles and the auxiliary particles, as well as between his or her own particles and the auxiliary particles prepared in advance. By measuring the auxiliary particles, the secret input will be revealed to the malicious party without being detected. For resisting this special attack, a feasible improved scheme is proposed by introducing a permutation operator before the third party (TP) sends the particle sequences to each participant.

**Keywords** quantum private comparison, GHZ state, twice-Hadamard-CNOT attack, improved scheme

**PACS numbers** 03.67.Dd, 03.67.Hk



## 1 Introduction

Since quantum mechanics was introduced into the cryptography field, quantum cryptography has attracted significantly more attention attention. Due to the characteristics of quantum unconditional security, many quantum cryptography protocols such as quantum key distribution (QKD) [1–3], quantum secure direct communication (QSDC) [4–10], quantum secret sharing (QSS) [11–13], and quantum teleportation (QT) [14, 15] have been proposed to solve various security problems. Some researchers have also studied protocols for continuous variable quantum communication [16, 17].

Recently, quantum private comparison (QPC) has become an important branch in quantum cryptography. Based on the properties of quantum mechanics, the participants can determine whether their secret inputs are equal without disclosing their own secrets to each other. In 2009, Yang *et al.* [18] presented a pioneering QPC scheme based on Bell states and a hash function. Since then, a large number of QPC protocols have been proposed utilizing entangled states such as Einstein–Podolsky–Rosen (EPR) pairs [18, 22, 24, 26, 27] and Greenberger–Horne–Zeilinger (GHZ) states [19, 21].

However, these QPC protocols [18–27] are feasible in the ideal scenario, but they are not secure in the practical scenario where faults (including noise and error) exist in the quantum channel and measurement. To solve this problem, in 2013, Li *et al.* [28] presented a novel QPC scheme based on GHZ states that used error-correcting code (ECC) against noise. However, through analyzing Li *et al.*'s QPC scheme, we found it is insecure under a special attack, called the twice-Hadamard-CNOT attack. To be specific, if any malicious party performed the twice-Hadamard-CNOT attack, he or she could obtain another party's secret input, which goes against the QPC principles [29]. Here, the twice-Hadamard-CNOT attack is essentially a special controlled-NOT (CNOT) operation used to attack the communication process. The CNOT operation has also been used in other attacks [30] and quantum repeaters [31]. To fix the loophole in Li *et*

*al.*'s QPC scheme, a simple solution is proposed that utilizes a permutation operator before the third party (TP) distributes the particles to the participants.

The remainder of this paper is organized as follows. Li *et al.*'s QPC protocol is briefly reviewed in Section 2. In Section 3, we analyze the security of Li *et al.*'s QPC protocol by introducing the twice-Hadamard-CNOT attack and an improved scheme in the QPC protocol is given in to fix the loophole in Section 4. Finally, our conclusions are summarized in Section 5.

## 2 Review of Li *et al.*'s QPC protocol

In Ref. [28], to guarantee the security of the QPC protocol in the practical scenario, Li *et al.* proposed a novel two-party QPC scheme using quantum ECC and the block transmission method [4]. The protocol consists of the following eight steps.

1) Alice, Bob, and Calvin prepare a $[m, n]$ ECC that uses a $m$ bit code word to encode an $n$ bit word. The ECC can correct $l$ error bits in the code word with the error-correcting function $D(x^m)$ according to the fault rate of the noise scenario. We suppose that the generator matrix of the ECC is $G$ and the check matrix is $Q$. Then, Alice, Bob, and Calvin encode $X = (x_0, x_1, \ldots, x_{n-1})$ and $Y = (y_0, y_1, \ldots, y_{n-1})$ to $X' = (x'_0, x'_1, \ldots, x'_{m-1})$ and $Y' = (y'_0, y'_1, \ldots, y'_{m-1})$, respectively, using the generator matrix $G$:

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

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

2) Calvin prepares $m$ triplet GHZ states that all have the state

$$|\psi\rangle_{CAB} = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{CAB} = \frac{1}{2}(|{+}{+}{+}\rangle + |{+}{-}{-}\rangle + |{-}{+}{-}\rangle + |{-}{-}{+}\rangle)_{CAB}, \tag{3}$$

where $|0\rangle$ and $|1\rangle$ are measured in the $Z$ basis, $|+\rangle$ and $|-\rangle$ are measured in the $X$ basis, and $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. Then, Calvin divides the GHZ states into three sequences, $S_A$, $S_B$, and $S_C$, which include the first, second, and third particles of all GHZ states, respectively.

3) Calvin randomly prepares decoy photons in states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. He inserts these decoy photons into $S_A$ and $S_B$ at random positions to form the sequences $S_A^*$ and $S_B^*$, respectively. Calvin retains the quantum sequence $S_C$ and sends the sequence $S_A^*$ to Alice and $S_B^*$ to Bob.

4) When Alice and Bob receive $S_A^*$ and $S_B^*$, respectively, Calvin announces the positions and measurement bases of the decoy photons. Alice and Bob measure decoy photons in the same base and announce their outcomes. If the error rate exceeds a rational threshold, Calvin aborts the protocol and restarts from Step i). 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 the result as the classical bit 0 (1). Thus, Alice, Bob, and Calvin will each obtain $m$ bits from $S_A$, $S_B$ and $S_C$, respectively. We denote the resulting $m$ bit strings as $k_i^A$, $k_i^B$, and $k_i^C$ $(i = 0, 1, \ldots, m-1)$.

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 $X'' = (x''_0, x''_1, \ldots, x''_{m-1})$ and $Y'' = (y''_0, y''_1, \ldots, y''_{m-1})$ to Calvin.

7) Calvin calculates $c'_i = k_i^C \oplus x''_i \oplus y''_i$ and finds the $m$ bit sequence $C' = (c'_0, c'_1, \ldots, c'_{m-1})$.

8) Then, Calvin uses the check matrix $Q$ to verify if the number of error bits exceeds the threshold $l$. If it does, Calvin aborts the protocol and restarts from Step 1). Otherwise, he obtains the $n$ bit sequence $C^*$ by decoding $C'$ with an error-correcting function $D(C')$. If there is at least one bit 1 in $C^*$, Calvin announces $X \neq Y$. Otherwise, he announces $X = Y$.

## 3 Twice-Hadamard-CNOT attack on Li *et al.*'s QPC protocol

As analyzed in Ref. [28], some well-known attacks such as the intercept-resend attack, measurement-resend attack, and entanglement-resend attack can be detected in Li *et al.*'s QPC protocol. However, we found it cannot resist a special attack, i.e., the twice-Hadamard-CNOT attack. To be specific, if either Alice or Bob performs the twice-Hadamard-CNOT attack, he or she can get the other party's secret input without being detected. The detailed procedure of the twice-Hadamard-CNOT attack is given as follows.

Without loss of generality, we suppose Bob is malicious and wants to get Alice's secret input. First, Bob prepares $m$ auxiliary particles all in the state $|0\rangle_e$. Then, the GHZ state and an auxiliary particle compose a composite system:

$$|\eta\rangle = |\psi\rangle_{CAB}|0\rangle_e = \frac{1}{\sqrt{2}}(|0000\rangle + |1110\rangle)_{CABe} = \frac{1}{2}(|{+}{+}{+}0\rangle + |{+}{-}{-}0\rangle + |{-}{+}{-}0\rangle + |{-}{-}{+}0\rangle)_{CABe}, \tag{4}$$

where the subscripts $C$, $A$, and $B$ represent the particles

in the hand of Calvin, Alice, and Bob, respectively, and the subscript $e$ represents an auxiliary particle.

In Step 3), when Calvin sends the sequence $S_A^*$ to Alice, Bob may intercept $S_A^*$ and execute a Hadamard ($H$) operation on every particle in $S_A^*$ to form sequence $S_A^{**}$. Then, Bob performs a CNOT operation $C_{Ae}$ on every particle in $S_A^{**}$ and the corresponding auxiliary particle $e$. Here, the particle in $S_A^{**}$ is the control qubit, while particle $e$ is the target qubit. After the CNOT operation, Bob performs another $H$ operation on every particle in $S_A^{**}$ to restore sequence $S_A^{**}$ to $S_A^*$ and sends $S_A^*$ to Alice. The transmitting sequence $S_A^*$ remains unchanged.

When Calvin announces the position of the decoy photons in Step 4), Bob can discard the auxiliary particles $e$ corresponding to the decoy photons in $S_A^*$. Then, in Step 5), after Bob recovers $S_B$ by discarding the decoy photons, he executes an $H$ operation on every particle in $S_B$ to form sequence $S_B^{**}$. Bob performs a CNOT operation $C_{Be}$ on every particle (control particle) in $S_B^{**}$ and the corresponding auxiliary particle $e$ (target particle). He then performs an $H$ operation on every auxiliary particle and on particle in $S_B^{**}$, which restores $S_B^{**}$ to $S_B$. Now, the state of the composite system is changed to

$$|\eta'\rangle = \frac{1}{2}(|++\rangle_{Ce}(|++\rangle + |--\rangle)_{AB} + |--\rangle_{Ce}(|+-\rangle + |-+\rangle)_{AB}). \quad (5)$$

From Eq. (5), the following rule can be deduced: if $e$ is $|+\rangle$, particle $A$ and particle $B$ are in the same state, and if $e$ is $|-\rangle$, particles $A$ and $B$ are in different states.

After Alice announces $X'' = (x_0'', x_1'', \ldots, x_{m-1}'')$ in Step 6), Bob measures $m$ auxiliary particles in the $X$ basis and obtains the measurement result $k_i^e (i = 0, 1, \ldots, m-1)$. According to $k_i^e$ and the rule from Eq. (5), Bob can obtain Alice's states $k_i^A (i = 0, 1, \ldots, m-1)$. Because $X'$ has been announced by Alice, Bob can calculate $x_i'' \oplus k_i^A = (k_i^A \oplus x_i') \oplus k_i^A = x_i'$, that is, he can find Alice's secret input $x_i'$.

The twice-Hadamard-CNOT attack can be intuitively demonstrated by Fig. 1.

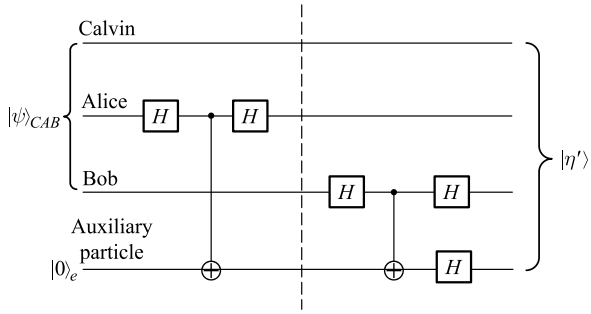


**Fig. 1** The circuit diagram of the process of twice-Hadamard-CNOT attack. Here, $|\psi\rangle_{CAB}$ is a GHZ state in the state $(|000\rangle + |111\rangle)/\sqrt{2}$ shared by Calvin, Alice and Bob. $H$ is Hadamard operation, and $\oplus$ represents the controlled-NOT gate where the top line denotes the control qubit, the bottom line the target qubit.

## 4 The improved scheme

To fix the loophole of Li *et al.*'s QPC protocol, we apply a permutation operator $\Pi$[1)] before TP sends the particle sequences to all participants. To be specific, Step 3), Step 4), and Step 5) in the original protocol need to be modified as follows.

3′) Calvin randomly prepares two groups of $r$-length decoy photons sequences in $\{|+\rangle, |-\rangle, |0\rangle, |1\rangle\}$, namely $R_A$ and $R_B$, and concatenates $R_A$ ($R_B$) with $S_A$ ($S_B$) to form the extended sequence $S_A' = R_A||S_A$ ($S_B' = R_B||S_B$). Then, Calvin applies a permutation operator $\Pi_{(r+m)}$ on $S_A'$ ($S_B'$) to create a new sequence $S_A^* = \Pi_{(r+m)}S_A'$ ($S_B^* = \Pi_{(r+m)}S_B'$) and sends the new sequence $S_A^*$ to Alice and $S_B^*$ to Bob.

4′) When Alice and Bob receive $S_A^*$ and $S_B^*$, Calvin announces the coordinates of the decoy qubits $\Pi_r S_A'$, $\Pi_r S_B'$ ($\Pi_r \subset \Pi_{r+m}$) sent to Alice and Bob and the corresponding measurement bases. Note that Calvin does not disclose the actual order of the message qubits. Then, Alice and Bob measure the decoy qubits in the same bases and announce their outcomes. 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 discard their decoy photons and denote the remaining qubits in their hands as $S_A''$ and $S_B''$ (i.e., $S_A'' = \Pi_m S_A$ and $S_B'' = \Pi_m S_B$), respectively. Then, Alice, Bob, and Calvin measure $S_A''$, $S_B''$, and $S_C$ in the $X$ basis, respectively, and obtain $m$ bits, $k_i^A$, $k_i^B$, and $k_i^C (i = 0, 1, \ldots, m-1)$, respectively. After they have completed the measurement operation, Calvin immediately announces the actual order of the message qubits $\Pi_m$ ($\Pi_m \subset \Pi_{r+m}$). Using this information, Alice (Bob) can rearrange $k_i^A$ ($k_i^B$) to correspond with the original order of $S_A$ ($S_B$).

As shown above, the key point is to add a permutation operator $\Pi$ in Li *et al.*'s QPC scheme. Thus, our improved protocol inherits the security properties of the original protocol, i.e., it can resist the intercept-resend attack, measurement-resend attack,

[1)] The permutation $\Pi$, also called the "arrangement number", is a rearrangement of the elements of an ordered sequence $S$ into a one-to-one correspondence with $S$ itself, $S \to S$. In this context, we will use $\Pi_{(r+m)}$ to represent the rearrangement (reordering) of the original sequence $S_A'$ or $S_A'$, and $\Pi_r$ represents the reordering operation only on the decoy qubits. For simplicity, we denote $\Pi_r \subset \Pi_{r+m}$ hereafter.

entanglement-resend attack, and some special inner attacks successfully discussed in Ref. [28]. Now, let us examine whether our improved scheme can resist the twice-Hadamard-CNOT attack. Similarly, we suppose the malicious Bob aims to find Alice's secret input. In Step 3′), since Calvin disrupts the sequences $S'_A$ and $S'_B$ using $\Pi_{(r+m)}$ to find $S^*_A$ and $S^*_B$, the orders of transmitted sequences $S^*_A$ and $S^*_B$ are fully disturbed. After discarding the decoy qubits $R_A$ and $R_B$ in Step 5′), Alice and Bob can only find $S''_A$ and $S''_B$ and cannot recover the original sequences $S_A$ and $S_B$ because $\Pi_m$ is only known by Calvin. Thus, even if Bob launch the twice-Hadamard-CNOT attack, he cannot find the final state $|\eta'\rangle = \frac{1}{2}(|{+}{+}\rangle_{Ce}(|{+}{+}\rangle+|{-}{-}\rangle)_{AB}+|{-}{-}\rangle_{Ce}(|{+}{-}\rangle+|{-}{+}\rangle)_{AB})$. That is to say, Bob cannot determine the correlations between Alice's and Bob's qubits by measuring the auxiliary particles $e$.

For simplicity, we take a simple two-bit private comparison as an example without considering ECC and the decoy photons. In this case, suppose Alice's input is 10, Bob's input is 11, and Calvin prepares two GHZ states all in the state given in Eq. (3),

$$\begin{aligned}|\psi\rangle_{C_1A_1B_1}\otimes|\psi\rangle_{C_2A_2B_2} &= 1/2(|{+}{+}{+}\rangle+|{+}{-}{-}\rangle\\ &+|{-}{+}{-}\rangle+|{-}{-}{+}\rangle)_{C_1A_1B_1}\\ &\otimes 1/2(|{+}{+}{+}\rangle+|{+}{-}{-}\rangle\\ &+|{-}{+}{-}\rangle+|{-}{-}{+}\rangle)_{C_2A_2B_2}. \end{aligned} \tag{6}$$

In Step 3′), Calvin executes the permutation operator $\Pi_{m=2}$ on sequence $S'_A$ and $S'_B$. Then, the system may be changed into

$$\begin{aligned}&\Pi_{m=2}(|\psi\rangle_{C_1A_1B_1}\otimes|\psi\rangle_{C_2A_2B_2})\\ &= |\psi\rangle_{C_1A_2B_2}\otimes|\psi\rangle_{C_2A_1B_1}\\ &= 1/4\{|{+}\rangle_{C_1}(|{+}{+}\rangle+|{-}{-}\rangle)_{A_2B_2}\\ &\quad\otimes|{+}\rangle_{C_2}(|{+}{+}\rangle+|{-}{-}\rangle)_{A_1B_1}\\ &\quad+|{+}\rangle_{C_1}(|{+}{-}\rangle+|{-}{+}\rangle)_{A_2B_2}\\ &\quad\otimes|{-}\rangle_{C_2}(|{+}{+}\rangle+|{-}{-}\rangle)_{A_1B_1}\\ &\quad+|{-}\rangle_{C_1}(|{+}{+}\rangle+|{-}{-}\rangle)_{A_2B_2}\\ &\quad\otimes|{+}\rangle_{C_2}(|{+}{-}\rangle+|{-}{+}\rangle)_{A_1B_1}\\ &\quad+|{-}\rangle_{C_1}(|{+}{-}\rangle+|{-}{+}\rangle)_{A_2B_2}\\ &\quad\otimes|{-}\rangle_{C_2}(|{+}{-}\rangle+|{-}{+}\rangle)_{A_1B_1}\}. \end{aligned} \tag{7}$$

After Bob performs the twice-Hadamard-CNOT attack, the composite system that consists of the GHZ state and the auxiliary particle becomes

$$\begin{aligned}|\eta'\rangle_1\otimes|\eta'\rangle_2 &= 1/4\{|{+}\rangle_{C_1}|{+}\rangle_{e_1}(|{+}{+}\rangle+|{-}{-}\rangle)_{A_2B_2}\\ &\otimes|{+}\rangle_{C_2}|{+}\rangle_{e_2}(|{+}{+}\rangle+|{-}{-}\rangle)_{A_1B_1}\\ &+|{+}\rangle_{C_1}|{-}\rangle_{e_1}(|{+}{-}\rangle+|{-}{+}\rangle)_{A_2B_2}\\ &\otimes|{+}\rangle_{C_2}|{-}\rangle_{e_2}(|{+}{-}\rangle+|{-}{+}\rangle)_{A_1B_1}\\ &+|{-}\rangle_{C_1}|{+}\rangle_{e_1}(|{+}{+}\rangle+|{-}{-}\rangle)_{A_2B_2}\\ &\otimes|{-}\rangle_{C_2}|{+}\rangle_{e_2}(|{+}{+}\rangle+|{-}{-}\rangle)_{A_1B_1}\\ &+|{-}\rangle_{C_1}|{-}\rangle_{e_1}(|{+}{-}\rangle+|{-}{+}\rangle)_{A_2B_2}\\ &\otimes|{-}\rangle_{C_2}|{-}\rangle_{e_2}(|{+}{-}\rangle+|{-}{+}\rangle)_{A_1B_1}\}. \end{aligned} \tag{8}$$

From the above equation, we cannot find the correlations between the states of $A_1$ and $B_1$ ($A_2$ and $B_2$) according to the final state of the auxiliary particle $e_1$ ($e_2$). Bob cannot steal Alice's input by measuring the auxiliary particles. Therefore, our improvement can resist the twice-Hadamard-CNOT attack.

## 5 Conclusion

In a secure QPC protocol, we must guarantee any participant only knows his or her own secret input without obtaining any other participant's secret input. In this paper, we reviewed and analyzed Li *et al.*'s two-party QPC protocol and found that it cannot resist the twice-Hadamard-CNOT attack, i.e., if one participant (Bob) launches this attack, he can get the other party's (Alice's) secret input without being detected. To avoid this loophole, we adopt a permutation operator to rearrange the quantum sequences sent to Alice and Bob from Calvin. Moreover, the analysis shows the security of our improved scheme can be guaranteed.

Although we showed that Li *et al.*'s protocol cannot resist the twice-Hadamard-CNOT attack, some other protocols [32, 33] also show weakness under this special attack. Many published quantum cryptography protocols have continually been identified as insecure. Perhaps one of the reasons for this insecurity is that we are used to applying the non-formalized analytical method (also called the attack-verification method) to verify the protocols, where some given attacks are listed to assault the present protocols. Obviously, this simple and crude analytical method has some shortcomings: (i) it lacks strictness because we cannot list all kinds of attacks, and (ii) even if a protocol can be proved to be secure against the known attacks, we cannot confirm that the protocol is flawless. Currently, formalism analysis and automated verification techniques have been extensively utilized for analyzing the security of the classic protocols and have demonstrated many achievements. It is possible that formalism analysis for quantum protocols will be the best choice to solve the above problems, and this is one direction of our future work.

**Acknowledgements** This work was supported by the National Natural Science Foundation of China (Grant Nos. 61103235,

61373131, and 61373016), the Priority Academic Program Development of Jiangsu Higher Education Institutions (PAPD), the Natural Science Foundation of Jiangsu Province under Grant No. BK20140651, and the Scientific Research Innovation Project for College Graduates of Jiangsu Province (Grant No. KYLX_0855).

## References

1. C. H. Bennett and G. Brassard, Quantum cryptography: Public-key distribution and coin tossing, In: *Proceedings of IEEE International conference on Computers, Systems and Signal Processing*, IEEE Press, New York, Bangalore, 1984, pp 175–179
2. A. K. Ekert, Quantum cryptography based on Bell's theorem, *Phys. Rev. Lett.* 67(6), 661 (1991)
3. L. M. Liang, S. H. Sun, M. S. Jiang, and C. Y. Li, Security analysis on some experimental quantum key distribution systems with imperfect optical and electrical devices, *Front. Phys.* 9(5), 613 (2014)
4. G. L. Long and X. S. Liu, Theoretically efficient high-capacity quantum-key distribution scheme, *Phys. Rev. A* 65(3), 032302 (2002)
5. F. G. Deng, G. L. Long, and X. S. Liu, Two-step quantum direct communication protocol using the Einstein–Podolsky–Rosen pair block, *Phys. Rev. A* 68(4), 042317 (2003)
6. F. G. Deng and G. L. Long, Secure direct communication with a quantum onetime pad, *Phys. Rev. A* 69(5), 052319 (2004)
7. G. L. Long, F. G. Deng, C. Wang, K. Wen, W. Y. Wang, and X. H. Li, Quantum secure direct communication and deterministic secure quantum communication, *Front. Phys. China* 2(3), 251 (2007)
8. W. J. Liu, H. W. Chen, Z. Q. Li, and Z. H. Liu, Efficient quantum secure direct communication with authentication, *Chin. Phys. Lett.* 25(7), 2354 (2008)
9. W. J. Liu, H. W. Chen, T. H. Ma, Z. Q. Li, Z. H. Liu, and W. B. Hu, An efficient deterministic secure quantum communication scheme based on cluster states and identity authentication, *Chinese Phys. B* 18(10), 4105 (2009)
10. Y. Chang, C. Xu, S. Zhang, and L. Yan, Controlled quantum secure direct communication and authentication protocol based on five-particle cluster state and quantum one-time pad, *Chin. Sci. Bull.* 59(21), 2541 (2014)
11. R. Cleve, D. Gottesman, and H. K. Lo, How to share a quantum secret, *Phys. Rev. Lett.* 83(3), 648 (1999)
12. M. Hillery, V. Bužek, A. Berthiaume, V. Bužek, and A. Berthiaume, Quantum secret sharing, *Phys. Rev. A* 59(3), 1829 (1999)
13. J. Xu, H. W. Chen, W. J. Liu, and Z. H. Liu, Selection of unitary operations in quantum secret sharing without entanglement, *Sci. China Inf. Sci.* 54(9), 1837 (2011)
14. D. Bouwmeester, J. W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, Experimental quantum teleportation, *Nature* 390(6660), 575 (1997)
15. A. Furusawa, J. L. Sorensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and E. S. Polzik, Unconditional quantum teleportation, *Science* 282(5389), 706 (1998)
16. A. Vidiella-Barranco and L. F. M. Borelli, Continuous variable quantum key distribution using polarized coherent states, *Int. J. Mod. Phys. B* 20, 1287 (2009)
17. C. D. Xie, J. Zhang, Q. Pan, X. J. Jia, and K. C. Peng, Continuous variable quantum communication with bright entangled optical beams, *Front. Phys. China* 1(4), 383 (2006)
18. Y. G. Yang and Q. Y. Wen, An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement, *J. Phys. A: Math. Theor.* 42(5), 055305 (2009)
19. X. B. Chen, G. Xu, X. X. Niu, Q. Y. Wen, and Y. X. Yang, 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 (2010)
20. H. Y. Jia, Q. Y. Wen, B. Y. Li, and F. Gao, Quantum private comparison using genuine four-particle entangled states, *Int. J. Theor. Phys.* 51(4), 1187 (2012)
21. W. Liu and Y. B. Wang, Quantum private comparison based on GHZ entangled states, *Int. J. Theor. Phys.* 51(11), 3596 (2012)
22. H. Y. Tseng, J. Lin, and T. Hwang, New quantum private comparison protocol using EPR pairs, *Quantum Inf. Process.* 11(2), 373 (2012)
23. W. Huang, Q. Y. Wen, B. Liu, F. Gao, and Y. Sun, Robust and efficient quantum private comparison of equality with collective detection over collective-noise channels, *Sci. China Phys. Mech.* 56(9), 1670 (2013)
24. W. J. Liu, C. Liu, Z. H. Liu, J. F. Liu, and H. T. Geng, Same initial states attack in Yang et al.'s quantum private comparison protocol and the improvement, *Int. J. Theor. Phys.* 53(1), 271 (2014)
25. W. J. Liu, C. Liu, H. W. Chen, Z. H. Liu, M. X. Yuan, and J. S. Lu, Improvement on "an efficient protocol for the quantum private comparison of equality with W state", *Int. J. Quantum Inf.* 12(01), 1450001 (2014)
26. J. Lin, C. W. Yang, and T. Hwang, Quantum private comparison of equality protocol without a third party, *Quantum Inf. Process.* 13(2), 239 (2014)
27. W. J. Liu, C. Liu, H. W. Chen, Z. Q. Li, and Z. H. Liu, Cryptanalysis and improvement of quantum private comparison protocol based on Bell entangled states, *Commun. Theor. Phys.* 62(2), 210 (2014)
28. Y. B. Li, T. Y. Wang, H. Y. Chen, M. D. Li, and Y. T. Yang, Fault-tolerate quantum private comparison based on GHZ states and ECC, *Int. J. Theor. Phys.* 52(8), 2818 (2013)
29. W. J. Liu, C. Liu, H. B. Wang, and T. T. Jia, Quantum private comparison: A review, *IETE Tech. Rev.* 30(5), 439 (2013)
30. C. Y. Lin and T. Hwang, CNOT extraction attack on "quantum asymmetric cryptography with symmetric keys", *Sci. China Phys. Mech.* 57(5), 1001 (2014)

31. Z. Y. Tong, P. Liao, and L. M. Kuang, Quantum repeaters based on CNOT gate under decoherence, *Front. Phys. China* 2(4), 389 (2007)
32. J. Lin, H. Y. Tseng, and T. Hwang, Intercept-resend attacks on Chen et al.'s quantum private comparison protocol and the improvements, *Opt. Commun.* 284(9), 2412 (2011)
33. W. W. Zhang and K. J. Zhang, Cryptanalysis and improvement of the quantum private comparison protocol with semi-honest third party, *Quantum Inf. Process.* 12(5), 1981 (2013)