Quantum Inf Process (2013) 12:559–568
DOI 10.1007/s11128-012-0395-6

Quantum private comparison protocol with d-dimensional Bell states

Song Lin · Ying Sun · Xiao-Fen Liu · Zhi-Qiang Yao

Received: 13 August 2011 / Accepted: 13 March 2012 / Published online: 5 April 2012

Abstract In this paper, a quantum private comparison protocol with Bell states is proposed. In the protocol, two participants can determine the relationship between their secret inputs in size, with the assistance of a semi-trusted third party. The presented protocol can ensure fairness, correctness, and security. Meanwhile, all the particles undergo only a one-way trip, which improves the efficiency and security of the communication. Furthermore, only Bell states are exploited in the implementation of the protocol, and two participants are just required having the ability to perform single particle operations, which make the presented protocol more feasible in technique.

Keywords Quantum private comparison · Bell state

1 Introduction

In 1984, Bennett and Brassard [1] proposed the first quantum key distribution protocol (BB84), which can ensure two remote users share a common random key securely. After that, people have tried to utilize quantum mechanics principles to solve some

S. Lin
School of Mathematics and Computer Science, Fujian Normal University, Fuzhou 350007, China

Y. Sun
Beijing Electronic Science and Technology Institute, Beijing 100070, China

X.-F. Liu
Key Lab of Network Security and Cryptology, Fujian Normal University, Fuzhou 350007, China

Z.-Q. Yao (✉)
Faculty of Software, Fujian Normal University, Fuzhou 350007, China
e-mail: yzq@fjnu.edu.cn

security tasks, which are problematic or impossible in classical cryptography, and presented many interesting applications, such as quantum key distribution [2], quantum secret sharing [3–19], quantum secure direct communication [20–35], and so on. Recently, a new application, quantum private comparison (QPC) has been put forward and become a hot research topic in the field of quantum information [36–40].

In a general private comparison scenario, there are two participants, Alice and Bob, who possess two secret input numbers s_a and s_b respectively. They wish to know which is the larger of the two numbers in the condition that both of them learn no information about s_a or s_b other than $s_a > s_b$, $s_a < s_b$, or $s_a = s_b$. Since this problem was initially suggested by Yao in 1982, it is also named as Yao's Millionaires' problem [41]. The solution of this problem has wide applications in e-commerce and data mining, such as private bidding and auction, secret ballot election, et al. Hence, as the fundamental to secure multi-party computation (SMC), private comparison is important and well-studied in classical cryptography.

The quantum counterpart of it is QPC, which has been studied recently. It is a pity that a quantum two-party secure computation is impossible, which has been shown by Lo in Ref. [42]. However, this goal may be achieved if the additional assumptions are made, such as adding a third party. In 2009, Yang and Wen [36] proposed a QPC protocol with the help of a dishonest third party, in which decoy particles and EPR pairs are used. Later, an efficient protocol with GHZ states and single-particle measurement is presented [37]. Both of them are designed to compare the equality of the private information. In 2011, Jia et al. put forward a quantum protocol for millionaire problem with GHZ states [38], in which two parties can compute the relationship between s_a and s_b in size with the aid of a semi-honest third party.

In this paper, we propose a novel QPC protocol based on Bell states with a semi-trusted third party (STTP), who may misbehave on its own but will not conspire with either of two parties. In the presented protocol, a STTP, Trent, prepares two particles in a Bell state, and then distributes them to Alice and Bob respectively. According to their secrets, two participants perform the corresponding operations on their respective particles, and then measure the particles separately. Based on the measurement results, Trent announces a calculated result, in terms of which two participants can attain the comparison result simultaneously. Meanwhile, any party, include Trent, cannot deduce any other party's secret input. Hence, the presented protocol is fair and secure. Furthermore, in this protocol, all the particles do not be transmitted repeatedly, which greatly reduces the opportunity of the particles being intercepted, and thus improves the efficiency and security of communication. In addition, only preparation of Bell state and local unitary operations are required, which make this protocol more convenient from an applied point of view.

2 Quantum private comparison protocol

As a kind of important resource, Bell state has many interesting properties, which are widely used in the research of quantum information. In a d-dimensional Hilbert space C^d, according to two variables $u, v \in \{0, 1, \ldots, d-1\}$, one can write down any Bell state as

$$|\phi_{u,v}\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} e^{\frac{2\pi ijv}{d}} |j\rangle|j \oplus u\rangle, \tag{1}$$

where the symbol $\oplus$ ($\ominus$) denotes addition (subtraction) module d. In a quantum cryptography protocol, it is general to ensure that the receiving particles are indeed in a certain Bell state by measuring them separately in two orthonormal bases at random [2]. Here, two mutually unbiased orthogonal bases in C^d are utilized. One is the basis $MB_Z = \{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}$, and the other is $MB_F = \{F|0\rangle, F|1\rangle, \ldots, F|d-1\rangle\}$, where F is the d-th order discrete Fourier transform defined as follows

$$F|j\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} e^{\frac{2\pi ijk}{d}} |k\rangle\,, \;\; j = 0, 1, \ldots, d-1. \tag{2}$$

After performing $F \otimes F$ operation on the Bell state $|\phi_{u,v}\rangle$, two particles will be in a state

$$\begin{aligned} F \otimes F|\phi_{u,v}\rangle &= \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} e^{\frac{2\pi ijv}{d}} F|j\rangle \otimes F|j \oplus u\rangle \\ &= \frac{1}{\sqrt{d}} \sum_{k \oplus l = v} e^{\frac{2\pi iul}{d}} |k\rangle|l\rangle. \end{aligned} \tag{3}$$

Additionally, a set of unitary operations $X_t = \sum_{j=0}^{d-1} |j \oplus t\rangle\langle j|$ $(t = 1, 2, \ldots, d)$ are used to encode the secret message on particle.

In the presented protocol, a semi-trusted third party is required. In cryptography, a trusted third party (TTP), who is trusted by two parties, can facilitate the interactions between them. It is common for TTP in a number of commercial transactions and in cryptographic digital transactions as well as cryptographic protocols. As compared with TTP, a semi-trusted third party (STTP) is allowed to misbehave on its own but can not conspire with either of two parties.

Now, let us give an explicit description of the presented protocol. Here, Alice and Bob hold two secret inputs s_a and s_b respectively, where $s_a, s_b \in \{0, 1, \ldots, n\}$, $n > 2$, and $d = 2 * n + 1$. Two participants execute the following steps to complete private comparison task with the help of a STTP, Trent.

(1) Alice and Bob share a common secret key m ($m \in \{0, 1\}$) via a secure quantum key distribution protocol, such as BB84 protocol.

(2) Trent prepares a sequence of $\lambda = 1 + 2\delta$ ordered EPR pairs, $\{P_1^1, P_2^1, \ldots, P_1^\lambda, P_2^\lambda\}$. Here the subscripts 1 and 2 represent two different particles in one Bell state and the superscripts $1, 2, \ldots, \lambda$ indicate the entangled pair orders in the sequence. These entangled particle pairs are in the state $|\phi_{0,v_t}\rangle$, where $v_t \in \{0, 1, \ldots, d-1\}$ is chosen at random. Trent takes one particle from each entangled pair to form two ordered particle sequences, $S_1 : \{P_1^1, P_1^2, \ldots, P_1^\lambda\}$ and $S_2 : \{P_2^1, P_2^2, \ldots, P_2^\lambda\}$. In order to ensure the security of the particle transmission, the technique of decoy single particles [43–45] is utilized. That is, Trent inserts some decoy particles, which are randomly in one of the states $\{|0\rangle, |1\rangle, \ldots, |d-1\rangle, F|0\rangle, F|1\rangle, \ldots, F|d-1\rangle\}$, into the sequences S_1 and S_2,

and constructs the transmitting sequences, S_1' and S_2'. Then, he sends these two particle sequences to Alice and Bob respectively.

(3) After Alice receives the sequence S_1', she executes the first eavesdropping check process. Here, Alice requires Trent to tell her the positions and the initial states of all decoy particles. She takes the decoy particles out of the sequence and measures them in a suitable basis, Then, they can judge whether the channel between them is secure by comparing the initial states and the measurement results of these particles. If there is no eavesdropper, they continue the protocol; otherwise, they abort it.

(4) Bob performs the same eavesdropping check process as step (3), to ensure the security of the channel between him and Trent.

(5) For resisting Trent's malicious behavior, Alice and Bob execute the second eavesdropping check process. Here, Alice (Bob) chooses randomly δ particles from the sequence S_1 (S_2) as sample. Then, she(he) measures these sample particles in the basis $MB_Z = \{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}$ or $MB_F = \{F|0\rangle, F|1\rangle, \ldots, F|d-1\rangle\}$, which is chosen at random. She (he) requires Trent to declare the initial states of the sample particles, and then informs the other participant the positions of the sample particles and the measurement basis. Bob (Alice) measures the corresponding particles in the sequence $S_2(S_1)$ in the same basis. Finally, Alice and Bob present their measurement outcomes to check the quantum channels. If the error rate exceeds a predetermined threshold, Alice and Bob will discard these entangled particles and abort the protocol. Otherwise, they continue the protocol.

(6) In terms of the value of m, Alice and Bob perform respectively the corresponding unitary operations $X_{a_t}F \otimes X_{b_t}F$ on the remainder particles in their hands. If $m = 0,\ a_t = s_a$ and $b_t = s_b$; otherwise, $a_t = d \ominus 1 \ominus s_a$ and $b_t = d \ominus 1 \ominus s_b$. Then they measure these two particles in the basis MB_Z, and declare the measurement results, m_a and m_b, separately.

(7) According to the values of v_t, m_a, and m_b, Trent can calculate the equation $y_t = m_b \ominus v_t \ominus m_a$. Then, Trent gets the calculated result r_t by using the following equation,

$$r_t = \begin{cases} 0, & y_t = 0 \\ -1, & 0 < y_t \leq n \\ 1, & n < y_t \leq 2n-1 \end{cases}. \tag{4}$$

After that, he declares the value of r_t to Alice and Bob publicly.

(8) In terms of Trent's announcement and the value of m which is only known by Alice and Bob, they can attain the comparison result r_c at the same time.

$$r_c = f(s_a, s_b) = \begin{cases} s_a = s_b, & r_t * (-1)^m = 0 \\ s_a < s_b, & r_t * (-1)^m = -1 \\ s_a > s_b, & r_t * (-1)^m = 1 \end{cases} \tag{5}$$

An example is given for better understanding the presented protocol. Suppose that Alice's secret is 2 ($s_a = 2$), and Bob's is 3 ($s_b = 3$). Here, $n = 4,\ d = 9$, and $m = 1$. Furthermore, we can assume that the initial state of d-dimensional Bell state is $|\phi_{0,5}\rangle$, i.e. $v_t = 5$. After two eavesdropping check processes, according to the values of $m,\ s_a$

and s_b, Alice and Bob perform respectively the operations X^6F and X^5F on the particles in their hand. After that, the whole system is in the state $|\phi_{4,0}\rangle$. Without loss of generality, we can suppose that Alice's measurement result is $|2\rangle$, i.e. $m_a = 2$. Thus, Bob's measurement result is $m_b = 6$. Based on the equation , Trent gets the calculated result $r_t = 1$ and broadcasts it to Alice and Bob. According to the announcement of Trent, Alice and Bob obtain simultaneously the relationship between s_a and s_b in size, i.e. $s_a < s_b$.

From the above example, we can see that two participants are able to achieve a private comparison by the proposed protocol. Meanwhile, it is evident that correctness and fairness are satisfied. The security of this protocol will be discussed in the following section.

3 Security analysis

In this section, we analyze the security of this protocol and show that it is secure in theory. To see this in a sufficient way, we will consider three possible cases. The first is that there exists an outside attacker, Eve, who wants to eavesdrop the comparison result. The second case concerns a situation, in which one participant is malicious and tries to obtain the other's secret input. In addition, the third party, Trent, is semi-trusted, who may misbehave on it own but does not collude with Alice or Bob. Trent's attack is discussed in the third case.

3.1 Outside attack

In the protocol, the signal particles are operated in the site of three parties, except that they are transmitted in step (2). So, if Eve attempts to eavesdrop the comparison result, he has to perform some actions on the particles during the process of transmission between Trent and Alice (or Bob). However, the particles are transmitted in manner of quantum data block [46]. The first eavesdropping check in step (3) can defend this attack. In the sequences S_1' and S_2', there exist some decoy particles, the positions of which are just known by Trent. Because both the decoy particles and the signal particles are in maximally mixed state for Eve, he cannot distinguish the decoy particles from the signal particles. Moreover, each decoy particle is in one of the states $\{|0\rangle, |1\rangle, \ldots, |d-1\rangle, F|0\rangle, F|1\rangle, \ldots, F|d-1\rangle\}$. From Heisenberg uncertainty principle, we can get that it is impossible to determinate these states perfectly. Therefore, for any Eve's attack, it is inevitable to introduce errors in the first eavesdropping check, which is similar to BB84 protocol. Hence, the proposed protocol is robust against this kind of eavesdropping.

3.2 Participant attack

Next, let us focus on the attack of an inside participant. The attack from dishonest participant, which is generally more powerful, is first proposed by Gao et al. in [47] and has attracted much attention in the cryptanalysis of quantum cryptography [48–51]. In the presented protocol, the actions of two participants, Alice and Bob, are the same.

Without loss of generality, we can assume that Bob is malicious, who tries to eavesdrop Alice's secret input without being detected. It is obvious that Bob can perform his attack on the sequence S_1' in step (2). However, from the analysis in the previous subsection, we can see that any attack action will be detected by the first eavesdropping check process. Hence, all Bob's attack actions are restricted to the sequence S_2'. Nevertheless, after Alice encodes s_a on the particle in step (6), the whole system is in the state:

$$|\Phi\rangle = X_{a_t} F \otimes I |\phi_{0,v}\rangle_{AB} = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} e^{\frac{2\pi i j v}{d}} (X_{a_t} F |j\rangle) \otimes |j\rangle$$

$$= \frac{1}{d} \sum_{j=0}^{d-1} e^{\frac{2\pi i v j}{d}} \left(\sum_{k=0}^{d-1} e^{\frac{2\pi i j k}{d}} |k \oplus a_t\rangle \right)_A |j\rangle_B. \tag{6}$$

The reduced density operator for the particle B, $tr_A(|\Phi\rangle\langle\Phi|) = \frac{1}{d} \sum_{j=0}^{d-1} |j\rangle\langle j|$, is the identity matrix no matter what encoding operation Alice performed. It is clear that any measurement on the qudit B cannot reveal information about Alice's secret input s_a. Consequently, Bob cannot obtain any information about Alice's secret input without introducing errors in the protocol.

3.3 STTP's attack

Now, the case, in which Trent tries to eavesdrop the comparison result and the secret inputs, is discussed. In the protocol, Trent prepares the quantum carrier and takes part in the whole process of the protocol, which provides him more power to attack. However, since m is distributed between Alice and Bob via a secure QKD protocol, Trent isn't able to learn the value of m. That is, he cannot obtain the comparison result r_c. Thus, the goal of Trent's attack is how to eavesdrop the secret inputs of two participants without being detected. The general attack strategy of Trent is described as follows

In step (2), Trent prepares three particles in a certain state, and then sends respectively one particles to Alice and Bob according to the legal process. After two participants encodes their secret inputs in step (6), Trent utilizes the particle in his hand and the measurement results announced by two participants, m_a and m_b, to gain information about the secret inputs. Obviously, this attack cannot be detected in the first eavesdropping check. However, it will be shown later that Trent isn't able to achieve any information about the secret inputs on condition that no errors are to occur in the second eavesdropping check, even if he has the ability to cheat.

Without loss of generality, we can assume that three particles produced by Trent are in a state:

$$|\psi\rangle = \sum_{j,k=0}^{d-1} |j\rangle_A |k\rangle_B |\delta_{j,k}\rangle_T. \tag{7}$$

Then, Trent distributes the particles A and B to Alice and Bob respectively, and holds the particle T in his hand. In step (5), Alice and Bob execute the second eavesdropping check proceed. When two participants measure these two particles in the basis MB_Z, the following equation is derived in order not to introduce errors:

$$|\delta_{j,k}\rangle = \mathbf{0}, \text{ where } j \neq k. \tag{8}$$

So, the state $|\psi\rangle$ is in the form of

$$|\psi\rangle = \sum_{j=0}^{d-1} |j\rangle_A |j\rangle_B |\delta_{j,j}\rangle_T. \tag{9}$$

In the other case, the two qudits are measured in the basis MB_F separately. Suppose that the measurement results are $F|k\rangle_A$ and $F|l\rangle_B$, it can be deduced that the particle T is in the state $|\varphi_{k\oplus l}\rangle_T = \sum_{j=0}^{d-1} e^{\frac{2\pi j(k\oplus l)}{d}} |\delta_{j,j}\rangle$. Under this condition, Trent has to make a measurement on the particle T. In terms of the measurement result, he tries to announce a fake message to avoid introducing errors. Thus, the following restraint can be yielded:

$$\langle\varphi_x|\varphi_y\rangle = 0, \text{ where } |\varphi_x\rangle = \sum_{j=0}^{d-1} e^{\frac{2\pi jx}{d}} |\delta_{j,j}\rangle, \quad x \neq y. \tag{10}$$

In terms of Eq. 9, the whole system is in the state depicted as follows after the encoding operation performed by two participants in step (6),

$$|\Psi\rangle = X_{a_t} F \otimes X_{b_t} F \otimes I|\psi\rangle = \frac{1}{d} \sum_{k=0}^{d-1} \sum_{l=0}^{d-1} |\varphi_{k\oplus l}\rangle |k \oplus a_t\rangle |l \oplus b_t\rangle. \tag{11}$$

It can be deduced that the reduced density operator for the particle T is, $tr_{AB}(|\Psi\rangle\langle\Psi|) = \frac{1}{d} \sum_{k=0}^{d-1} |\delta_{k,k}\rangle\langle\delta_{k,k}|$. Meanwhile, from the Eq. (9), we can get the corresponding reduced density operator, $tr_{AB}(|\psi\rangle\langle\psi|) = \frac{1}{d} \sum_{j=0}^{d-1} |\delta_{j,j}\rangle\langle\delta_{j,j}|$, before two participants encodes the secret inputs on the particles A and B. Obviously, $tr_{AB}(|\Psi\rangle\langle\Psi|) = tr_{AB}(|\psi\rangle\langle\psi|)$, which implies that Trent will gain no information about the secret inputs from observing the particle T. That is, if Trent is to eavesdrop information about the secret inputs, he must invariably introduce errors in the second eavesdropping check. As a consequence, the presented protocol is secure against the attack of the STTP.

From the detailed security analysis of the proposed protocol depicted above, we can see that this protocol is secure against some common attacks. Hence, although a quantum two-party secure computation is impossible [42], a QPC with a semi-trusted third party may be achieved.

4 Discussion and summary

Before giving a conclusion, it is worthwhile to illustrate the differences between the presented protocol and related studies, which is described in Table 1. It is shown that the presented protocol has some distinct advantages. On the one hand, except that a common secret key is shared between two users beforehand, all the particles undergo only a one-way trip. Thus, the presented protocol greatly reduces the opportunity of

Table 1 Comparison of the presented protocol and previous protocols

	Ref. [33]	Ref. [35]	The presented protocol
Quantum resouce	Bell state	d-dimensional GHZ state	d-dimensional Bell state
Quantum measurement	Multi-particle measurement	Multi-particle measurement	Single-particle measurement
Object of the study	Equality	Relationship in size	Relationship in size
Need of hash function	Yes	No	No
Particle trip	Two-way	Two-way	One-way

the particles being intercepted relative to some two-way protocols, and improves the efficiency and security of communication. On the other hand, the implementation of the protocol only need exploit Bell states as quantum resource, and two participants are just required having the ability to perform single qudit operations, which make the presented protocol more feasible in technique.

In summary, we have proposed an efficient QPC based on Bell states. The presented protocol can determinate whether $s_a > s_b$, $s_a < s_b$, or $s_a = s_b$ for two secret input numbers s_a and s_b with the help of a semi-trusted third party, who prepares the quantum resource and records intermediate result. The security of the protocol with respect to different kinds of attack is analyzed, which shows that this protocol is secure. However, as said in Ref. [38], the use of a third party may be a weakest point of the protocols of this kind. Hence, how to enhance the robustness of it is still a problem. Moreover, the presented two-party private comparison protocol cannot be generalized to the case of multi-party directly. These problems are worth further studying. We will consider these problems in the future works.

Acknowledgments The author is grateful to the anonymous referees for their constructive and important suggestions. This work was supported by the National Natural Science Foundation of China (Grant Nos. 60903152, 61072080, 61102093, 61103210), Fujian Province Natural Science Foundation (Grant Nos. 2009J01274, 2010J05128, 2011J01339), the Foundation of Fujian Education Bureau (Grant No. JA11054), a Program for Innovative Research Team in Science and Technology in Fujian Province University, and a Key Project of Fujian Provincial Universities–Information Technology Research Based on Mathematics.

References

1. Bennett, C.H., Brassard, G.: Quantum cryptography: public-key distribution and coin tossing. In: Proceedings IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, pp. 175-C179. IEEE, New York (1984)
2. Gisin, N., Ribordy, G., Tittel, W., Zbinden, H.: Quantum cryptography. Rev. Mod. Phys. **74**, 145 (2002)
3. Hillery, M., Bužek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A **59**, 1829 (1999)
4. Karlsson, A., Koashi, M., Imoto, N.: Quantum entanglement for secret sharing and secret splitting. Phys. Rev. A **59**, 162 (1999)
5. Cleve, R., Gottesman, D., Lo, H.K.: How to share a quantum secret. Phys. Rev. Lett. **83**, 648 (1999)
6. Tittel, W., Zbinden, H., Gisin, N.: Experimental demonstration of quantum secret sharing. Phys. Rev. A **63**, 042301 (2001)
7. Guo, G.P., Guo, G.C.: Quantum secret sharing without entanglement. Phys. Lett. A **310**, 247 (2003)
8. Lance, A.M., Symul, T., Bowen, W.P., Sanders, B.C., Lam, P.K.: Tripartite quantum state sharing. Phys. Rev. Lett. **92**, 177903 (2004)

9. Xiao, L., Long, G.-L., Deng, F.-G., Pan, J.-W.: Efficient multiparty quantum-secret-sharing schemes. Phys. Rev. A **69**, 052307 (2004)
10. Deng, F.G., Li, X.H., Li, C.Y., Zhou, P., Zhou, H.-Y.: Multiparty quantum-state sharing of an arbitrary two-particle state with Einstein-Podolsky-Rosen pairs. Phys. Rev. A **72**, 044301 (2005)
11. Hsu, L.-Y., Li, C.-M.: Quantum secret sharing using product states. Phys. Rev. A **71**, 022321 (2005)
12. Yan, F.-L., Gao, T.: Quantum secret sharing between multiparty and multiparty without entanglement. Phys. Rev. A **72**, 012304 (2005)
13. 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)
14. Yu, I-C., Lin, F.-L., Huang, C.-Y.: Quantum secret sharing with multilevel mutually (un)biased bases. Phys. Rev. A **78**, 012344 (2008)
15. Muralidharan, S., Panigrahi, P.K.: Perfect teleportation, quantum-state sharing, and superdense coding through a genuinely entangled five-qubit state. Phys. Rev. A **77**, 032321 (2008)
16. Li, Q., Chan, W.H., Long, D.-Y.: Semiquantum secret sharing using entangled states. Phys. Rev. A **82**, 022303 (2010)
17. Li, Q., Long, D.Y., Chan, W.H., Qiu, D.W.: Sharing a quantum secret without a trusted party. Quantum Inf. Process. **10**, 97–106 (2011)
18. Shi, R.-H., Huang, L.-S., Yang, W., Zhong, H.: Multi-party quantum state sharing of an arbitrary two-qubit state with Bell states. Quantum Inf. Process. **10**, 231–239 (2011)
19. Nie, Y.-Y., Li, Y.-H., Liu, J.-C., Sang, M.-H.: Quantum state sharing of an arbitrary three-qubit state by using four sets of W-class states. Opt. Commun. **284**, 1457 (2011)
20. Boströem, K., Felbinger, T.: Deterministic secure direct communication using entanglement. Phys. Rev. Lett. **89**, 187902 (2002)
21. 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)
22. Deng, F.G., Long, G.L.: Secure direct communication with a quantum one-time pad. Phys. Rev. A **69**, 052319 (2004)
23. Cai, Q.Y., Li, B.W.: Improving the capacity of the Boström–Felbinger protocol. Phys. Rev. A **69**, 054301 (2004)
24. Wang, C., Deng, F.G., Li, Y.S., Liu, X.S., Long, G.L.: Quantum secure direct communication with high-dimension quantum superdense coding. Phys. Rev. A **71**, 044305 (2005)
25. Li, X.H., Deng, F.G., Zhou, H.Y.: Improving the security of secure direct communication based on the secret transmitting order. Phys. Rev. A **74**, 054302 (2006)
26. Lucamarini, M., Mancini, S.: Secure deterministic communication without entanglement. Phys. Rev. Lett. **94**, 140501 (2005)
27. Wang, C., Deng, F.G., Long, G.L.: Multi-step quantum secure direct communication using multi-particle Green-Horne-Zeilinger state. Opt. Commun. **253**, 15 (2005)
28. Zhu, A.D., Xia, Y., Fan, Q.B., Zhang, S.: Secure direct communication based on secret transmitting order of particles. Phys. Rev. A **73**, 022338 (2006)
29. Wang, J., Zhang, Q., Tang, C.J.: Multiparty controlled quantum secure direct communication using Greenberger-Horne-Zeilinger state. Opt. Commun. **266**, 732 (2006)
30. Jin, X.R., Ji, X., Zhang, Y.Q. et al.: Three-party quantum secure direct communication based on GHZ states. Phys. Lett. A **354**, 67 (2006)
31. 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)
32. Zhan, Y.-B., Zhang, L.-L., Zhang, Q.-Y.: Quantum secure direct communication by entangled qutrits and entanglement swapping. Opt. Commun. **282**, 4633 (2009)
33. Chamoli, A., Bhandari, C.M.: Secure direct communication based on ping-pong protocol. Quantum Inf. Process. **8**, 347–356 (2009)
34. Gao, F., Qin, S.-J., Wen, Q.-Y., Zhu, F.-C.: Cryptanalysis of multiparty controlled quantum secure direct communication using Greenberger-Horne-Zeilinger state. Opt. Commun. **283**, 192 (2010)
35. Xiu, X.-M., Dong, L., Gao, Y.-J.: Secure four-site distribution and quantum communication of X type entangled states. Opt. Commun. **284**, 2065 (2011)
36. 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)

37. 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)
38. Jia, H.-Y., Wen, Q.-Y., Song, T.-T., Gao, F.: Quantum protocol for millionaire problem. Opt. Commun. **284**, 545 (2011)
39. 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)
40. Liu, W., Wang, Y.-B., Jiang, Z.-T., Cao, Y.-Z.: A protocol for the quantum private comparison of equality with X-type state. Int. J. Theor. Phys. (online)
41. Yao A.C.: Protocols for secure computations. In: 23rd Annual Symposium on Foundations of Computer Science, pp. 160–162. IEEE Computer Society Press, Silver Spring (1982)
42. Lo, H.K.: Insecurity of quantum secure computations. Phys. Rev. A **56**, 1154 (1997)
43. Li, C.Y., Zhou, H.Y., Wang, Y., Deng, F.G.: Secure quantum key distribution network with bell states and local unitary operations. Chin. Phys. Lett. **22**, 1049–1052 (2005)
44. Li, C.Y., Li, X.H., Deng, F.G., Zhou, P., Liang, Y.J., Zhou, H.Y.: Efficient quantum cryptography network without entanglement and quantum memory. Chin. Phys. Lett. **23**, 2896–2899 (2006)
45. Li, X.H., Deng, F.G., Li, C.Y., Liang, Y.J., Zhou, P., Zhou, H.Y.: Deterministic secure quantum communication without maximally entangled states. J. Korean Phys. Soc. **49**, 1354 (2006)
46. Long, G.L., Liu, X.S.: Theoretically efficient high-capacity quantum-key-distribution scheme. Phys. Rev. A **65**, 032302 (2002)
47. 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)
48. 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)
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., 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)