Computers, Materials & Continua CMC, vol.63, no.3, pp.1297-1307, 2020

Quantum Secure Direct Communication Protocol with Mutual Authentication Based on Single Photons and Bell States

Lili Yan[1, *], Shibin Zhang[1], Yan Chang[1], Zhibin Sun[2] and Zhiwei Sheng[1]

Abstract: Quantum secure direct communication (QSDC) can transmit secret messages directly from one user to another without first establishing a shared secret key, which is different from quantum key distribution. In this paper, we propose a novel quantum secure direct communication protocol based on signal photons and Bell states. Before the execution of the proposed protocol, two participants Alice and Bob exchange their corresponding identity ID_A and ID_B through quantum key distribution and keep them secret, respectively. Then the message sender, Alice, encodes each secret message bit into two single photons ($|01\rangle$ or $|10\rangle$) or a Bell state ($|\phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$ or $|\phi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle - |1\rangle|1\rangle)$), and composes an ordered secret message sequence. To insure the security of communication, Alice also prepares the decoy photons and inserts them into secret message sequence on the basis of the values of ID_A and ID_B. By the secret identity ID_A and ID_B, both sides of the communication can check eavesdropping and identify each other. The proposed protocol not only completes secure direct communication, but also realizes the mutual authentication. The security analysis of the proposed protocol is presented in the paper. The analysis results show that this protocol is secure against some common attacks, and no secret message leaks even if the messages are broken. Compared with the two-way QSDC protocols, the presented protocol is a one-way quantum communication protocol which has the immunity to Trojan horse attack. Furthermore, our proposed protocol can be realized without quantum memory.

Keywords: Quantum secure direct communication, mutual authentication, bell states, single photons.

1 Introduction

The development of quantum computation and quantum information has brought new challenges and opportunities for the research of information security [Zhang, Chang, Yan et al. (2019)]. The principle of quantum mechanics provides unconditionally secure information exchange. Since the first quantum key distribution (QKD) was proposed in 1984 Bennett et al. [Bennett and Brassard (1984)], many quantum secure protocols have

[1] School of Cybersecurity, Chengdu University of Information Technology, Chengdu, 610000, China.

[2] Natural Resource Ecology Laboratory, Colorado State University, Fort Collins, CO 80523, USA.

[*] Corresponding Author: Lili Yan. Email: yanlili@cuit.edu.cn.

Received: 23 January 2020; Accepted: 26 February 2020.

been proposed [Zhong, Liu and Xu (2018); Hao, Zhang, Huang et al. (2019)]. Quantum secure direct communication (QSDC) is a very important branch of quantum communication. In the QSDC protocol, secret messages are transmitted directly without first establishing a key to encrypt them.

The first QSDC protocol, based on Einstein-Pololsky-Rosen (EPR) pairs, was proposed by Long et al. [Long and Liu (2002)]. Subsequently, Deng et al. [Deng, Long and Liu (2003)] developed the standard criteria and safety judgment condition for QSDC. It has also been shown that QSDC can be used to distribute secret keys, and it has a higher capacity than typical QKD schemes. In 2004, Deng et al. [Deng and Long (2004)] proposed a QSDC protocol based on a single photon and a quantum one-time pad (OTP). Since then, many researchers have proposed a variety of QSDC protocols on the basis of these principles by using different quantum states as quantum channels. These quantum channels include single photons [Lucamarini and Mancini (2005); Wang, Quan and Tang (2006)], EPR pairs [Zhu, Xia, Fan et al. (2006)], GHZ class states [Jin, Ji, Zhang et al. (2006); Banerjee and Pathak (2012)], W class states [Cao and Song (2006); Chang, Zhang, Yan et al. (2014)], cluster state [Wang, Fang and Tan (2006); Cao, Yang and Wen (2010); Sun, Du and Long (2012); Li, Song, Guo et al. (2012); Nie, Li, Liu et al. (2011); Kui, Guo and Xue (2011)], and multiparticle entangled state [Lin, Wen, Gao et al. (2008); Xiu, Dong, Dong et al. (2009); Lin, Gao and Liu (2011)].

QSDC protocols are usually weak in impersonation attack. Since no identity authentication scheme is adopted in QSDC, the eavesdropper can impersonate one of two legal users to communicate with the other. He/she might impersonate the receiver to receive the secret message from the sender, or impersonate the sender to send a fake message to the receiver. Identity authentication is an effective way to guard against impersonation attack for QSDC protocols. In 2006, Lee et al. [Lee, Lim and Yang (2006)] proposed the first quantum direct communication with authentication protocol. A third party, Trent, is introduced to authenticate the users participating in the Lee et al.'s protocol. Subsequently, Zhang et al. [Zhang, Liu, Wang et al. (2007)] pointed out that Lee et al.'s protocol suffered from different initial state attack by a dishonest third party, such as Trent. They proposed an improvement to avoid the attack. Yen et al. [Yen, Horng, Goan et al. (2009)] pointed out the Zhang et al.'s protocol still suffered from the same attack and a further improved scheme was proposed by using EPR pairs and dense coding. Yang et al. [Yang, Wang and Zhang (2010)] presented two protocols for QSDC with authentication expansion using single photons. The third party, Trent, authenticates the users participating in the communication. But Yang et al.'s protocols [Yang, Jia, Xia et al. (2012)] cannot resist man-in-the-middle attack. Yu et al. [Yu, Guo and Lin (2013)] proposed a QSDC protocol with authentication using two nonorthogonal states, but the proposed protocol requires participants to have two-way communication ability.

In the paper we propose a mutual authenticated QSDC protocol based on single photons and Bell states. Different form the previous protocols, the proposed protocol has only two participations, Alice and Bob. Alice transmits secret messages directly to Bob. Both sides of the communication can confirm the legitimacy of each other's identity, and only authenticated users can send or receive the correct secret messages. The proposed protocol does not require the receiver to be equipped with quantum memory.

The rest of this paper is organized as follows. In Section 2, we introduce our protocol based on single photons and Bell states. In Section 3, we show the security verification of the protocol under some common attacks. Section 4 present conclusions.

2 The QSDC protocol with mutual authentication

In this section, we propose a quantum protocol for quantum secure direct communication using Bell states. There are two participants in the protocol. Alice wants to transmit *N*-bit secret message *M* to Bob. ID_A and ID_B are the identities of Alice and Bob, respectively. Let's first introduce some prior theoretical basis in the proposed protocol. The four Bell states can be denoted as

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle) \tag{1}$$

$$|\phi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle - |1\rangle|1\rangle) \tag{2}$$

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle + |1\rangle|0\rangle) \tag{3}$$

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle) \tag{4}$$

We assume that Alice and Bob generate and pre-share their own secret identity ID_A and ID_B, respectively ($ID_A, ID_B \in \{0,1\}^N$). To facilitate discussion, without loss of generality, we assume that the length of ID_A and ID_B is exactly equal to *N*. When Alice sends the photons to Bob, ID_A is used to prepare the decoy photons, and ID_B is used to determine the position of the decoy photons.

The process of the proposed protocol will be described in steps as follows.

Step 1: ID_A and ID_B are pre-shared between Alice and Bob, respectively, via an unconditionally secure quantum key distribution (QKD) protocol.

Step 2: Alice prepares an ordered 2*N* qubit pairs which are in one of the states $\{|01\rangle, |10\rangle, |\phi^+\rangle, |\phi^-\rangle\}$. All of these qubits compose an ordered sequence *S*.

To insure the security of communication, *N* qubit pairs are used to send a secret message where $|01\rangle$ and $|10\rangle$ represent bit 0, and $|\phi^+\rangle$ and $|\phi^-\rangle$ represent bit 1. More specifically, if the *i-th* bit ($1 < i < N$) of the secret message is 0, Alice produces state $|01\rangle$ or $|10\rangle$. Otherwise, she produces state $|\phi^+\rangle$ or $|\phi^-\rangle$. All of these qubit pairs compose sequence S_A.

On the basis of the values of ID_A, Alice prepares the remaining *N* qubit pairs which are used to check eavesdropping. If the value of the *i-th* bit of ID_A is 0, Alice produces state $|01\rangle$ or $|10\rangle$. Otherwise, she produces state $|\phi^+\rangle$ or $|\phi^-\rangle$. All of these qubit pairs compose sequence S_B. Then Alice inserts decoy photons into the qubit sequence of the secret message based on the values of ID_B. If the value of the *i-th* bit of ID_B is 0, Alice inserts the decoy photons (i.e., the *i-th* bit of S_B) before the secret message (i.e., the *i-th* bit

of S_A). Otherwise, Alice inserts the decoy photons behind it. Thus, S_A and S_B compose an ordered sequence S.

For example, when N=4, ID_A=0110, ID_B=1010, message M=1100, the sequence S_A will be $\{|\phi^+\rangle, |\phi^-\rangle, |10\rangle, |10\rangle$, the sequence S_B will be $\{|01\rangle, |\phi^+\rangle, |\phi^-\rangle, |10\rangle\}$, and the sequence S will be $\{|\phi^+\rangle, |01\rangle, |\phi^+\rangle, |\phi^-\rangle, |10\rangle, |\phi^-\rangle, |10\rangle, |10\rangle\}$.

Finally, Alice sends S to Bob. Here the block transmission technology is used to send S [2, 3].

Step 3: Upon receiving the photons, Bob obtains the positon of the decoy photons according to ID_B. He measures the decoy photons in the corresponding basis. If the value of the *i-th* bit of ID_A is 0, Bob measures it in $Z=\{|0\rangle,|1\rangle\}$ basis. If the value of the *i-th* bit of ID_A is 1, he measures it in Bell basis. For the photon pairs of the secret message, he measures them in the basis $Z=\{|0\rangle,|1\rangle\}$ or Bell basis randomly. Finally, he publicly announces an acknowledgment.

Step 4: Then Alice and Bob check eavesdropping. Alice announces the initial states of the decoy photon pairs. Bob's measurement result should be the same as Alice's prepared state. If the error rate is higher than the predetermined error rate, they will terminate the protocol and restart from Step 1. After all the decoy photon pairs announced by Alice are checked, the protocol will continue to the next step.

Step 5: Using the same way as described in Steps 3 to 4, Alice and Bob can also authenticate each other. The initial state of the decoy photon pairs is the same as ID_A. Only authenticated Bob can obtain the secret message.

Step 6: Bob discards measurement results of the decoy pairs, then he can obtain the secret message based on the remaining measurement results. The relationship among this information is shown in Tab. 1.

Table 1: Relationship among the initial state, measurement basis, measurement result and the secret message

initial state	measure basis	measurement results	secret message
$\|01\rangle$	Z basis	01	0
	Bell basis	$\|\psi^+\rangle$ or $\|\psi^-\rangle$	
$\|10\rangle$	Z basis	10	0
	Bell basis	$\|\psi^+\rangle$ or $\|\psi^-\rangle$	
$\|\phi^+\rangle$	Z basis	00 or 11	1
	Bell basis	$\|\phi^+\rangle$	
$\|\phi^-\rangle$	Z basis	00 or 11	1
	Bell basis	$\|\phi^-\rangle$	

Therefore, the proposed protocol achieves the secure transmission of data from Alice to Bob.

Step 7: Comparison of secret information

To ensure that Bob receives the same secret message, Alice and Bob can compare parts of the message. Bob announces parts of the message. If Alice finds that Bob has published the same value as hers, it means that the secret message has been sent successfully.

The process of the information encoding and decoding phase is shown in Fig. 1. The white dots represent $|01\rangle$ or $|10\rangle$, and black dots represent $|\phi^+\rangle$ or $|\phi^-\rangle$.

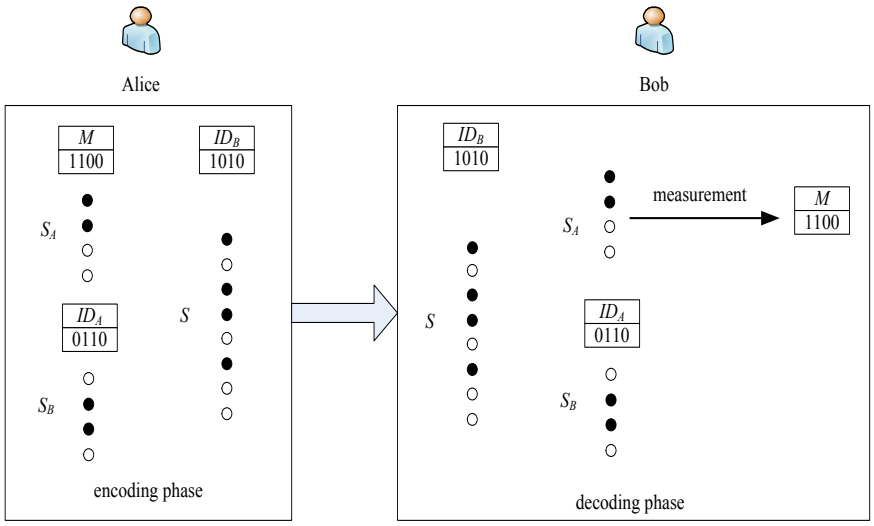

Figure 1: The process of the information encoding and decoding phase

3 Security analysis

In this section, the security of the presented protocol against some common attacks is discussed.

3.1 The impersonation attack

Eve may try to impersonate one of two legal users to communicate with the other one. Suppose Eve generates a sequence S_E. and sends the forged message to Bob in Step 2. After Bob measures the decoy photons in S_E, Eve must announce the initial states of decoy photons to Bob. However, Eve cannot public the correct initial states without knowing the ID_A, and the comparison will be failed. On the other hand, suppose Eve impersonates Bob to obtain the encoding message of Alice. To recover the secret message, Eve has to obtain the right position of decoy photons. However, she has no idea about the identity ID_A and ID_B.

According to the analysis above, the proposed protocol is secure against the impersonation attack.

3.2 The intercept-and-resend attack

In the communication phase, in order to recover the secret message without being detected, Eve can launch an intercept-and-resend attack as follows. In Step 2, Eve intercepts the

sequence S and measures it in Z basis or Bell basis. Then Eve generates the same states based on the measurement results and sends them to Bob. Without knowing the positon of decoy photons, Eve will be detected inevitably.

In detail, let us first consider the case that the state of decoy photon pair is $\left|\phi^{+}\right\rangle$. If Eve intercepts this qubit and performs a measurement on it along the Bell basis, the measurement result will be $\left|\phi^{+}\right\rangle$. Subsequently, Eve retransmits this result state $\left|\phi^{+}\right\rangle$ to Bob. As a result, no error has been introduced. If Eve chooses the Z basis, the measurement result is $\left|00\right\rangle$ or $\left|11\right\rangle$. Then Eve sends $\left|00\right\rangle$ or $\left|11\right\rangle$ to Bob. Bob measures it in Bell basis and obtains $\left|\phi^{+}\right\rangle$ or $\left|\phi^{-}\right\rangle$ each with probability of 1/2. Thus, the error rate introduced by Eve is 50%. Therefore, the probability for Eve to pass the security checking is $\frac{3}{4}=\frac{1}{2}\times 1+\frac{1}{2}\times\frac{1}{2}$.

Now considering the case that the state of decoy photon is $\left|01\right\rangle$, If Eve intercepts this qubit and performs a measurement on it along the Z basis, the measurement result will be $\left|01\right\rangle$. Subsequently, Eve retransmits this result state $\left|01\right\rangle$ to Bob. As a result, no error has been introduced. If Eve chooses the Bell basis, the measurement result is $\left|\psi^{+}\right\rangle$ or $\left|\psi^{-}\right\rangle$. Then Eve sends $\left|\psi^{+}\right\rangle$ or $\left|\psi^{-}\right\rangle$ to Bob. Bob measures it in Z basis and obtains $\left|01\right\rangle$ or $\left|10\right\rangle$ each with probability of 1/2. Thus, the error rate introduced by Eve is 50%. Therefore, the probability for Eve to pass the security checking is $\frac{3}{4}=\frac{1}{2}\times 1+\frac{1}{2}\times\frac{1}{2}$.

Thus, for Eve's intercept-measure-resend attack, the probability of being detected is $d=1-(\frac{3}{4})^{n}$. This probability approximates to 1, if n is large enough.

3.3 Man-in-the-middle attack

In Step 2, if Eve intercepts the sequence S from Alice and Bob, she prepares another sequence S_E and sends it to Bob. However, Alice only announces the initial states of the decoy photon pairs during the protocol. Eve knows nothing about identity ID_A and ID_B, so Eve cannot correctly distinguish between the decoy photons and the secret message photons. Therefore, even if Eve catches these qubits, she cannot obtain the secret message, and her attack cannot pass the eavesdropping check.

3.4 Entangle-measure attack

In this section, we discuss the entangle-measure attack. Eve intercepts sequence S and adds an ancillary state $\left|\varepsilon_{a,b}\right\rangle$ to every particle. Then she performs a unitary attack operation $\hat{E}$ on the composed system. In the proposed protocol, all the transmitted particles are sent together before eavesdropping is detected. Because Eve does not know

which particle is used to detect eavesdropping, she can only perform the same attack operation on all the particles. As for Eve, the state of qubits is distinguishable from the complete mixture, so all qubits are considered in either of the states $|0\rangle$ or $|1\rangle$ with an equal probability $p_0 = p_1 = 0.5$.

After the attack by Eve, the state $|0\rangle$ and $|1\rangle$ become [Gisin, Ribordy, Tittel et al. (2002)]

$$|\varphi_0'\rangle = \hat{E}|0,\varepsilon\rangle = a|0,\varepsilon_{00}\rangle + b|1,\varepsilon_{01}\rangle, \tag{5}$$

$$|\varphi_1'\rangle = \hat{E}|1,\varepsilon\rangle = c|0,\varepsilon_{10}\rangle + d|1,\varepsilon_{11}\rangle \tag{6}$$

where $|a|^2 + |b|^2 = 1$, $|c|^2 + |d|^2 = 1$, $|a|^2 = |d|^2 = F$, $|b|^2 = |c|^2 = D$.

Suppose Alice prepares Bell states $|\phi^+\rangle$ and sends them to Bob after the attack operator $\hat{E}$ is performed, then the state of the composed system becomes:

$$|\varphi\rangle_{Eve} = \frac{1}{\sqrt{2}}[|0\rangle_A (a|0,\varepsilon_{00}\rangle + b|1,\varepsilon_{01}\rangle)_{BE} + |1\rangle_A (c|0,\varepsilon_{10}\rangle + d|1,\varepsilon_{11}\rangle)_{BE}]$$

$$= \frac{1}{\sqrt{2}}(a|0,0,\varepsilon_{00}\rangle + b|0,1,\varepsilon_{01}\rangle + c|1,0,\varepsilon_{10}\rangle + d|1,1,\varepsilon_{11}\rangle)_{ABE}$$

$$= \frac{1}{\sqrt{2}}[(a|0,\varepsilon_{00}\rangle + c|1,\varepsilon_{10}\rangle)_{AE}|0\rangle_B + (b|0,\varepsilon_{01}\rangle + d|1,\varepsilon_{11}\rangle)_{AE}|1\rangle_B]. \tag{7}$$

After measurement, $|\varphi\rangle_{Eve}$ will collapse to $(a|0,\varepsilon_{00}\rangle + c|1,\varepsilon_{10}\rangle)_{AE}|0\rangle_B$ or $(b|0,\varepsilon_{01}\rangle + d|1,\varepsilon_{11}\rangle)_{AE}|1\rangle_B$, each of which is with probability of 1/2.

Obviously, when Bob performs Bell measurement on the decoy photons, the probability for Eve not to be detected is

$$p|\varphi\rangle = \frac{1}{2}(|a|^2 + |d|^2) = |a|^2 = |d|^2 = F. \tag{8}$$

So the lower bound of the detection probability d is

$$d = 1 - p|\varphi\rangle = 1\text{-}F = D. \tag{9}$$

Eve can eavesdrop. The maximal amount of the information I is

$$I = -F\log_2 F + (1-F)\log_2(1-F), \tag{10}$$

$$I = -(1-d)\log_2(1-d) + d\log_2 d. \tag{11}$$

When Eve obtains the information, the detection probability is shown in Fig. 2.

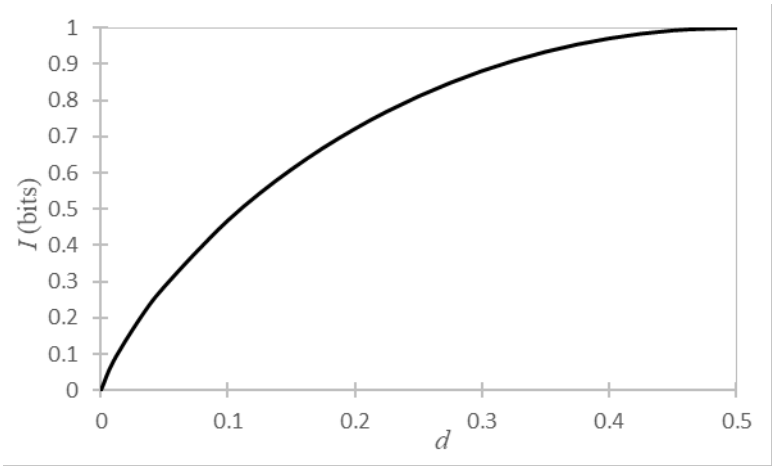

Figure 2: Detection probability of eavesdropping information

The above results show that if Eve wants to gain the full information (I=1), the probability of the eavesdropping detection is d=50%.

3.5 Correctness of the secret message

To ensure that Bob receives the same secret message M' as M, he needs to compare the message with Alice. They can employ one-way hash function [Damgard (1990); Ren, Zhu, Sharma et al. (2020)] (i.e., $h:\{0,1\}^n \to \{0,1\}^m$, where n denotes the length of the inputted data, and m denotes the length of the hash code.) on their secret message M' and M to obtain two hash codes, $h(M')$ and $h(M)$, each of which is with m bit length. Finally, Alice publishes all or part of $h(M')$. If Bob finds that Alice has published the same value as herself, it means that the secret message has been sent successfully. Otherwise, it means that the protocol fails to execute. But without knowing the positon of the decoy photons, the eavesdropper could not recover secret message. He/she could not eavesdrop on any information of the secret message.

4 Conclusion

In this paper, we propose a quantum secure direct communication protocol with user authentication based on signal photons and Bell states. The process has been explained in detail, and its security is analyzed.

In the proposed protocol, participants share their identity *ID* through QKD. Under the condition that the identity *ID* is secret and leak-free, Alice and Bob can identify each other and detect eavesdropping behavior. The eavesdropper could not eavesdrop on any information of the secret message.

Compared with previous QSDC protocols, the presented protocol has several advantages. Firstly, all the particles prepared by Alice are sent to Bob one time. The proposed protocol is a one-step quantum communication protocol which has the immunity to Trojan horse attack. Secondly, the proposed protocol can be realized without quantum memory. Finally,

the checking particle sequence has been fully used for both verifying users' identities and detecting eavesdropping behavior, which will help to save quantum resources.

Funding Statement: This work was supported by the National Natural Science Foundation of China (Grant Nos. 61572086, 61402058), Major Project of Education Department in Sichuan (Grant No. 18ZA0109), Planning project of Sichuan Network Culture Research Center (Grant No. WLWH18-22), Key Research and Development Project of Sichuan Province (No. 20ZDYF2324, No. 2019ZYD027, No. 2018TJPT0012), Innovation Team of Quantum Security Communication of Sichuan Province (No. 17TD0009), Academic and Technical Leaders Training Funding Support Projects of Sichuan Province (No. 2016120080102643), Application Foundation Project of Sichuan Province (No. 2017JY0168), Science and Technology Support Project of Sichuan Province (No. 2018GZ0204, No. 2016FZ0112).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study

References

Banerjee, A.; Pathak, A. (2012): Maximally efficient protocols for direct secure quantum communication. *Physics Letters A*, vol. 376, no. 45, pp. 2944-2950.

Bennett, C. H.; Brassard, G. (1984): Public key distribution and coin tossing. *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, pp. 175-179.

Cao, H. J.; Song, H. S. (2006): Quantum secure direct communication with W state. *Chinese Physics Letters*, vol. 23, no. 2, pp. 290.

Cao, W. F.; Yang, Y. G.; Wen, Q. Y. (2010): Quantum secure direct communication with cluster state. *Science in China Series G*, vol. 53 no. 71, pp. 1271-1275.

Chang, Y.; Zhang, S. B.; Yan, L. L.; Li, J. (2014): Deterministic secure quantum communication and authentication protocol based on three-particle W state and quantum one-time pad. *Chinese Science Bulletin*, vol. 59 no. 23, pp. 2835-2840.

Damgard, I. B. (1990): A design principle for hash functions. *Advances in Cryptology*, *CRYPTO' 89 Proceedings*, no. 435, pp. 416-427.

Deng, F. G.; Long, G. L.; Liu, X. S. (2003): Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. *Physics Review A*, vol. 68, no. 4.

Deng, F. G.; Long, G. L. (2004): Secure direct communication with a quantum one-time pad. *Physical Review A*, vol. 69, no. 5.

Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. (2002): Quantum cryptography. *Review of Modern Physics*, vol. 74, no. 1, pp. 145-795.

Jin, X. R.; Ji, X.; Zhang, Y. Q.; Hong, S. K.; Yeon, K. H. et al. (2006): Three-party quantum secure direct communication based on GHZ states. *Physics Letters A*, vol. 354, no, 1-2, pp. 67-70.

Kui, H.; Guo, H. L.; Xue, Y. Z. (2011): An efficient scheme for five-party quantum state sharing of an arbitrary m-qubit state using multiqubit cluster states. *Quantum Information Processing*, vol. 10, no. 4, pp. 463-473.

Lee, H.; Lim, J.; Yang, H. (2006): Quantum direct communication with authentication. *Physical Review A*, vol. 73, no. 4, 042305.

Li, J.; Song, D. J.; Guo, X. J.; Jing, B. (2012): A quantum secure direct communication protocol based on a five-particle cluster state and classical XOR operation. *Chinese Physics C*, vol. 36, no. 1, pp. 31-36.

Lin, S.; Gao, F.; Liu, X. F. (2011): Quantum secure direct communication with five-qubit entangled state. *Chinese Physics Letters*, vol. 28, no. 3.

Lin, S.; Wen, Q. Y.; Gao, F.; Zhu, F. C. (2008): Quantum secure direct communication with χ-type entangled states. *Physical Review A*, vol. 78.

Long, G. L.; Liu, X. S. (2002): Theoretically efficient high-capacity quantum-key-distribution scheme. *Physical Review A*, vol. 65.

Lucamarini, M.; Mancini, S. (2005): Secure deterministic communication without entanglement. *Physical Review Letters*, vol. 94, no. 14.

Nie, Y. Y.; Li, Y. H.; Liu, J. H.; Sang, M. H. (2011): Quantum information splitting of an arbitrary three-qubit sate by using two four-qubit cluster states. *Quantum Information Processing*, vol. 10, no. 3, pp. 297-305.

Ren, Y. J.; Zhu, F. J; Sharma, P. K.; Wang, T.; Wang, J. et al. (2020): Data query mechanism based on hash computing power of blockchain in Internet of Things. *Sensors*, vol. 20, no. 1.

Sun, Z. W.; Du, R. G.; Long, D. Y. (2012): Quantum secure direct communication with two-photon four-qubit cluster states. *International Journal of Theoretical Physics*, vol. 51, no. 6, pp. 1946-1952.

Wang, G. Y.; Fang, X. M.; Tan, X. H. (2006): Quantum secure direct communication with cluster state. *Chinese Physics Letters*, vol. 23, no. 10, pp. 2658-2661.

Wang, J.; Quan, Z.; Tang, C. J. (2006): Quantum secure direct communication based on order rearrangement of single photons. *Physical Letters A,* vol. 358 no. 4, pp. 256-258.

Xiao, H.; Zhang, J.; Huang, W. H.; Zhou, M.; Hu, W. C. (2019): An efficient quantum key distribution protocol with dense coding on single photons. *Computers, Materials & Continua*, vol. 61, no. 2, pp. 759-775.

Xiu, X. M.; Dong, H. K.; Dong, L.; Gao, Y. J.; Chi, F. (2009): Deterministic secure quantum communication using four-particle genuine entangled state and entanglement swapping. *Optics Communications*, vol. 282, no. 12, pp. 2457-2459.

Yang, J.; Wang, C.; Zhang, R. (2010): Quantum secure direct communication with authentication expansion using single photons. *Communications in Theoretical Physics*, vol. 54, no. 5, pp. 829-834.

Yang, Y. G.; Jia, X.; Xia, J.; Shi, L.; Zhang, H. (2012): Comment on "quantum secure direct communication with authentication expansion using single photons". *International Journal of Theoretical Physics*, vol. 51 no. 12, pp. 3681-3687.

Yen, C. A.; Horng, S. J.; Goan, H. S.; Kao, T. W.; Chou, Y. H. (2009): Quantum direct communication with mutual authentication. *Quantum Information & Comput*ation, vol. 9 no. 5, pp. 376-394.

Yu, C. H.; Guo, G. D.; Lin, S. (2013): Quantum secure direct communication with authentication using two nonorthogonal states. *International Journal of Theoretical Physics*, vol. 52, no. 6, pp. 1937-1945.

Zhang, S. B; Chang, Y.; Yan, L. L.; Sheng, Z. W.; Yang, F. et al. (2019): Quantum communication networks and trust management: a survey. *Computers, Materials & Continua*, vol. 61, no. 3, pp. 1145-1174.

Zhang, Z. J.; Liu, J.; Wang, D.; Shi, S. H. (2007): Comment on "Quantum direct communication with authentication". *Physical Review A*, vol. 75, no. 2.

Zhong, J. F.; Liu, Z. H.; Xu J. (2018): Analysis and improvement of an efficient controlled quantum secure direct communication and authentication protocol. *Computers, Materials & Continua*, vol. 57, no. 3, pp. 621-633.

Zhu, A. D.; Xia, Y.; Fan, Q. B.; Zhang, S. (2006): Secure direct communication based on secret transmitting order of particles. *Physical Review A*, vol. 73, no. 2, pp. 457-460.