Quantum Information Processing (2019) 18:186
https://doi.org/10.1007/s11128-019-2301-y

Cryptanalysis and improvement of dynamic quantum secret sharing protocol based on two-particle transform of Bell states

Gan Gao[1,4] · Chang-Cheng Wei[2] · Dong Wang[3]

Received: 24 October 2018 / Accepted: 25 April 2019 / Published online: 8 May 2019

Abstract
Recently, Du and Bao proposed a quantum secret sharing protocol based on two-particle transform of Bell states. We study the security of the proposed protocol and find that it is not secure, that is, the two dishonest agents, Bob and Zach, can collude to obtain Alice's secret messages without the help of the other agents. Finally, we give a possible improvement of the proposed protocol.

Keywords Security loophole · Entanglement swapping · Bell state comparison · Quantum secret sharing

1 Introduction

The cryptography is playing a significant role in the information society and can be classified into the classical cryptography and the quantum cryptography. The main difference between the two cryptography focuses on the protection of security. The security of classical cryptography depends on the computational complexity. However, this kind of computational complexity might be broken by the strong power of advanced algorithms. The security of quantum cryptography depends on the principles

✉ Gan Gao
gaogan0556@163.com

Chang-Cheng Wei
309107121@qq.com

1 Department of Electrical Engineering, Tongling University, Tongling 244000, China

2 Department of Mathematics and Computer Science, Tongling University, Tongling 244000, China

3 School of Physics and Material Science, Anhui University, Hefei 230601, China

4 Engineering Technology Research Center of Optoelectronic Technology Appliance, Tongling University, Tongling 244000, China

of quantum mechanics and can guarantee the unconditional security not only theoretically but also in an actual implementation. Thus far, many branches of quantum cryptography have been presented to offer various security properties, including quantum key distribution (QKD) [1–9], quantum secure direct communication (QSDC) [10–26], quantum secret sharing (QSS) [27–57], and so on. In the following, let us introduce the three listed branches one by one. QKD, which is the earliest and maturest branch, is a process in which two communication parties first generate a shared secret key by quantum states and then apply this key to encrypt and decrypt the secret messages. Since Bennett and Brassard [1] introduced the first QKD protocol with nonorthogonal single polarization states, all kinds of QKD protocols were put forward. For example, Deng and Long [2] proposed a two-step QKD protocol using practical faint laser pulses. Boyer et al. [3] proposed a QKD scheme in which one participant owns the quantum device and the other does not. Li et al. [4] proposed two QKD protocols over two different collective-noise channels. Gao [5] proposed a QKD protocol by swapping the entanglement of χ-type states. Lo et al. [7] proposed a measurement-device-independent QKD protocol, and so on. Different from QKD, QSDC is to directly transmit secret messages without first generating a key to encrypt them. In 2002, Long and Liu [10] proposed the first QSDC protocol using the concept of quantum data block. In 2004, Deng and Long [11] proposed a QSDC protocol using only a sequence of single photons. In 2005, Wang et al. [12] proposed a QSDC protocol with quantum superdense coding in high-dimensional Hilbert space. In 2007, Li et al. [15] proposed a QSDC protocol with quantum encryption by using pure entanglement states. In 2013, Ren et al. [22] proposed a robust QSDC protocol with the spatial-mode entanglement of two-photon systems, and so on. In general, there exist only two communication parties in QKD and QSDC. However, there are at least three communication parties in QSS. In 1999, Hillery, Buzěk and Berthiaume [27] used three-particle GHZ state and four-particle GHZ state to propose the first QSS protocol. In 2003, Bagherinezhad and Karimipour [28] utilized reusable GHZ states as secure carriers to propose a QSS protocol. In 2006, Deng et al. [32] proposed a circular QSS protocol in which the quantum information carrier, single photons or entangled particles can circularly run. In 2008, Markham et al. [36] gave a unified approach to secret sharing of both quantum and classical secrets using graph states. In 2012, Jia et al. [45] proposed two dynamic QSS protocols in which the change of the agent group is allowable during the procedure of sharing information. In 2017, Wang et al. [55] proposed a secure (k, n)-threshold QSS protocol based on local distinguishability of orthogonal multiqudit entangled states, and so on. By the way, the research about QSS focuses on the designs of not only novel protocols, but also attack strategies on some existing protocols. Sometimes, the improvements of original QSS protocols are incidentally given after proposing attack strategies. Notice that up to now, how to completely prove the security of QSS from the information theory is not solved, so to speak, this has become an open question.

Recently, Du and Bao [56] proposed a novel multiparty QSS protocol (hereafter called DB protocol). It is interesting that the DB protocol uses the two-particle transform of Bell states and has the functions of dynamic parameter update. However, it is somewhat a pity that there exists a security loophole in the DB protocol. That is, the

two dishonest agents, Bob and Zach, can collaborate to obtain Alice's secret messages without being detected.

2 Security loophole in the DB protocol

In order to clearly show the security loophole, firstly, let us review the five-party case of the DB protocol [56] as follows.

(1) Alice prepares k pairs of Bell states (i.e.,$|\varphi_1\rangle_{th}, \ldots, |\varphi_k\rangle_{th}$), where each pair is randomly in $\{|\phi^{\pm}\rangle_{th} = (|00\rangle_{th} \pm |11\rangle_{th})/\sqrt{2}, |\psi^{\pm}\rangle_{th} = (|01\rangle_{th} \pm |10\rangle_{th})/\sqrt{2}\}$. She takes out photons t and h of these Bell states to form T-sequence and H-sequence, respectively. Then, the T-sequence is sent to Bob.

(2) After receiving the T-sequence, firstly, Bob checks whether it is composed of single photons. Then, he performs the local unitary operation $U(\alpha_i) = \cos\alpha_i|0\rangle\langle 0| + \cos\alpha_i|1\rangle\langle 1| - \sin\alpha_i|1\rangle\langle 0| + \sin\alpha_i|0\rangle\langle 1|$ on photon t_i. Here, $i = 1, 2, \ldots, k$ and $\alpha_i \in \{0, \frac{2\pi}{3}, \frac{4\pi}{3}\}$. Lastly, Bob sends the $T^{(1)}$-sequence, which is transformed from the T-sequence, to Charlie.

(3) After Charlie receives the $T^{(1)}$-sequence, what he does is the same as what Bob does. Then Charlie sends the $T^{(2)}$-sequence, which is transformed from the $T^{(1)}$-sequence, to Green. What Green does is also the same as what Bob does. Then he sends the $T^{(3)}$-sequence, which is transformed from the $T^{(2)}$-sequence, to Zach. Zach also performs the local unitary operation $U(\alpha_i)$ on photon t_i of his receiving sequence and remains the $T^{(4)}$-sequence which is transformed from the $T^{(3)}$-sequence.

(4) Alice performs the four Pauli operations ($\sigma_{00} = |0\rangle\langle 0| + |1\rangle\langle 1|, \sigma_{01} = |0\rangle\langle 1| + |1\rangle\langle 0|, \sigma_{10} = |0\rangle\langle 0| - |1\rangle\langle 1|, \sigma_{11} = |0\rangle\langle 1| - |1\rangle\langle 0|$) on photons of the H-sequence to encode her secret M. Then she sends the $H^{(1)}$-sequence, which is transformed from the H-sequence, to Zach.

(5) After Zach receives the $H^{(1)}$-sequence, all the agents and Alice start to check eavesdropping. First, Alice randomly selects k_1 positions of the $T^{(4)}$-sequence and tells the selected positions to all the agents. Then, all the agents choose Green to collect the others' messages of operations on k_1 positions and to perform the reverse compound operations. Next, Green performs Bell-basis measurements on two corresponding photons in k_1 positions of both the $T^{(4)}$-sequence and the $H^{(1)}$-sequence and tells his measurement outcomes to Alice. In result, Alice can judge whether the eavesdropping exists or not. If no eavesdropping exists, Alice will announce all of the initial Bell states. So all the agents can collaborate to recover Alice's secret M.

We can see that, in the DB protocol, the local unitary operation performed by each agent is chosen from the phase shift operation set $S = \{U(0), U(2\pi/3), U(4\pi/3)\}$. Since the three operations cannot be exactly distinguished by measuring the different quantum states, Du and Bao stated that their QSS protocol was secure. However, this is not a fact. In what follows, we will prove that the above five-party case is not secure by designing a attack strategy on it. Our attack strategy, which is implemented by the two dishonest agents, Bob and Zach, is described as follows.

In advance, Bob and Zach prepare some Bell states, where each is $|\psi^+\rangle_{t'h'} = \frac{1}{\sqrt{2}}(|01\rangle_{t'h'} + |10\rangle_{t'h'})$. According to the forming-sequence manner in the above step (1), they also get the two sequences, T'-sequence and H'-sequence. Here, the T'-sequence is in Bob's hand and the H'-sequence is in Zach's hand. In the above step (2), after Bob receives the T-sequence from Alice, he does not perform any operations on it, but secretly sends it to Zach. In addition, he performs the local unitary operation $U(\alpha_i)$ on photon t'_i of the T'-sequence and sends the $T'^{(1)}$-sequence, which is transformed from the T'-sequence, to Charlie. At this moment, the $T^{(1)}$-sequence has been replaced with the $T'^{(1)}$-sequence, which is not known by Charlie, Green and Alice. After receiving the $T'^{(1)}$-sequence, Charlie performs the local unitary operation $U(\alpha_i)$ on it *as of old* and sends the $T'^{(2)}$-sequence, which is transformed from the $T'^{(1)}$-sequence, to Green. After Green receives the $T'^{(2)}$-sequence, what he needs to do is the same as what Charlie does. This means that Zach will receive the $T'^{(3)}$-sequence, which is transformed from the $T'^{(2)}$-sequence, from Green. After receiving the sequence, he also performs the local unitary operation $U(\alpha_i)$ on it. Now, Zach holds the three sequences: the $T'^{(4)}$-sequence (transformed from the $T'^{(3)}$-sequence), the H'-sequence and the T-sequence. As soon as Alice sends the $H^{(1)}$-sequence to him, he will hold all the sequences. When Alice announces k_1 positions of the $T^{(4)}$-sequence, Zach immediately performs Bell-basis measurements on two corresponding photons in k_1 positions of both the T-sequence and the H'-sequence. Obviously, there exists a process of swapping entanglement. Let us give an example to show this process. Suppose that Alice's unitary operation on photon $h_{k_1^j}$ (the subscript k_1^j denotes the jth in k_1 positions) and her initial Bell state are σ_{01} and $|\psi^-\rangle_{t_{k_1^j}h_{k_1^j}}$, respectively, and Bob's, Charlie's, Green's and Zach's local unitary operations on photon $t'_{k_1^j}$ are $U(2\pi/3), U(0), U(2\pi/3)$ and $U(4\pi/3)$, respectively. When Zach performs Bell-basis measurement on photons $t_{k_1^j}$ and $h'_{k_1^j}$, the system evolves as follows:

$$
\begin{aligned}
&(\sigma_{01}|\psi^-\rangle_{t_{k_1^j}h_{k_1^j}}) \otimes \left(U(4\pi/3)U(2\pi/3)U(0)U(2\pi/3)|\psi^+\rangle_{t'_{k_1^j}h'_{k_1^j}}\right) \\
&= \frac{1}{2}\Bigg(|\phi^+\rangle_{t_{k_1^j}h'_{k_1^j}} U(2\pi/3)|\psi^-\rangle_{t'_{k_1^j}h_{k_1^j}} \\
&\quad + |\phi^-\rangle_{t_{k_1^j}h'_{k_1^j}} U(2\pi/3)|\psi^+\rangle_{t'_{k_1^j}h_{k_1^j}} - |\psi^+\rangle_{t_{k_1^j}h'_{k_1^j}} U(2\pi/3)|\phi^-\rangle_{t'_{k_1^j}h_{k_1^j}} \\
&\quad - |\psi^-\rangle_{t_{k_1^j}h'_{k_1^j}} U(2\pi/3)|\phi^+\rangle_{t'_{k_1^j}h_{k_1^j}}\Bigg)
\end{aligned} \tag{1}
$$

According to Eq. (1), we see that Zach's Bell-basis measurement outcome is one of $|\phi^+\rangle_{t_{k_1^j}h'_{k_1^j}}$, $|\phi^-\rangle_{t_{k_1^j}h'_{k_1^j}}$, $|\psi^+\rangle_{t_{k_1^j}h'_{k_1^j}}$ and $|\psi^-\rangle_{t_{k_1^j}h'_{k_1^j}}$. After the process of swapping entanglement is over, Zach makes a comparison for his Bell-basis measurement outcome and $|\psi^-\rangle_{t'h'}$ and obtains a unitary operation. This kind of Bell state comparison method and its comparison steps can be consulted in the papers [5,6]. Then, Zach

performs the obtained unitary operation on photon $h_{k_1^j}$. At the same time, he performs Bell-basis measurements on two corresponding photons in $k - k_1$ positions of both the T-sequence and the $H^{(1)}$-sequence. Since Green is chosen to collect messages, to perform the reverse compound operations and to perform Bell-basis measurements in the above step (5), this indirectly means that Zach needs to send two sequences to him. Notice that, in order not to be detected, the two sequences sent by Zach should be the $T'^{(4)}$-sequence and the $H^{(1)}$-sequence. Here, we can't help asking why Bob's and Zach's replacing action is not detected. In the following, we will give the reason by continuing to use the above example. Suppose that Zach's Bell-basis measurement outcome is $|\psi^-\rangle_{t_{k_1^j} h'_{k_1^j}}$, and he compares $|\psi^-\rangle_{t_{k_1^j} h'_{k_1^j}}$ with $|\psi^+\rangle_{t'h'}$ to obtain σ_{10}. According to equation (1), photons $t'_{k_1^j}$ and $h_{k_1^j}$ are in $U(2\pi/3)|\phi^+\rangle_{t'_{k_1^j} h_{k_1^j}}$. When σ_{10} is performed on photon $h_{k_1^j}$, the system evolves as follows:

$$\sigma_{10} U(2\pi/3)|\phi^+\rangle_{t'_{k_1^j} h_{k_1^j}} = U(2\pi/3)|\phi^-\rangle_{t'_{k_1^j} h_{k_1^j}} \tag{2}$$

Now, let us see which state photons $t_{k_1^j}$ and $h_{k_1^j}$ are in if Bob and Zach don't perform the replacing action. When Bob's $U(2\pi/3)$, Charlie's $U(0)$, Green's $U(2\pi/3)$ and Zach's $U(4\pi/3)$ are performed on photon $t_{k_1^j}$ and Alice's σ_{01} are performed on photon $h_{k_1^j}$, the system evolves as follows:

$$\sigma_{01} U(4\pi/3) U(2\pi/3) U(0) U(2\pi/3)|\psi^-\rangle_{t_{k_1^j} h_{k_1^j}} = U(2\pi/3)|\phi^-\rangle_{t_{k_1^j} h_{k_1^j}} \tag{3}$$

That is, photons $t_{k_1^j}$ and $h_{k_1^j}$ are in $U(2\pi/3)|\phi^-\rangle_{t_{k_1^j} h_{k_1^j}}$. Obviously, the state of photons $t_{k_1^j}$ and $h_{k_1^j}$ is the same as that of photons $t'_{k_1^j}$ and $h_{k_1^j}$. Therefore, Bob's and Zach's replacing action cannot be detected, so that Alice thinks that the whole quantum channel is secure. Next, she announces all of the initial Bell states. As soon as Zach knows Alice's initial Bell states, plus the states that two corresponding photons in $k - k_1$ positions of both the T-sequence and the $H^{(1)}$-sequence are in, he easily infers Alice's unitary operation, that is, her secret M.

In order to resist the above attack that Bob and Zach implement, we will give an improvement of the DB protocol. Here, this improvement begins with the fourth step because steps (1′), (2′) and (3′) in it are same as the former three steps in the DB protocol. (4′) Alice randomly selects some photons from the H-sequence and randomly uses the basis $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}, |-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}\}$ to measure each selected photon. Then, Alice announces the positions of the selected photons in the H-sequence and asks Zach to send the partner photons of the selected photons in the $T^{(4)}$-sequence to her and all the agents to publish their local unitary operations in a random order. Next, Alice performs the reverse compound operations on the partner photons and then measures the partner photons with the same basis that are used when measuring the selected photons in the H-sequence. According to her measurement outcomes, Alice can judge whether the eavesdropping exists or not. If no eavesdropping exists,

Alice performs the four Pauli operations on photons of the H-sequence to encode her secret M and sends the $H^{(1)}$-sequence (transformed from the H-sequence) to Zach. (5′) This step is the same as step (5) in the DB protocol.

We see that another process to check the security is added in the improvement. This process is mainly used to prevent the two dishonest agents from eavesdropping, which had been shown in Wang et al.'s improving QSS protocol [34]. Of course, in the DB protocol, the attack from a dishonest agent is also discussed (please see Section 4.2.2 in the paper [56]), but Du and Bao only analyze a special inside attack implemented by one dishonest agent, which is called a single attack customarily. For the joint attack that is implemented by two dishonest agents, they do not discuss while analyzing the security. As we all know, the joint attack has stronger attack power than the single attack because more messages may be utilized while eavesdropping. At this moment, we cannot help asking that the added process to check the security is able to resist the joint attack? The answer is "yes." And the reason is given as follows.

Suppose that Bob and Zach also employ the above attack strategy to attack the improvement of the DB protocol. Since Alice uses the basis $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$ to make a single-qubit measurement for one Bell states in step (4′), the probability that Bob and Zach aren't detected after implementing the replacing action will be $\frac{1}{16}$. As the number of the selected Bell states increases, the probability tends to be 0. Therefore, the improvement can resist the above attack strategy. In addition, we also need to discuss whether the improvement can resist the entangle-measure attack strategy or not. Suppose that Bob and Zach beforehand prepare an auxiliary photon that is in $|\varepsilon\rangle$. When photon t is traveling, Bob and Zach perform an unitary operation U_E on it and the auxiliary photon. Without loss of generality, the system state of photons t, h and the auxiliary photon can be written as:

$$\begin{aligned} U_E|\varphi\rangle_{th}|\varepsilon\rangle &= |00\rangle_{th}|\varepsilon_{00}\rangle + |01\rangle_{th}|\varepsilon_{01}\rangle + |10\rangle_{th}|\varepsilon_{10}\rangle + |11\rangle_{th}|\varepsilon_{11}\rangle \\ &= \frac{1}{2}|+-\rangle_{th}(|\varepsilon_{00}\rangle - |\varepsilon_{01}\rangle + |\varepsilon_{10}\rangle - |\varepsilon_{11}\rangle) \\ &\quad + \frac{1}{2}|++\rangle_{th}(|\varepsilon_{00}\rangle + |\varepsilon_{01}\rangle + |\varepsilon_{10}\rangle + |\varepsilon_{11}\rangle) \\ &\quad + \frac{1}{2}|--\rangle_{th}(|\varepsilon_{00}\rangle + |\varepsilon_{01}\rangle + |\varepsilon_{10}\rangle + |\varepsilon_{11}\rangle) \\ &\quad + \frac{1}{2}|-+\rangle_{th}(|\varepsilon_{00}\rangle + |\varepsilon_{01}\rangle + |\varepsilon_{10}\rangle + |\varepsilon_{11}\rangle) \end{aligned} \tag{4}$$

Here, let us firstly suppose that $|\varphi\rangle_{th}$ that Alice prepares is $|\phi^-\rangle_{th}$ or $|\phi^+\rangle_{th}$. In step (4′) of the improvement, we can see that Alice uses the two sets of basis: $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$, to make a single-qubit measurement for the selected Bell states. If she chooses $\{|0\rangle, |1\rangle\}$ as the measurement basis, in order to avoid introducing error, the following must be satisfied:

$$|\varepsilon_{01}\rangle = |\varepsilon_{10}\rangle = \mathbf{0} \tag{5}$$

where $\mathbf{0}$ denotes a null vector. That is, the system states are:

$$U_E|\varphi\rangle_{th}|\varepsilon\rangle = |00\rangle_{th}|\varepsilon_{00}\rangle + |11\rangle_{th}|\varepsilon_{11}\rangle \tag{6}$$

On the other hand, if Alice chooses $\{|+\rangle, |-\rangle\}$ as the measurement basis, the following constraint can be similarly deduced:

$$|\varepsilon_{00}\rangle = |\varepsilon_{11}\rangle \tag{7}$$

By the way, if $|\varphi\rangle_{th}$ that Alice prepares is $|\psi^-\rangle_{th}$ or $|\psi^+\rangle_{th}$, the analysis is similar. Thus, $U_E|\varphi\rangle_{th}|\varepsilon\rangle = |\varphi\rangle_{th} \otimes |\varepsilon\rangle$, that is, $U_E|\varphi\rangle_{th}|\varepsilon\rangle$ is a product of a Bell state and a single qubit. This implies that Bob and Zach cannot gain any useful information from observing the auxiliary photon. In other words, if they want to eavesdrop on Alice's secret messages by using the entangle-measure attack strategy, their action must introduce errors.

3 Conclusion

In conclusion, we successfully show that, in the five-party case of the DB protocol, Bob and Zach can collude to obtain Alice's secret M without the help of the other agents; moreover, Bob's and Zach's eavesdropping action does not introduce any error. In other words, by designing a joint attack, the DB protocol is successfully proved to be insecure by us. In addition, in order to resist the joint attack, we make a modification for the DB protocol, that is, we give an improvement of the DB protocol. To the end, it is worth emphasizing that the above attack strategy is proposed by combining Bell state comparison and entanglement swapping, which is similar to that in the paper [42,48]. In addition, another attack strategy to combine Bell state comparison and quantum teleportation can also be seen in the papers [38,40]. So we hope that the application of Bell state comparison can be noticed in the future research on QSS.

Acknowledgements The author Gao thanks his parents for their encouragements. This work is supported by the 2014-year Program for Excellent Youth Talents in University of Anhui Province, the Talent Scientific Research Fundation of Tongling University under grant No. 2015tlxyrc01 and the top-notch talents cultivation project of Anhui Higher Education under grant No.gxyq2017081.

References

1. Bennett, C.H., Brassard, G.: In a Proceedings of the IEEE International Conference on Computers, Systems and Signal Processings, Bangalore, India, pp. 175–179. IEEE, New York (1984)
2. Deng, F.G., Long, G.L.: Bidirectional quantum key distribution protocol with practical faint laser pulses. Phys. Rev. A **70**, 012311 (2004)
3. Boyer, M., Kenigsberg, D., Mor, T.: Quantum key distribution with classical Bob. Phys. Rev. Lett. **99**, 140501 (2007)
4. Li, X.H., Deng, F.G., Zhou, H.Y.: Efficient quantum key distribution over a collective noise channel. Phys. Rev. A **78**, 022321 (2008)
5. Gao, G.: Quantum key distribution by comparing Bell states. Opt. Commun. **281**, 876 (2008)
6. Gao, G.: Quantum key distribution scheme with high efficiency. Commun. Theor. Phys. **51**, 820 (2009)
7. Lo, H.K., Curty, M., Qi, B.: Measurement-device-independent quantum key distribution. Phys. Rev. Lett. **108**, 130503 (2012)
8. Gong, L.H., Song, H.C., He, C.S., Liu, Y., Zhou, N.R.: A continuous variable quantum deterministic key distribution based on two-mode squeezed states. Phys. Scr. **89**, 035101 (2014)

9. Yang, X., et al.: Measurement-device-independent entanglement-based quantum key distribution. Phys. Rev. A **93**, 052303 (2016)
10. Long, G.L., Liu, X.X.: Theoretically efficient high-capacity quantum-key-distribution scheme. Phys. Rev. A **65**, 032302 (2002)
11. Deng, F.G., Long, G.L.: Secure direct communication with a quantum one-time pad. Phys. Rev. A **69**, 052319 (2004)
12. 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)
13. 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)
14. Lucamarini, M., Mancini, S.: Secure deterministic communication without entanglement. Phys. Rev. Lett. **94**, 140501 (2005)
15. Li, X.H., Li, C.Y., Deng, F.G., Zhou, P., Liang, Y.J., Zhou, H.Y.: Quantum secure direct communication with quantum encryption based on pure entangled states. Chin. Phys. **16**, 2149 (2007)
16. 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)
17. Wang, C., Xiao, L., Wang, W.Y., Zhang, G.Y., Long, G.L.: Quantum key distribution using polarization and frequency hyperentangled photons. J. Opt. Soc. Am. B. **26**, 2072 (2009)
18. Gao, G., Fang, M., Wang, Y., Zang, D.J.: A ping-pong quantum dialogue scheme using genuine four-particle entangled states. Int. J. Theor. Phys. **50**, 3089 (2011)
19. Wang, T.J., Li, T., Du, F.F., Deng, F.G.: High-capacity quantum secure direct communication based on quantum hyperdense coding with hyperentanglement. Chin. Phys. Lett. **28**, 040305 (2011)
20. Dong, L., Xiu, X.M., Gao, Y.J., Ren, Y.P., Liu, H.W.: Controlled three-party communication using GHZ-like state and imperfect Bell-state measurement. Opt. Commun. **284**, 905 (2011)
21. Kao, S.H., Hwang, T.: Cryptanalysis and improvement of controlled secure direct communication. Chin. Phys. B **22**, 060308 (2013)
22. Ren, B.C., Wei, H.R., Hua, M., Li, T., Deng, F.G.: Photonic spatial Bell-state analysis for robust quantum secure direct communication using quantum dot-cavity systems. Eur. Phys. J. D **67**, 30 (2013)
23. Gong, L.H., Liu, Y., Zhou, N.R.: Novel quantum virtual private network scheme for PON via quantum secure direct communication. Int. J. Theor. Phys. **52**, 3260 (2013)
24. Gao, G.: Bidirectional quantum secure communication based on one-dimensional four-particle cluster states. Int. J. Theor. Phys. **53**, 2282 (2014)
25. Ye, T.Y.: Robust quantum dialogue based on the entanglement swapping between any two logical Bell states and shared auxiliary logical Bell state. Quantum Inf. Process. **14**, 1469 (2015)
26. Zhang, W., et al.: Quantum secure direct communication with quantum memory. Phys. Rev. Lett. **118**, 220501 (2017)
27. Hillery, M., Buzk, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A **59**, 1829 (1999)
28. Bagherinezhad, S., Karimipour, V.: Quantum secret sharing based on reusable Greenberger–Horne–Zeilinger states as secure carriers. Phys. Rev. A **67**, 044302 (2003)
29. Yan, F.L., Gao, T.: Quantum secret sharing between multiparty and multiparty without entanglement. Phys. Rev. A **72**, 012304 (2005)
30. Deng, F.G., Li, X.H., et al.: Improving the security of multiparty quantum secret sharing against Trojan horse attack. Phys. Rev. A **72**, 044302 (2005)
31. Wang, H.F., et al.: Improving the security of multiparty quantum secret splitting and quantum state sharing. Phys. Lett. A **358**, 11 (2006)
32. Deng, F.G., et al.: Circular quantum secret sharing. J. Phys. A Math. Gen. **39**, 14089 (2006)
33. Xue, Z.Y., Yi, Y.M., Cao, Z.L.: Scheme for sharing classical information via tripartite entangled states. Chin. Phys. B **15**, 01421 (2006)
34. 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 (2008)
35. Guo, Y., Zeng, G.H., Chen, Z.G.: Multiparty quantum secret sharing of quantum states using entanglement states. Chin. Phys. Lett. **24**, 863 (2007)
36. Markham, D., Sanders, B.C.: Graph states for quantum secret sharing. Phys. Rev. A **78**, 042309 (2008)
37. Yang, Y.G., Wen, Q.Y.: Circular threshold quantum secret sharing. Chin. Phys. B **17**, 0419 (2008)
38. Gao, G.: Reexamining the security of the improved quantum secret sharing scheme. Opt. Commun. **282**, 4464 (2009)

39. Gao, G.: Multiparty quantum secret sharing using two-photon three-dimensional Bell states. Commun. Theor. Phys. **52**, 421 (2009)
40. Zhu, Z.C., Zhang, Y.Q.: Cryptanalysis and improvement of a quantum secret sharing protocol between multiparty and multiparty with single photons and unitary transformations. Chin. Phys. Lett. **27**, 060303 (2010)
41. Yang, Y.G., Cao, W.F., Wen, Q.Y.: Three-party quantum secret sharing of secure direct communication based on χ-type entangled states. Chin. Phys. B **19**, 050306 (2010)
42. Gao, G.: Cryptanalysis of multiparty quantum secret sharing with collective eavesdropping-check. Opt. Commun. **283**, 2997 (2010)
43. Yang, S., Chen, X.B., Yang, Y.X.: Attack on the enhanced multiparty quantum secret sharing. Commun. Theor. Phys. **58**, 51 (2012)
44. Chen, X.B., Yang, S., Su, Y., Yang, Y.X.: Cryptanalysis on the improved multiparty quantum secret sharing protocol based on the GHZ state. Phys. Scr. **86**, 055002 (2012)
45. Jia, H.Y., Wen, Q.Y., Gao, F., Qin, S.J., Guo, F.Z.: Dynamic quantum secret sharing. Phys. Lett. A **376**, 1035 (2012)
46. Zhu, Z.C., Zhang, Y.Q., Fu, A.M.: Cryptanalysis and improvement of a quantum secret sharing scheme based on χ-type entangled states. Chin. Phys. B **21**, 010307 (2012)
47. Zhu, Z.C., Hu, A.Q., Fu, A.M.: Cryptanalysis of a new circular quantum secret sharing protocol for remote agents. Quantum Inf. Process. **12**, 1173–1183 (2013)
48. Gao, G.: Secure multiparty quantum secret sharing with the collective eavesdropping-check character. Quantum Inf. Process. **12**, 55 (2013)
49. Chen, X.B., Niu, X.X., Zhou, X.J., Yang, Y.X.: Multi-party quantum secret sharing with the single-particle quantum state to encode the information. Quantum Inf. Process. **12**, 365 (2013)
50. Wang, M.M., Chen, X.B., Yang, Y.X.: Comment on High-dimensional deterministic multiparty quantum secret sharing without unitary operations. Quantum Inf. Process. **12**, 785–792 (2013)
51. Wang, M.M., Chen, X.B., Yang, Y.X.: Quantum secret sharing for general access structures based on multiparticle entanglements. Quantum Inf. Process. **13**, 429 (2014)
52. Wang, M.M., Wang, W., Chen, J.G., Farouk, A.: Secret sharing of a known arbitrary quantum state with noisy environment. Quantum Inf. Process. **14**, 4211 (2015)
53. Song, X.L., Liu, Y.B.: Cryptanalysis and improvement of verifiable quantum (k, n) secret sharing. Quantum Inf. Process. **15**, 851–868 (2016)
54. Lin, S., Guo, G.D., Xu, Y.Z., Sun, Y., Liu, X.F.: Cryptanalysis of quantum secret sharing with d-level single particles. Phys. Rev. A **93**, 062343 (2016)
55. Wang, J., Li, L., Peng, H., Yang, Y.: Quantum-secret-sharing scheme based on local distinguishability of orthogonal multiqudit entangled states. Phys. Rev. A **95**, 022320 (2017)
56. Du, Y.T., Bao, W.S.: Dynamic quantum secret sharing protocol based on two-particle transform of Bell states. Chin. Phys. B **27**, 080304 (2018)
57. Chen, X.B., Tang, X., Xu, G., Dou, Z., Chen, Y.L., Yang, Y.X.: Cryptanalysis of secret sharing with a single d-level quantum system. Quantum Inf. Process. **17**, 225 (2018)