

A Quantum Secure Direct Communication Protocol Based on Six-qubit Cluster State

Danjie SONG, Chun LONG, Wei WAN, Jing ZHAO, Shaojie WANG

Computer Network Information Center, Chinese Academy of Sciences, China

songdanjie@cnic.cn, longchun@cnic.cn, wanwei@cnic.cn, jingzhao@cnic.cn, wangshaojie@cnic.cn

Abstract—To enhance the efficiency of eavesdropping detection in quantum secure direct communication, a quantum secure direct communication protocol based on six-qubit cluster state is proposed. In the security analysis, the method of the entropy theory is introduced, and three detection strategies are compared quantitatively by using the constraint between the information eavesdroppers can obtain and the interference introduced. If the eavesdropper obtains the same amount of information, she must face a larger detection probability in the presented scheme than the other two, and if obtains the whole information, the detection rate of the Ping-Pong protocol is 50%; the second protocol which used two particles of EPR pair as detection particles is also 50%; while the presented protocol is 94%. At last, the security of the proposed protocol is discussed. The analysis results indicate that the protocol in this paper is more secure than the other two.

Keywords— quantum secure direct communication, six-qubit cluster state, eavesdropping detection

I. INTRODUCTION

Quantum secure communication consists of quantum key distribution (QKD) and quantum secure direct communication (QSDC), the latter is taken into great consideration in the paper. Quantum mechanics offers some unique capabilities for processing and transmitting quantum information. Over the past decades, scientists have made dramatic progress in the field of quantum communication. Since Bennett and Brassard [1] proposed the pioneer QKD protocol in 1984 in which two remote authorized users (Alice and Bob) can create a shared private key, a lot of quantum information security processing schemes have been proposed, such as quantum teleportation [2-4], quantum dense coding [5-6], Deterministic Secure Quantum Communication (DSQC) [7-8], QSDC [9-13] and so on.

In 2002 Boström and Felbinger proposed a Ping-Pong protocol using Einstein-Podolsky-Rosen (EPR) pairs as quantum information carriers [9]. But it proved to be an only deterministic QKD scheme

rather than a QSDC scheme. Later, researchers are interested in QSDC, and many protocols were presented, including the protocols without using entanglement [14-15], the protocols using entanglement [16-21], and the two-way QSDC protocols [22-23]. In these protocols, the secret message is transmitted through the transmission channel directly. Compared with the QKD, the security requirement of QSDC is higher because whether the eavesdropper is detected or not, the secret message cannot be leaked out absolutely. For example, there will be some security problems when the ‘ping-pong’ protocol is used for QSDC [24-28]. But the unconditional security can still be achieved by adopting a well-designed QSDC protocol in theory [29-31].

Long et al. proposed a theoretical two-step QKD scheme using EPR pairs [10], which is the first QSDC protocol. It introduced the method of quantum data block transmission for the security in QSDC based on error rate analysis. To guard the secret message, one has to ensure the security of a block of quantum data [8-13] before encoding the secret message. When errors exist, error correction and quantum privacy amplification can be used to maintain its security. In 2003, modifying the basic idea in [10], Deng et al. proposed a two-step secure QSDC scheme with EPR pairs [11] transmitted in blocks as well. Moreover, error correction and quantum privacy amplification can be used to maintain its security.

The efficiency of the different detection strategies can be compared by using the Entropy method. To increase the efficiency of eavesdropping detection in the QSDC protocol, an improved protocol based on six-qubit cluster state, used to detect eavesdroppers is presented. In [13], it calls the

original Ping-Pong protocol as OPP, and the protocol it proposed as MPP for convenience. Referred to [13], the proposed protocol in this paper is called SPP just for short. During the security analysis, the method of the entropy theory is introduced, and three detection strategies are compared quantitatively by using the constraint between the information that eavesdroppers can obtain and the interference introduced. If the eavesdroppers get the full information, the detection rate of OPP is 50%, and MPP is also 50%; while SPP is 94%. In the end, the security of the proposed protocol is discussed. The analysis results show that the proposed protocol is more secure than the other two.

II. RELATED WORKS

A. The original "Ping-pong" protocol

As is known to all, the basic principle of the OPP, which is presented by Boström and Felbinger in 2002 [9], is that one bit information can be encoded in the states $|\psi^{\pm}\rangle$, which is completely unavailable to anyone who has access to either of the qubits. To extract secret message from Alice, Bob must own both particles, for no experiment performed on only one photon can distinguish these states from each other. To get information from Alice in secret, Bob prepares two photons in the Bell state $|\psi^+\rangle$ at first. He stores one photon, the home qubit, and sends the other one, the travel qubit, to Alice through a quantum channel. In message mode, receiving the travel qubit, Alice takes a coding operation either I or σ_z on the travel qubit, then sends it back to Bob. Bob, who has now both qubits again, performs a Bell measurement on both qubits, resulting in the final state $|\psi^+\rangle$ or $|\psi^-\rangle$, and he decodes the message as $|\psi^+\rangle \Rightarrow 0, |\psi^-\rangle \Rightarrow 1$, thus he has received one bit of information from Alice. To detect eavesdropping, Alice can switch to control mode with probability c or message mode with probability $1-c$ in random. In control mode, Alice measures the polarization of the travel qubit in the Z-basis $B_Z = \{|0\rangle, |1\rangle\}$ and broadcasts the result using the public channel. Receiving the result from Alice, Bob also switches to control mode and measures the home qubit in the

same basis B_Z and compares both the results, which should be opposite in the absence of Eve. If both results coincide, Bob knows that Eve is in the line and stops the communication.

B. The MPP protocol in [13]

The basic principle of the eavesdropping detection strategy in the MPP protocol in [13] is that in control mode, Bob sends two qubits in the Bell state $|\psi^+\rangle$ to Alice. After receives both particles, Alice performs a Bell measurement. If there is no eavesdropper, every result should be in the Bell state $|\psi^+\rangle$. Otherwise, the communication is interrupted.

Suppose that the message transmitted is in a sequence $x^N = (x_1, \dots, x_N)$, where $x_i \in \{0, 1\}, i = 1, 2, \dots, N$. Now let us give an explicit introduction of MPP [13].

(S1) Bob prepares a number of quantum bits as follows.

(i) Bob prepares a large enough number (N) of Bell states $|\psi^+\rangle$ in sequence. He extracts all the first particles in the Bell states, forming a series of particles S1 (the travel qubits) in order, used to transmit message, and the remaining particles in the Bell states form a series of particles S2 (the home qubits). This step corresponds to message mode in the OPP.

(ii) Bob prepares a large number ($cN/(1-c)$) of Bell states $|\psi^+\rangle$, forming a series of particles S3 in order, used to detect eavesdropping, and this step corresponds to control mode in the OPP. Here, c expresses the probability of entering into control mode in OPP [9]. Note that S3 includes $2cN/(1-c)$ quantum bits.

(iii) Bob inserts the decoy photon S3 to the particles S1 in random. Then a new sequence S4 where there are Bell type decoy photons is produced, but only Bob knows their positions.

(S2) Bob stores the particles S2 and sends the particles S4 to Alice.

(S3) After Alice receives the particles S4, Bob tells her the positions where the decoy photons are.

(S4) Alice extracts all the decoy photon pairs from the particles S4, forming a series of qubits S5, and performs a Bell state measurement. If there is

no eavesdropper, every decoy photon pairs should be in the Bell state $|\psi^+\rangle$. Otherwise, the communication stops.

(S5) Define $C0=I$ and $C1=\sigma_z$. Alice performs the coding operation $C0$ or $C1$ on $S5$ with probability $p0$ and $p1$ respectively, and then sends them back to Bob.

(S6) Receiving the encoded particles, Bob performs Bell state measurements on particles from $S2$ and $S5$. Every measurement result should be either $|\psi^+\rangle$ or $|\psi^-\rangle$, which encodes 0 and 1 respectively. Now, the communication ends successfully.

III. THE SPP PROTOCOL

A. The process of SPP protocol

In the protocol in [10], the transmission is managed in batches of N EPR pairs. An advantage of block transmission scheme is that we can check the security of the transmission by measuring some of the decoy photons in the first step, where both Alice and Bob contain a particle sequence at hand, which means that 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 SPP scheme is proposed.

Suppose that the message transmitted is in a sequence $x^N = (x_1, \dots, x_N)$, where $x_i \in \{0,1\}, i = 1,2,\dots,N$.

Define

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad (1)$$

$$|\psi\rangle = \frac{1}{2}(|000000\rangle + |000111\rangle + |111000\rangle - |111111\rangle). \quad (2)$$

Now let us give all the details of SPP scheme.

(S1) Bob prepares a large number of Bell states, inserts enough six-qubit cluster states as follows

(i) Bob prepares a large number (N) of Bell states $|\Phi^+\rangle$ in sequence. He extracts all the first particles in the Bell states, forming a series of particles A (the travel qubits) in order, used to transmit secure message. The remaining particles in the Bell states form a series of particles B (the home qubits). Thus this step corresponds to the message mode in OPP.

(ii) Bob prepares a large number ($cN/(1-c)$) of ordered six-qubit cluster states $|\psi\rangle$ and forms a series of particles C to detect eavesdropping, corresponding to control mode in OPP. Here, c expresses the probability of switching to control mode in the OPP. Note that the particles C includes $6cN/(1-c)$ qubits. Bob inserts particles of six-qubit cluster state to the particles A randomly, forming a new sequence D , which exists decoy photons of six-qubit cluster state, but only Bob knows the positions of decoy photons. Bob stores the particles B and sends the particles D to Alice.

(S2) The eavesdropping detection by Alice

After Alice receives the particles D , Bob tells her the positions where are the decoy photons of six-qubit cluster state in C . Alice extracts the decoy photons from particles D and performs six particles cluster state measurement. If there is no eavesdropper, every result should be in the six particles cluster state, and SPP protocol is keeping on. Otherwise, the communication is interrupted, and the SPP protocol switches to (S1).

(S3) Alice encodes her ciphertext, inserts enough decoy photons of six-qubit cluster states randomly like Bob

Define $C0=I$ and $C1=\sigma_z$. Alice performs the coding operation $C0$ or $C1$ on the remaining particles of D with probability $p0$ and $p1$ respectively,

Alice inserts particles six-qubit cluster state to the particles D randomly, forming a new sequence E , which exists decoy photons of six-qubit cluster state, but only Alice knows the positions of decoy photons. Alice sends E back to Bob.

(S4) The eavesdropping detection by Bob

On receiving particles E , Bob extracts the decoy photons from particles E and performs six-qubit cluster state measurement to ensure the security of the quantum channel, the same as step $S2$. If there is no eavesdropper, Bob starts to decode the ciphertext, and the remaining particles names F . Otherwise, the communication is interrupted, and the SPP protocol stopped.

(S5) Bob decodes the ciphertext

Bob measures the state of the particles B and F in the Bell basis. There are only two possible outcomes of the measurement, $|\psi^+\rangle$ or $|\psi^-\rangle$ which

encodes 0 or 1 respectively. The SPP protocol ends successfully.

B. The security analysis of SPP protocol

In the OPP, the author calculates the maximal amount of the information $I(d|O)$ that Eve can eavesdrop and the probability $d|O$ that Eve is detected. And the function $I(d|O)$ is provided.

$$\text{When } p_0 = p_1 = 1/2, \\ I(d|O) = -d|O \log_2 d|O - (1-d|O) \log_2 (1-d|O). \quad (3)$$

The above method can be used to compare the efficiency of eavesdropping detection among the three protocols.

In the MPP, the maximal amount of the information $I(d|M)$ that Eve can eavesdrop is

$$I(d|M) = H\left(\frac{1-\sqrt{1-2d|M}}{2}\right), \quad (4)$$

where

$$H(x) = -x \log_2 x - (1-x) \log_2 (1-x). \quad (5)$$

and $d|M$ is the probability that Eve is detected.

Now, let us analyze the efficiency of the eavesdropping detection in SPP protocol. In order to gain the information Alice operates on the travel qubits, Eve performs a unitary attack operation $\hat{E}$ on the composed system at first. Then Alice takes a coding operation on the travel qubits. Eve performs a measurement on the composed system at last. Note that, all the transmitted particles are sent as block before detecting eavesdropping, which is different from OPP. For Eve does not know which particles are used to detect eavesdropping, so what she can do is only performing the same attack operation on all the particles. As for Eve, the state of the travel qubits is indistinguishable from the complete mixture, so all the travel qubits are considered in either of the states $|0\rangle$ or $|1\rangle$ with equal probability $p=0.5$.

Generally speaking, suppose that there is a group of decoy photons at the state of six-qubit cluster states $|\psi\rangle$, and after performed the attack operation $\hat{E}$, the states $|0\rangle$ and $|1\rangle$ become

$$|\phi_0'\rangle = \hat{E} \otimes |0x\rangle = \alpha |0x_0\rangle + \beta |1x_1\rangle, \quad (6)$$

$$|\phi_1'\rangle = \hat{E} \otimes |1x\rangle = m |0y_0\rangle + n |1y_1\rangle. \quad (7)$$

where $|x_i\rangle$ and $|y_i\rangle$ are the pure ancillary states only determined by $\hat{E}$ uniquely, and

$$|\alpha|^2 + |\beta|^2 = 1, \quad |m|^2 + |n|^2 = 1. \quad (8)$$

Then let us calculate the detection probability. Attacked by Eve, the state of composed system becomes

$$\begin{aligned} |\psi\rangle_E &= E \otimes E \otimes E \otimes E \otimes E \otimes E \\ &= \left[\frac{1}{2} (|000000\rangle + |000111\rangle + |111000\rangle - |111111\rangle) \right] \\ &= (\alpha |0x_0\rangle + \beta |1x_1\rangle) \otimes (\alpha |0x_0\rangle + \beta |1x_1\rangle) \otimes (\alpha |0x_0\rangle + \beta |1x_1\rangle) \\ &\quad \otimes (\alpha |0x_0\rangle + \beta |1x_1\rangle) \otimes (\alpha |0x_0\rangle + \beta |1x_1\rangle) \otimes (\alpha |0x_0\rangle + \beta |1x_1\rangle) \\ &\quad + (\alpha |0x_0\rangle + \beta |1x_1\rangle) \otimes (\alpha |0x_0\rangle + \beta |1x_1\rangle) \otimes (\alpha |0x_0\rangle + \beta |1x_1\rangle) \\ &\quad \otimes (m |0y_0\rangle + n |1y_1\rangle) \otimes (m |0y_0\rangle + n |1y_1\rangle) \otimes (m |0y_0\rangle + n |1y_1\rangle) \\ &\quad + (m |0y_0\rangle + n |1y_1\rangle) \otimes (m |0y_0\rangle + n |1y_1\rangle) \otimes (m |0y_0\rangle + n |1y_1\rangle) \\ &\quad \otimes (\alpha |0x_0\rangle + \beta |1x_1\rangle) \otimes (\alpha |0x_0\rangle + \beta |1x_1\rangle) \otimes (\alpha |0x_0\rangle + \beta |1x_1\rangle) \\ &\quad - (m |0y_0\rangle + n |1y_1\rangle) \otimes (m |0y_0\rangle + n |1y_1\rangle) \otimes (m |0y_0\rangle + n |1y_1\rangle) \\ &\quad \otimes (m |0y_0\rangle + n |1y_1\rangle) \otimes (m |0y_0\rangle + n |1y_1\rangle) \otimes (m |0y_0\rangle + n |1y_1\rangle) \end{aligned} \quad (9)$$

Obviously, when the measurement is taken on the decoy photons, the probability without eavesdroppers is

$$\begin{aligned} p(|\psi\rangle_E) &= \frac{1}{4} (|\alpha^6|^2 + |\alpha^3\beta^3|^2 + |\alpha^3\beta^3|^2 + |\beta^6|^2 + |\alpha^3m^3|^2 + |\alpha^3n^3|^2 \\ &\quad + |\beta^3m^3|^2 + |\beta^3n^3|^2 + |\alpha^3m^3|^2 + |\alpha^3n^3|^2 + |\beta^3m^3|^2 + |\beta^3n^3|^2 \\ &\quad + |m^6|^2 + |m^3n^3|^2 + |m^3n^3|^2 + |n^6|^2) \\ &= \frac{1}{4} (|\alpha^6|^2 + 2|\alpha^3\beta^3|^2 + |\beta^6|^2 + 2|\alpha^3m^3|^2 + 2|\alpha^3n^3|^2 \\ &\quad + 2|\beta^3m^3|^2 + 2|\beta^3n^3|^2 + |m^6|^2 + 2|m^3n^3|^2 + |n^6|^2) \end{aligned} \quad (10)$$

So the lower bound of the detection probability($d|S$) is

$$d|_S = 1 - p(|\psi\rangle_E). \quad (11)$$

Now, let us analyze how much information Eve can gain maximally when there is no control run.

Suppose that $|\alpha|^2 = a, |\beta|^2 = b, |m|^2 = s, |n|^2 = t$, where a, b, s and t are positive real numbers, and $a+b=s+t=1$. Then

$$\begin{aligned} d|_S &= 1 - \frac{1}{4} (|\alpha^6|^2 + 2|\alpha^3\beta^3|^2 + |\beta^6|^2 + 2|\alpha^3m^3|^2 + 2|\alpha^3n^3|^2 \\ &\quad + 2|\beta^3m^3|^2 + 2|\beta^3n^3|^2 + |m^6|^2 + 2|m^3n^3|^2 + |n^6|^2) \\ &= 1 - \frac{1}{4} (a^6 + 2a^3b^3 + b^6 + 2a^3s^3 + 2a^3t^3 + 2b^3s^3 + 2b^3t^3 + s^6 + 2s^3t^3 + t^6) \\ &= 1 - \frac{1}{4} (3a^2 - 3a + 3t^2 - 3t + 2)^2 \end{aligned} \quad (12)$$

In the case of $p_0=p_1=0.5$, when Bob sends $|0\rangle$ to Alice, the maximal amount of information is equal to the Shannon entropy of a binary channel,

$$I_0 = -a \log_2 a - (1-a) \log_2 (1-a) = H(a) \quad (13)$$

Then assume that Bob sends $|1\rangle$ rather than $|0\rangle$. The above security analysis can be done in full analogy, resulting in the same crucial relations. The maximal amount of information is equal to the Shannon entropy of a binary channel,

$$I_1 = -t \log_2 t - (1-t) \log_2 (1-t) = H(t) \quad (14)$$

So the maximal amount of information Eve can obtain is

$$I = \frac{1}{2}(I_0 + I_1) = \frac{1}{2}[H(a) + H(t)] \quad (15)$$

After some simple mathematical calculations, when $a=t$, we can get

$$d_{IS} = 1 - \left(3a^2 - 3a + 1\right)^2 \quad (16)$$

and the maximum I is

$$I(d_{IS}) = H\left(\frac{3 + \sqrt{-3 + \sqrt{144 - 144d_I}}}{6}\right) \quad (17)$$

The above analysis shows that function $I(d_{IO})$, $I(d_{IM})$ and $I(d_{IS})$ have the similar algebraic properties. If Eve gains full information ($I=1$), the probabilities of eavesdropping detection are d_{IO} ($I=1$) = 0.5 and d_{IM} ($I=1$) = 0.5 in the OPP and the MPP separately, while in the SPP, d_{IS} ($I=1$) = 0.75.

In order to contrast the three functions, Fig.1 and Table I are given. As are shown in Fig.1 and Table I, if Eve gains the same amount of information, she must face a larger detection probability in the SPP than the other two. They also indicate that the SPP is more secure than the other two. Of course, in order to detect eavesdropping, Bob needs send $6cN/(1-c)$ qubits more than the OPP, and send $4cN/(1-c)$ particles more than the MPP. In other words, Bob gains the better security at the cost of sending more particles.

TABLE 1. THE ACCURATE COMPARISON FIGURES

protocol d I/bit	OPP	MPP	SPP
0.2	0.03	0.06	0.17
0.4	0.08	0.15	0.39
0.6	0.15	0.25	0.61
0.8	0.24	0.37	0.80
1.0	0.50	0.50	0.94

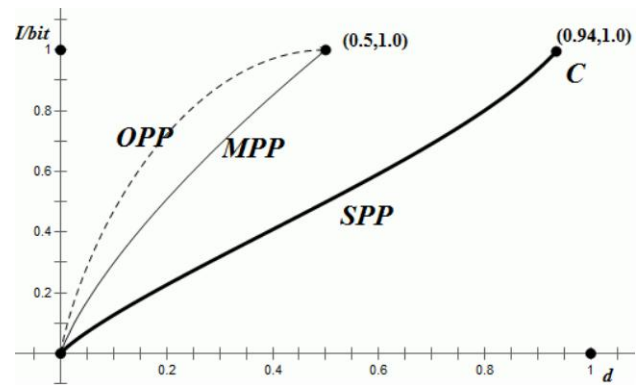


Figure 1. The comparison of the three detection results

In Fig.1, The dotted line expresses the function $I(d_{IO})$ in the OPP, the thin line expresses the function $I(d_{IM})$ in the MPP, and the thick line expresses the function $I(d_{IS})$ in the SPP. Obviously, if Eve wants to get the same amount information, she must encounter the higher detection efficiency in SPP. Also, if there is the same detection efficiency, Eve will eavesdrop less information.

Taking into account probability c in control mode, the effective transmission rate, i.e. the number of message bits per protocol run, is $1-c$, equal to the probability for a message transfer. Thus, if Eve wants to eavesdrop one message transfer without being detected, the probability for this event reads

$$s(c, d) = (1-c) + c(1-d)(1-c) + c^2(1-d)^2(1-c) + \dots = \frac{1-c}{1-c(1-d)} \quad (18)$$

Thus the probability to successfully eavesdrop

$I = nI(d)$ bits reads $s(I, c, d) = s(c, d)^{I/I(d)}$. So

$$s(I, c, d) = \left(\frac{1-c}{1-c(1-d)}\right)^{I/I(d)}, \quad (19)$$

where

$$I(d_{IS}) = H\left(\frac{3 + \sqrt{-3 + \sqrt{144 - 144d_I}}}{6}\right) \quad (20)$$

In the limit $I \rightarrow \infty$ (a message or key of infinite length) we have $s \rightarrow 0$, so the presented protocol in this paper is asymptotically secure. If the security of the quantum channel is ensured, the protocol is completely secure. For example, a choice of the control mode is $c=0.5$. In Fig.2 we have plotted the eavesdropping success probability as a function of the information gain I , for $c=0.5$ and for different detection probabilities d which Eve can choose. Note that for $d < 0.5$, Eve only gets part of the message right and does not even know which part.

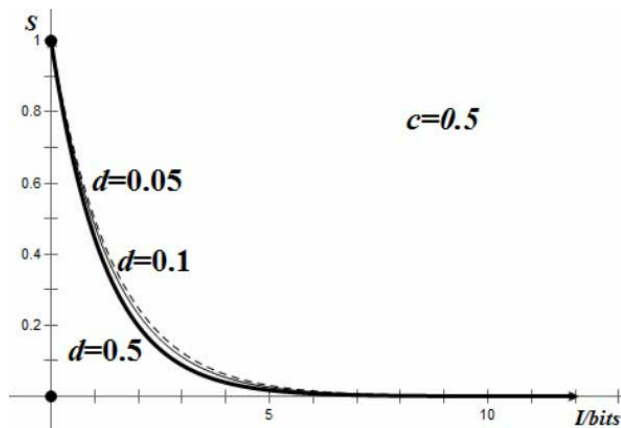


Figure 2. Eavesdropping success probability

IV. CONCLUSIONS

In summary, we have introduced a QSDC protocol using six-qubit cluster state, and three eavesdropping detection strategies are compared quantitatively by using the constraint between the information eavesdropper obtains and the interference introduced. In the analysis, if the eavesdropper obtains the same amount of information, she must face a larger detection probability in the SPP than the other two, which shows that the efficiency of eavesdropping detection in SPP is higher than the other two, so it can ensure the “Ping-pong” protocol more secure. While in order to detect eavesdropping, Bob sends $6cN/(1-c)$ particles more than the OPP, and $4cN/(1-c)$ qubits more than the MPP. That is, Bob gains the better security at the cost of sending more particles. However, suppose that there are 600 decoy photons used in eavesdropper detection, the proposed protocol only needs to send 100 six-qubit cluster states, while the MPP used two particles of EPR pair as detection particles must send 300 EPR pairs. That is, the proposed protocol, which seems that has low efficient and complex in qubit transportation, is more efficient and convenient indeed. In the further work, the other QSDC protocol's security and its improvement will be researched.

ACKNOWLEDGMENT

This work is supported by National Key R&D Program of China (2017YFB0801900).

REFERENCES

- [1] C. H. Bennett, G. Brassard, “Quantum cryptography: Public-key distribution and coin tossing,” Proceeding of the IEEE International Conference on Computer, Systems and Signal Processing, Bangalore, 1984, 175-179.
- [2] Y. H. Kim, S. P. Kulik, Y. Shih, “Quantum teleportation with a complete Bell state measurement,” Quantum Electronics and Laser Science Conference, 2001, 223.
- [3] H. Prakash, “Quantum Teleportation,” International Conference on Emerging Trends in Electronic and Photonic Devices and Systems, 2009.
- [4] A. Furusawa, “Quantum teleportation and quantum information processing,” Quantum Electronics and Laser Science Conference, 2010.
- [5] C. H. Bennett, S. J. Wiesne, “Communication via one and two particle operators on Einstein-Podolsky-Rosen states,” Phys. Rev. Lett., 1992, 69, 2881.
- [6] K. Mattle, H. Weinfurter, P. G. Kwiat, A. Zeilinger, “Dense coding in experimental quantum communication,” Phys. Rev. Lett., 1996, 76, 25.
- [7] K. Shimizu, N. Imoto, “Communication channels secured from eavesdropping via transmission of photonic Bell states,” Phys. Rev. A, 1999, 60, 157-166.
- [8] A. Beige, B. G. Englert, C. Kurtsiefer, H. Weinfurter, “Secure communication with a publicly known key,” Acta Phys. A, 2002, 101, 357.
- [9] K. Boström, T. Felbringer, “Deterministic secure direct communication using entanglement,” Phys. Rev. Lett., 2002, 89, 187902.
- [10] G. L. Long, X. S. Liu, “Theoretically efficient high-capacity quantumkey-distribution scheme,” Phys. Rev. A, 2002, 65(3), 032302.
- [11] F. G. Deng, G.L. Long, X.S. Liu, “Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block,” Phys. Rev. A, 2003, 68, 042317.
- [12] F. G. Deng, G.L. Long, “Secure direct communication with a quantum one-time pad,” Phys. Rev. A, 2004, 69, 052319.
- [13] F. Gao, F. Z. Guo, Q. Y. Wen, F.C. Zhu, “Comparing the efficiency of different detection strategies of the ‘Ping-pong’ protocol,” Sci. China Ser G-Phys Mech. Astron, 2009, 39(2), 161-166.
- [14] R. Matsumoto, “Multiparty quantum-key-distribution protocol without use of entanglement,” Phys. Rev. A, 2007, 76(6), 2316.
- [15] W. Liu, Y. B. Wang, X. M. Wang, “Multi-party Quantum Private Comparison Protocol Using d-Dimensional Basis States Without Entanglement Swapping,” Int. J. Theor. Phys., 2014, 53(4), 1085-1091.
- [16] F. Zarmehi, M. Houshmand, “Controlled Bidirectional Quantum Secure Direct Communication Network Using Classical XOR Operation and Quantum Entanglement,” IEEE COMMUN LETT, 2016, 20(10), 2071-2074.
- [17] C. H. Chang, C. W. Yang, G. R. Hzu, “Quantum dialogue protocols over collective noise using entanglement of GHZ state,” QUANTUM INFORMATION PROCESSING, 2016, 15(7), 2971-2991.
- [18] J. R. Cai, Z. W. Pan, T.J. Wang, “High-capacity quantum secure direct communication using hyper-entanglement of photonic qubits,” INT J QUANTUM INF, 2016, 14(8), 1650043.
- [19] A. Anshu, R. Jain, P. Mukhopadhyay, “New One Shot Quantum Protocols With Application to Communication Complexity,” IEEE Trans. Inf. Theory, 2016, 62(12), 7566-7577.
- [20] B. S. Choudhury, A. Dhara, “An entanglement concentration protocol for cluster states using CNOT gate operation,” PRAMANA-JOURNAL OF PHYSICS, 2016, 86(5), 973-983.
- [21] N. Li, J. Li, L. L. Li, “Deterministic Secure Quantum Communication and Authentication Protocol based on Extended GHZ-W State and Quantum One-time Pad,” Int. J. Theor. Phys., 2016, 55(8), 3579-3587.
- [22] X. H. Li, “Quantum secure direct communication,” ACTA PHYSICA SINICA, 2015, 64(16), 160307.
- [23] T. Hwang, Y. P. Luo, “Probabilistic authenticated quantum dialogue,” QUANTUM INF PROCESS, 2015, 14 (12), 4631-4650.
- [24] P. Zawadzki, “Eavesdropping on quantum secure direct communication in quantum channels with arbitrarily low loss rate,” QUANTUM INF PROCESS, 2016, 15 (4), 1731-1741.
- [25] A. Nepeivoda, “Ping-pong protocols as prefix grammars: Modelling and verification via program transformation,” J LOG ALGEBRA METHODS, 2016, 85(5), 782-804.
- [26] P. Zawadzki, J. A. Miszczak, “A General Scheme for Information Interception in the Ping-Pong Protocol,” ADVANCES IN MATHEMATICAL PHYSICS, 2016, 3162012.
- [27] J. Li, N. Li, L. L. Li, “One Step Quantum Key Distribution Based on EPR Entanglement,” SCIENTIFIC REPORTS, 2016, 28767.

- [28] Z. W. Cao, G. Zhao, S. H. Zhang, "Quantum secure direct communication protocol based on the mixture of Bell state particles and single photons," ACTA PHYSICA SINICA, 2016, 65(23), 230301.
- [29] H. Hoffmann, K. Boström, T. Felbinger, "Comment on 'Secure direct communication with a quantum one-time pad'," Phys.Rev. A, 2005, 72, 016301.
- [30] F. G. Deng, G.L. Long, "Reply to 'Comment on 'Secure direct communication with a quantum one-time pad'," Phys. Rev. A, 2005, 72, 016302.
- [31] F. G. Deng, X. H. Li, C. Y. Li, P. Zhou, H. Y. Zhou "Quantum secure direct communication network with Einstein-Podolsky-Rosen pairs," Phys. Lett. A, 2006, 359, 359-365.



Danjie Song is a Network Security R&D Engineer of Computer Network Information Center, Chinese Academy of Sciences, interested in research on cybersecurity security, information security, quantum communication security, cybersecurity situational awareness, big data analysis. (Email: songdanjie@cnic.cn)



Chun Long Ph.D., Senior Engineer of Computer Network Information Center, Chinese Academy of Sciences, CISSP, interested in exploration and research on frontier of cyberspace security technology, and has made breakthroughs in the research of cybersecurity situational awareness, secure big data mining and analysis, and has made innovation and improvement in key technologies such as aggregation of security events, multi-source secure data fusion and composite attack prediction. He received Ph.D. degrees from University of Chinese Academy of Sciences in 2015, B.S. degrees from Huazhong University of Science and Technology in 2004, and M.S. degrees from Huazhong University of Science and Technology in 2001. (Email: longchun@cnic.cn)

from Huazhong University of Science and Technology in 2004, and M.S. degrees from Huazhong University of Science and Technology in 2001. (Email: longchun@cnic.cn)



Wei Wan Ph.D., Senior Engineer of Computer Network Information Center, Chinese Academy of Sciences, CISA, interested in research on network security, cloud computing security, cybersecurity situational awareness. He received Ph.D. degrees from University of Chinese Academy of Sciences in 2015, B.S. degrees from Beijing Information Technology Institute in 2004, and M.S. degrees from Graduate University of Chinese Academy of Sciences in 2007. (Email: wanwei@cnic.cn)



Jing Zhao Ph.D. candidate, Network Security R&D Engineer of Computer Network Information Center, Chinese Academy of Sciences, PMP, interested in cybersecurity and system security research and project management. She received B.S. degrees from Beijing University of Posts and Telecommunications in 2009 and M.S. degree from Beijing University of Posts and Telecommunications in 2012. (Email: jingzhao@cnic.cn)



Shaojie Wang is a Network Security R&D Engineer of Computer Network Information Center, Chinese Academy of Sciences, interested in research on cybersecurity and next generation network architecture. He received M.S. degrees in Computer Science and Technology from University of Chinese Academy of Sciences in 2015. (Email: wangshaojie@cnic.cn)