Entropy **2015**, *17*, 6743-6752; doi:10.3390/e17106743

OPEN ACCESS

entropy

ISSN 1099-4300

www.mdpi.com/journal/entropy

Article

Quantum Secure Direct Communication Based on Dense Coding and Detecting Eavesdropping with Four-Particle Genuine Entangled State

Jian Li [1,2,3], Zeshi Pan [1,*], Fengqi Sun [1], Yanhua Chen [1], Zheng Wang [1] and Zuozhi Shi [1]

[1] School of Computer, Beijing University of Posts and Telecommunications, Beijing 100876, China; E-Mails: lijian@bupt.edu.cn (J.L.); sunfengqi@bupt.edu.cn (F.S.); yhchen2013@163.com (Y.C.); wangzheng@bupt.edu.cn (Z.W.); shizuozhi1992@163.com (Z.S.)

[2] Hefei National Laboratory for Physical Sciences at the Microscale, University of Science and Technology of China, Hefei 230026, China

[3] Science and Technology on Communication Security Laboratory, Sichuan 610041, China

* Author to whom correspondence should be addressed; E-Mail: abdrew001@163.com; Tel.: +86-10-6228-3259; Fax: +86-10-6228-3259.

Academic Editors: Demosthenes Ellinas, Giorgio Kaniadakis, Jiannis Pachos and Antonio M. Scarfone

Received: 27 March 2015 / Accepted: 19 August 2015 / Published: 30 September 2015

Abstract: A novel quantum secure direct communication protocol based on four-particle genuine entangled state and quantum dense coding is proposed. In this protocol, the four-particle genuine entangled state is used to detect eavesdroppers, and quantum dense coding is used to encode the message. Finally, the security of the proposed protocol is discussed. During the security analysis, the method of entropy theory is introduced, and two detection strategies are compared quantitatively by comparing the relationship between the maximal information that the eavesdroppers (Eve) can obtain, and the probability of being detected. Through the analysis we can state that our scheme is feasible and secure.

Keywords: quantum secure direct communication; four-particle genuine entangled state; eavesdropping detection; quantum dense coding

---

1. Introduction

Quantum cryptography has been a main field of research in quantum information over the past twenty years. It employs fundamental theories in quantum mechanics to obtain unconditional security. With the rapid development of information technology and quantum physics, quantum cryptography has achieved many significant results.

Researchers have put forward many protocols to continuously improve the safety and efficiency of communication. One of the most famous is the first quantum key distribution (QKD) protocol (BB84 protocol), which was proposed by Bennett and Brassard in 1984 [1]. QKD is an important research direction in quantum cryptography, which is used to share a secret key in communication between the sender (Alice) and the receiver (Bob), afterwards they transfer information by utilizing the generated keys to encode and decode.

Unlike QKD's need to distribute the key, a large number of protocols are used to transfer the secret information in the communication between the two sides directly, such as quantum secret sharing (QSS) [2–6], deterministic secure quantum communication (DSQC) [7–10], and quantum secure direct communication (QSDC) [11]. Since Alice and Bob will directly transfer effective information in the channel, the safety requirements of the protocol are higher than QKD. With the continuous study by researchers, there are many efficient QSDC protocols that have been presented in recent years, including protocols without using entanglement [12,13], and protocols using entanglement [14–17]. In addition, methods using two-way communication and quantum one-time pad are introduced to improve security [18–22].

In this paper, an improved quantum secure direct communication protocol, based on four-particle genuine entangled state (as shown in Equation (2)), is presented, aiming to improve communication security. In the protocol, the four-particle genuine entangled state is used to detect eavesdroppers, and quantum dense coding is used to encode the message. Finally, the security of the proposed protocol is discussed. We analyze the security of the protocol by comparing the relationship between the information that the eavesdroppers can obtain and the probability of being detected. The results showed that our scheme is feasible and secure.

For simplicity, we use the four-particle genuine entangled state protocol (FGEP) to represent the proposed protocol.

2. Description of Protocol

In many quantum secure direct communication protocols, the transmission is managed in batches of EPR pairs. An advantage of the block transmission scheme is that we can check the security of the transmission by measuring some of the decoy photons [23–26] in the first step, where Alice and Bob each hold a particle sequence, which means that if an eavesdropper has no access to the first particle sequence, then no information will be leaked to her whatever she has done to the second particle sequence. Following this method using block transmission, the FGEP scheme is proposed.

Suppose that the message to be transmitted from Alice to Bob is the sequence $x^N = (x_1, x_2, ..., x_N)$, where $x_i \in \{0,1\}$, $i = 1, 2, ..., N$.

(1) Bob prepares N pairs of Bell states $\left|\psi^{+}\right\rangle$ in order and inserts M pairs of four-particle genuine entangled states $\left|G_4\right\rangle$.

$$\left|\psi^{+}\right\rangle=\frac{\left|00\right\rangle+\left|11\right\rangle}{\sqrt{2}} \tag{1}$$

$$\left|G_4\right\rangle=\frac{1}{2\sqrt{2}}\left(\left|0000\right\rangle+\left|0011\right\rangle-\left|0101\right\rangle+\left|0110\right\rangle+\left|1001\right\rangle+\left|1010\right\rangle+\left|1100\right\rangle-\left|1111\right\rangle\right) \tag{2}$$

(i) Bob extracts all the first particles in these Bell states, and forms the sequence S_A (the travel qubits) in order. The sequence S_A is used to transmit a secure message. Then, the remaining particles in the Bell states form the sequence S_B (the home qubits) in order.

(ii) Bob forms a sequence S_G in order with the M pairs of four-particle genuine entangled states as decoy photons to detect eavesdropping. Note that the sequence S_G includes 4 × M qubits.

(iii) Bob inserts S_G to sequence S_A randomly, forms a new sequence S_A'. Only Bob knows the position of these decoy photons. Then Bob stores particles S_B and sends particles S_A' to Alice.

Figure 1 shows this process with concrete examples.

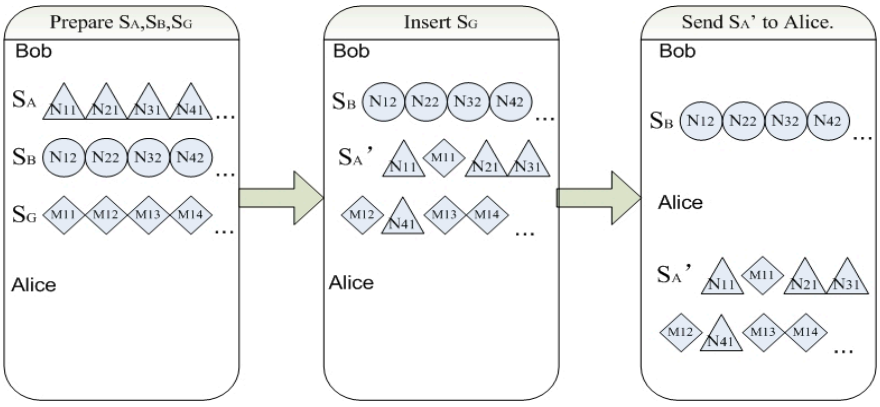

Figure 1. An example of Bob preparing S_A' and sending to Alice.

(2) The detection of eavesdropping.

After Alice receives sequence S_A', Bob tells her the position where the decoy photons are. Then, Alice extracts the decoy photons from sequence S_A' and performs four-particle genuine entangled state measurement. If there is no eavesdropper, her outcomes are all four-particle genuine entangled state, and they continue to execute the next step. Otherwise, the communication is interrupted, and the FGEP protocol switches to (1).

(3) Alice encodes her secure message on remaining photons based on dense coding.

Alice extracts all the decoy photons from sequence S_A' and the remaining particles form the series of particles S_E. According to the secure message she wants to transmit, Alice chooses one of the four unitary operations U_0, U_1, U_2 and U_3 for each of her particles to perform the unitary transformation on particles S_E from the series of S_E'. Here, U_0, U_1, U_2 and U_3 are Equations (3)–(6). Then, Alice sends the particles S_E' to Bob.

$$U_0 = I = |0\rangle\langle 0| + |1\rangle\langle 1| \tag{3}$$

$$U_1 = \sigma_Z = |0\rangle\langle 0| - |1\rangle\langle 1| \tag{4}$$

$$U_2 = \sigma_x = |1\rangle\langle 0| + |0\rangle\langle 1| \tag{5}$$

$$U_3 = i\sigma_y = |1\rangle\langle 0| - |0\rangle\langle 1| \tag{6}$$

(4) Bob decodes the cipher text with the Bell measurement.

After receiving Alice's particles, Bob performs the Bell measurement on both particles, S_E' and S_B. Then, he can acquire Alice's secure message.

(5) The FGEP protocol ends successfully.

3. The Security Analysis of the Protocol

Now, let us analyze the efficiency of the eavesdropping detection in the FGEP protocol. In order to gain the information that Alice encoded on the travel qubits, Eve, first, performs unitary attack operation $\hat{E}$ on the composed system. Then, Alice takes a coding operation on the travel qubits. Eve finally performs a measurement on the composed system. Since Eve does not know which particles are used to detect eavesdropping, she can only perform the same attack operation on all the particles. With respect to Eve, the state of the travel qubits is indistinguishable from the complete mixture, thus, all the travel qubits are considered in either of the states $|0\rangle$ or $|1\rangle$ with equal probabilities $p = 0.5$.

Generally speaking, after performing attack operation $\hat{E}$, the states $|0\rangle$ and $|1\rangle$ become:

$$|\psi_0'\rangle = \hat{E}|0x\rangle = \alpha|0x_0\rangle + \beta|1x_1\rangle \tag{7}$$

$$|\psi_1'\rangle = \hat{E}|1x\rangle = m|0y_0\rangle + n|1y_1\rangle \tag{8}$$

where $|x_i\rangle$ and $|y_i\rangle$ are the pure ancillary states determined uniquely by $\hat{E}$. Since $\hat{E}$ must be unitary, we can know $|\alpha|^2 + |m|^2 = 1$, $|\beta|^2 + |n|^2 = 1$ and $\alpha\beta^* + n^* m = 1$, then we can get $|\alpha|^2 = |n|^2$, $|\beta|^2 = |m|^2$ [11].

First, suppose the obtained particles by Alice are $|0\rangle$, and Eva's system can be described by $|\psi_0'\rangle$. The corresponding density matrix of the system can be expressed as $\rho = |\psi_0'\rangle\langle\psi_0'|$. With the orthogonal basis $\{|0x_0\rangle, |1x_1\rangle, |0y_0\rangle, |1y_1\rangle\}$, the state ρ can be rewritten as:

$$\rho = \begin{pmatrix} |\alpha|^2 & 0 & 0 & \alpha\beta^* \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \alpha^*\beta & 0 & 0 & |\beta|^2 \end{pmatrix} \tag{9}$$

Alice encodes her message by performing the unitary operations U_0, U_1, U_2 and U_3 with the probabilities p_0, p_1, p_2 and p_3, and $p_0+p_1+p_2+p_3=1$. After Alice's encoding operation, the state ρ becomes ρ':

$$\begin{aligned}\rho' &= p_0U_0\rho U_0 + p_0U_0\rho U_0 + p_0U_0\rho U_0 + p_0U_0\rho U_0 \\ &= \begin{pmatrix} (p_0+p_1)|\alpha|^2 & (p_0-p_1)\alpha\beta^* & 0 & 0 \\ (p_0-p_1)\alpha^*\beta & (p_0+p_1)|\beta|^2 & 0 & 0 \\ 0 & 0 & (p_2+p_3)|\alpha|^2 & (p_2-p_3)\alpha\beta^* \\ 0 & 0 & (p_2-p_3)\alpha^*\beta & (p_2+p_3)|\beta|^2 \end{pmatrix}\end{aligned} \tag{10}$$

According to the theory of Von-Neumann entropy, the maximal amount of information I_0 extracted from this state can be expressed as $I_0 = S(\rho') = -Tr(\rho'\log_2\rho')$.

Because of the existence of a large number of particles, we can suppose $p_0 = p_1 = p_2 = p_3 = 1/4$. By solving the $\det(\rho'-\lambda)$ we can get the eigenvalues of ρ' that are:

$$\begin{aligned}\lambda_0 = \lambda_1 &= \frac{1}{2}|\alpha|^2, \\ \lambda_2 = \lambda_3 &= \frac{1}{2}|\beta|^2.\end{aligned} \tag{11}$$

Thus the maximal information can be rewritten.

$$I_0 = -\sum_{i=0}^{3}\lambda_i\log_2\lambda_i \tag{12}$$

Suppose $|\alpha|^2 = a$, $|\beta|^2 = b$, $|m|^2 = s$, $|n|^2 = t$. From the front analysis, we can get $a = |\alpha|^2 = |n|^2 = t$, $b = |\beta|^2 = |m|^2 = s$ and $a+b=1$. Thus, the maximal amount of information contained in qubit $|0\rangle$ is expressed as

$$\begin{aligned}I_0 &= -\left(\frac{a}{2}\log_2\frac{a}{2} + \frac{b}{2}\log_2\frac{b}{2} + \frac{a}{2}\log_2\frac{a}{2} + \frac{b}{2}\log_2\frac{b}{2}\right) \\ &= -\left(a\log_2\frac{a}{2} + (1-a)\log_2\frac{(1-a)}{2}\right)\end{aligned} \tag{13}$$

As above, the maximum amount of information contained in qubit $|1\rangle$ is expressed as:

$$I_0 = -\left(t\log_2\frac{t}{2} + (1-t)\log_2\frac{(1-t)}{2}\right) \tag{14}$$

Assuming that the probability of $|0\rangle, |1\rangle$ being sent by Alice is one half, respectively, finally, Eve can gain the maximal information I.

$$I = \frac{1}{2}(I_0 + I_1) = I_0 = -\left(a\log_2\frac{a}{2} + (1-a)\log_2\frac{(1-a)}{2}\right) \tag{15}$$

The above analysis obtained the maximal information that Eve can obtain. Next, let us analyze the probability of Eve being detected. As Eve does not know which particles are the decoy photons, she performs the same attack operation on all particles. After Eve's attack, the state of the decoy photons becomes $\left|G_4\right\rangle_{Eve}$.

$$\left|G_4\right\rangle_{Eve} = \hat{E}\hat{E}\hat{E}\hat{E}\left[\frac{1}{2\sqrt{2}}\left(\begin{array}{l}\left|0x0x0x0x\right\rangle+\left|0x0x1x1x\right\rangle-\left|0x1x0x1x\right\rangle+\left|0x1x1x0x\right\rangle\\+\left|1x0x0x1x\right\rangle+\left|1x0x1x0x\right\rangle+\left|1x1x0x0x\right\rangle-\left|1x1x1x1x\right\rangle\end{array}\right)\right] \tag{16}$$

When Alice received sequence S_A', she extracts the decoy photons and performs the four-particle genuine entangled state measurement. Assuming the number of decoy photons M equals to one, and the probability $p_{|G_4\rangle}$ that Alice gets the four-particle genuine entangled state is the probability that the channel is safe. By solution formula $\left|G_4\right\rangle_{Eve}$ we can get:

$$p_{|G_4\rangle} = \frac{1}{8}\left(a^4+b^4+s^4+t^4+6a^2b^2+6a^2s^2+6a^2t^2+24abst+6b^2s^2+6b^2t^2+6s^2t^2\right) \tag{17}$$

Due to $a=t$, $b=s$ and $a+b=1$, we get the following relations:

$$\begin{aligned} p_{|G_4\rangle} &= \frac{1}{8}\left(8a^4+8b^4+48a^2b^2\right) \\ &= 8a^4-16a^3+12a^2-4a+1 \end{aligned} \tag{18}$$

Thus, the probability p_{Eve} that Eve can be detected can be expressed as:

$$p_{Eve} = 1-p_{|G_4\rangle} = -8a^4+16a^3-12a^2+4a \tag{19}$$

From Equations (15) and (19), we can get the relationship between the maximal information that Eve can obtain and the probability that Eve can be detected. In order to observe the effect of the protocol, we compare the results of our protocol to Reference [23], which is one of the most famous QSDCs (Figure 2). As shown in Figure 2, the solid line expresses the effect in FGEP and the dotted line expresses the effect in Reference [23]. Obviously, if Eve wants to get the same amount of information, she must face a larger detection probability in FGEP. This can indicates that FGEP is secure. It is worth noting that this result is only in the case where M equals one.

Then, we consider the case where M is greater than one. In this case, the only chance that Eve gets the information and is not detected is if Alice measures each group of decoy photons and all are in the four-particle genuine entangled state. Thus, the probability p_{MEve} that Eve can be detected can be expressed as:

$$p_{MEve} = 1-\left(p_{|G_4\rangle}\right)^M = 1-\left(8a^4-16a^3+12a^2-4a+1\right)^M \tag{20}$$

We can see from Figure 3 that if the number of decoy photons increases, the result will be better. When M is 10 and I taken to 1.5, the detection probability is $P=0.977$. This means that it is hard for Eve to get the information without being detected.

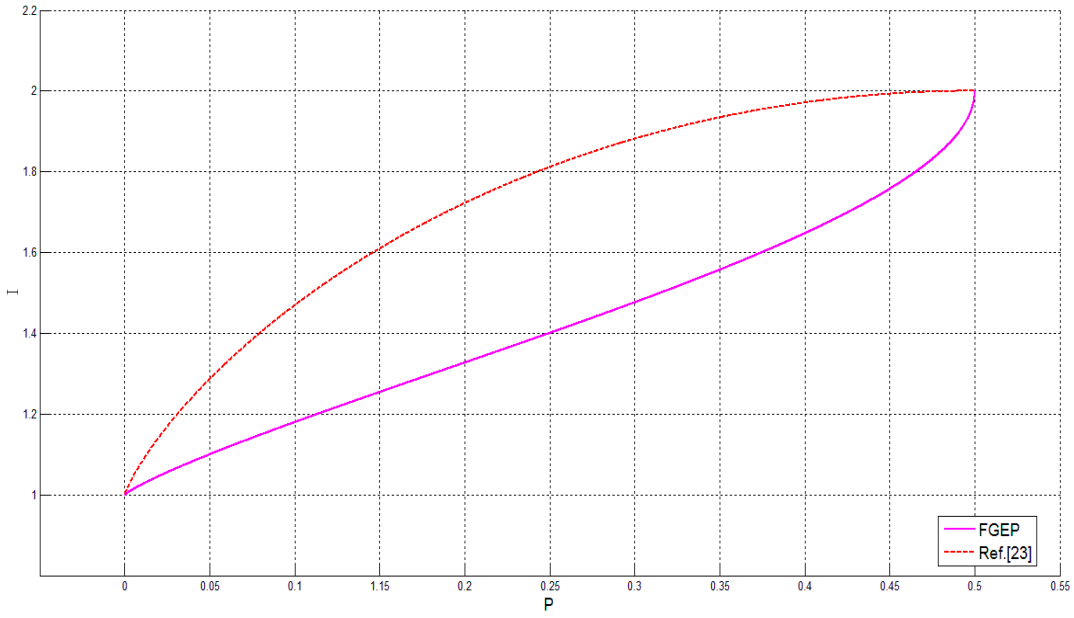

Figure 2. The comparison of the two detection results. The solid line expresses the effect in FGEP and the dotted line expresses the effect in Reference [23]. In the figure above, horizontal coordinates indicate the probability P that Eve can be detected, and vertical coordinates indicate the maximal information I that Eve can obtain.

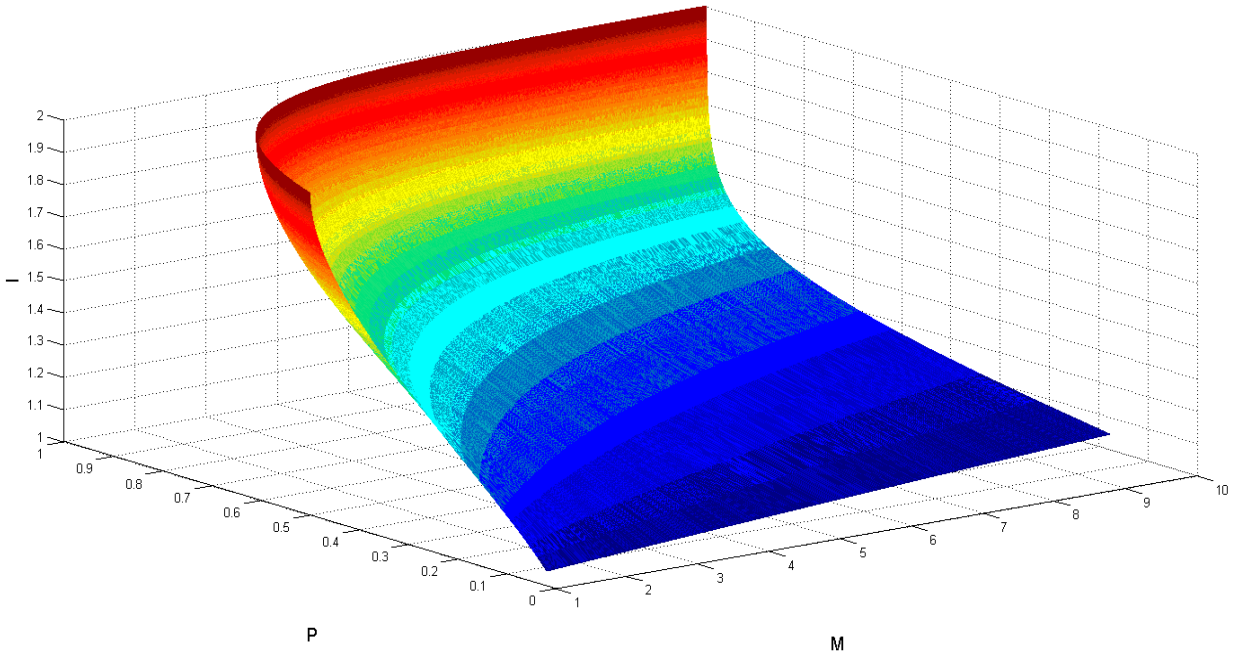

Figure 3. The relationship between the maximal information I that Eve can obtain, and the probability P that Eve can be detected and the number of decoy photons M.

4. Conclusions

Compared to other quantum secure direct communication protocols, FGEP has the following differences:

(i) The eavesdropping detection method using the four-particle genuine entangled state as decoy photons in the FGEP protocol is similar to the method using the control mode [23].
(ii) In the FGEP protocol, the Bell states are prepared by Bob rather than by Alice. This guarantees that the home qubits could not leak to Eve, and the Bell states that carries the secure message can be reused.
(iii) The FGEP protocol is based on the four-particle genuine entangled state, which can reduce the times of detection.

In summary, an eavesdropping detection strategy based on four-particle genuine entangled state in quantum direct communication protocol has been introduced, and the results are analyzed quantitatively by comparing the relationship between the information that the eavesdroppers can obtain and the probability of being detected.

In the analysis, if the eavesdropper obtains the same amount of information, she must face a larger detection probability in FGEP, which shows that the efficiency of eavesdropping detection in FGEP is relatively high. Through analysis we can also know that the security of our protocol will be greatly improved by increasing the number of decoy photons. In order to obtain enough security required for quantum secure direct communication, Bob only needs to increase by a small amount of decoy photons. This fully shows that our protocol is secure and feasible.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (Grant No. 61472048, No. 61402058, No. 61472046, No. 61202082, No. 61370194), the Beijing Natural Science Foundation (4152038), the China Postdoctoral Science Foundation funded project No. 2014M561826.

Author Contributions

Jian Li, Zeshi Pan, Fengqi Sun, Yanhua Chen, Zheng Wang and Zuozhi Shi proposed the main idea and analyzed the data. Zeshi Pan wrote the manuscript. All authors have read and approved the final manuscript.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theor. Computer Sci*. **2014**, *560*, 7–11.
2. Deng, F.G.; Li, X.H.; Zhou, H.Y.; Zhang, Z.-J. Improving the security of multiparty quantum secret sharing against Trojan horse attack. *Phys. Rev. A* **2005**, *72*, doi:10.1103/PhysRevA.72.044302.
3. Song, T.T.; Wen, Q.Y.; Gao, F.; Chen, H. Participant attack and improvement to multiparty quantum secret sharing based on GHZ states. *Int. J. Theor. Phys*. **2013**, *52*, 293–301.

4. Adhikari, S.; Roy, S.; Chakraborty, S.; Chakraborty, S.; Jagadish, V.; Haris, M.K.; Kumar, A. Controlled secret sharing protocol using a quantum cloning circuit. *Quantum Inf. Process*. **2014**, *13*, 2071–2080.
5. Liao, C.H.; Yang, C.W.; Hwang, T. Dynamic quantum secret sharing protocol based on GHZ state. *Quantum Inf. Process*. **2014**, *13*, 1907–1916.
6. Wu, Y.; Cai, R.; He, G.; Zhang, J. Quantum secret sharing with continuous variable graph state. *Quantum Inf. Process*. **2014**, *13*, 1085–1102.
7. Wang, C.; Liu, J.-W.; Liu, X.; Shang, T. A Novel Deterministic Secure Quantum Communication Scheme with Einstein—Podolsky—Rosen Pairs and Single Photons. *Commun. Theor. Phys*. **2013**, *60*, doi:10.1088/0253-6102/60/4/03.
8. Kao, S.H.; Tsai, C.W.; Hwang, T. Comment on: Supervisory Asymmetric Deterministic Secure Quantum Communication. *Int. J. Theor. Phys*. **2012**, *51*, 3868–3875.
9. Huang, W.; Wen, Q.Y.; Liu, B.; Gao, F.; Chen, H. Deterministic secure quantum communication with collective detection using single photons. *Int. J. Theor. Phys*. **2012**, *51*, 2787–2797.
10. Yuan, H.; Zhang, Q.; Hong, L.; Yin, W.-J.; Xu, D.; Zhou, J. Scheme for Deterministic Secure Quantum Communication with Three-qubit GHZ State. *Int. J. Theor. Phys*. **2014**, *53*, 2558–2564.
11. 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* **2003**, *68*, doi:10.1103/PhysRevA.68.042317
12. Stefano, L.M.M. Secure Deterministic Communication without Entanglement. *Phys. Rev. Lett* **2005**, doi:10.1103/PhysRevLett.94.140501.
13. Lucamarini, M.; Mancini, S. Secure deterministic communication without entanglement. *Phys. Rev. Lett.* **2005**, *94*, doi:10.1103/PhysRevLett.94.140501.
14. Li, W.; Chen, J.; Wang, X.; Li, C. Quantum Secure Direct Communication Achieved by Using Multi-Entanglement. *Int. J. Theor. Phys.* **2014**, *54*, 100–105.
15. Yan, C.; Zhang, S.-B.; Yan, L.-L.; Sheng, Z.-W. A multiparty controlled bidirectional quantum secure direct communication and authentication protocol based on EPR pairs. *Chin. Phys. Lett*. **2013**, *30*, doi:10.1088/0256-307X/30/6/060301.
16. Li, J.; Jin, H.F.; Jing, B. Improved eavesdropping detection strategy based on four-particle cluster state in quantum direct communication protocol. *Chin. Sci. Bull*. **2012**, *57*, 4434–4441.
17. Deng, F.G.; Li, X.H.; Li, C.Y.; Zhou, P.; Zhou, H.Y. Quantum secure direct communication network with Einstein–Podolsky–Rosen pairs. *Phys. Lett. A* **2006**, *359*, 359–365.
18. Hwang, T.; Li, C.M; Lee, N.Y. Secure direct communication using deterministic BB84 protocol. *Int. J. Mod. Phys. C* **2008**, *19*, 625–635.
19. Bin, G.; Yu-Gai, H.; Xia, F.; Yi, Z.C. A two-step quantum secure direct communication protocol with hyperentanglement. *Chin. Phys. B* **2011**, *20*, doi:10.1088/1674-1056/20/10/100309.
20. Chang, Y.; Xu, C.; Zhang, S.; Yan, L. Controlled quantum secure direct communication and authentication protocol based on five-particle cluster state and quantum one-time pad. *Chin. Sci. Bull.* **2014**, *59*, 2541–2546.
21. Du, R.; Sun, Z.; Wang, B.; Long, D. Quantum secret sharing of secure direct communication using one-time pad. *Int. J. Theor. Phys*. **2012**, *51*, 2727–2736.

22. Gu, B.; Zhang, C.Y.; Cheng, G.S.; Huang, Y.G. Robust quantum secure direct communication with a quantum one-time pad over a collective-noise channel. *Sci. China Phys. Mech. Astron.* **2011**, *54*, 942–947.
23. Boström, K.; Felbinger, T. Deterministic secure direct communication using entanglement. *Phys. Rev. Lett*. **2002**, *89*, doi:10.1103/PhysRevLett.89.187902.
24. Gu, B.; Xu, F.; Ding, L.; Zhang, Y. High-capacity three-party quantum secret sharing with hyperentanglement. *Int. J. Theor. Phys*. **2012**, *51*, 3559–3566.
25. Chang, Y.; Zhang, S.B.; Li, J.; Yan, L.L. Robust EPR-pairs-based quantum secure communication with authentication resisting collective noise. *Sci. China Phys. Mech. Astron*. **2014**, *57*, 1907–1912.
26. Wang, T.Y.; Cai, X.Q. An Efficient Quantum Secret Sharing Scheme with Decoy States. *Int. J. Mod. Phys. B* **2012**, *26*, doi:10.1142/S0217979212501226.