Cryptanalysis of Controlled Bidirectional Quantum Secure Direct Communication Network Using Classical XOR Operation and Quantum Entanglement

Zhihao Liu and Hanwu Chen

***Abstract*— The multi-user controlled bidirectional quantum secure direct communication network protocol based on classical EXCLUSIVE-OR operation and quantum entanglement is analyzed. It is shown that this protocol has the information leakage problem, that is, one half of the information the users transmit is leaked out unconsciously. Furthermore, it is also weak against the intercept-measure-resend attack and the Controlled-Not operation attack from an outside adversary, and the different initial state attack from the controller.**

***Index Terms*— Bidirectional quantum secure direct communication, information leakage, intercept-measure-resend attack, Controlled-Not operation attack, different initial state attack.**

I. Introduction

TO ENSURE the security of stored or communicated data in a public environment such as the cloud computing and big data environments [1]–[8], an efficient way is to encrypt the data with a private key or to use information hiding techniques [9], [10]. Since the first quantum key distribution (QKD) protocol was put forward by Bennett and Brassard [11] in 1984, it has been developing quickly [12], [13]. Afterwards, another branch of quantum cryptography called quantum secure direct communication (QSDC) [14] was put forward and has attracted significant attention [15]. Different from QKD, QSDC allows that the sender directly transmits the secret or the deterministic key (instead of a random key) to the receiver in a deterministic and secure manner. In 2004, the concept of bidirectional QSDC (BQSDC) or quantum dialogue (QD) was proposed [16] and followed by some researchers. However, they usually have information leakage problems [17]–[20]. Therefore, researchers have proposed BQSDC protocols without information leakage [21], [22].

Recently, a novel multi-user controlled BQSDC (CBQSDC) network protocol based on cluster states was proposed [23]. In this protocol, four users can exchange their secret messages two by two under the permission of a controller. The quantum channel is only used for sharing the qubits, and no encoded photons are transmitted via the quantum channel, which decreases the economic cost of communication and the effect of channel noise on the secret messages. Besides, this protocol works with single-photon measurement which is easier to implement than other measurements. The authors also claimed that this protocol is unconditionally secure and has higher efficiency than previously proposed protocols. However, if it is considered carefully, there are security problems in this protocol. To be specific, the information leakage problem exists in this protocol. It is also fragile against the intercept-measure-resend attack [24], [25] and the Controlled-Not (CNOT) operation attack [25] by an outside adversary. In addition, the controller can make an effective attack, the so-called different initial state attack [26], to gain all the messages the users transmitted. In the following, we will explain the reasons in detail.

Manuscript received April 8, 2017; revised June 12, 2017; accepted June 16, 2017. Date of publication June 30, 2017; date of current version October 7, 2017. This work was supported in part by the National Natural Science Foundation of China under Grant 61502101 and Grant 61170321, in part by the Natural Science Foundation of Jiangsu Province, China, under Grant BK20140651 and Grant BK20140823, and in part by PAPD, in part by CICAEET, and in part by China Scholarship Council. This work was partially done when Z. Liu was visiting the Centre for Quantum Software and Information, Faculty of Engineering and Information Technology, University of Technology Sydney, Ultimo, NSW 2007, Australia. The associate editor coordinating the review of this letter and approving it for publication was M. F. Flanagan. *(Corresponding author: Zhihao Liu.)*

The authors are with the School of Computer Science and Engineering, Southeast University, Nanjing 211189, China, and also with the Key Laboratory of Computer Network and Information (Southeast University), Ministry of Education, Nanjing 211189, China (e-mail: liuzhtopic@163.com).

Digital Object Identifier 10.1109/LCOMM.2017.2721952

II. The Original CBQSDC Network Protocol

First we review the original CBQSDC protocol. There are four users, Alice1, Alice2, Bob1 and Bob2, and a controller Charlie who is also the reference node. The original CBQSDC network protocol is described as follows.

Step 1: Alice1 and Bob1 build a connection, and Alice2 and Bob2 build another connection as well with Charlie being the common controller. Charlie creates $2N+\delta$ numbers of ordered four-qubit cluster states, in which the i-th state is

$$|o.)_{a_i b_i c_i d_i} = \frac{1}{2}(|0000) + |0101) + |1010) - |1111))_{a_i b_i c_i d_i}, \quad (1)$$

where the subscripts a, b, c and d indicate four correlated photons of the cluster state. Then Charlie randomly selects $2N$ numbers of these cluster states as information carriers and he randomly performs the unitary operations $I = |0)(0| + |1)(1|$ or $X = |0)(1| + |1)(0|$ on the first and the second photons of these cluster states. The remaining δ numbers of cluster states will be used as the sample.

Step 2: Charlie sorts all the particles a, b, c and d to form the A-sequence, the B-sequence, the C-sequence and the D-sequence, and sends them to Alice1, Alice2, Bob1 and Bob2, respectively.

Step 3: Charlie announces the positions of the sample photons in each divided sequence. Meanwhile, he randomly selects one of the two measurement bases, the B_Z basis

$\{|0\rangle, |1\rangle\}$ or the B_X basis $= \{|+\rangle, |-\rangle\} = 1/\sqrt{2}\,(|0\rangle \pm |1\rangle)$, and tells the users to apply the same bases to measure the sample photons. Then all the users compare their results to analyze the error rate. If it is greater than the threshold, the communication will stop. Otherwise, it will continue.

Step 4: After dropping the sample photons that are used for eavesdropping check in each divided sequence, each user makes N numbers of two-photon groups. For example, (a_{2n-1}, a_{2n}), (b_{2n-1}, b_{2n}), (c_{2n-1}, c_{2n}) and (d_{2n-1}, d_{2n}) are the n-th two-photon group of Alice1, Alice2, Bob1 and Bob2.

Step 5: All users measure their photons in the B_Z basis and save the results. Then they use classical XOR operations to encode their secret messages with these results. That is, having taken two bits of the saved measurement results as the first inputs and two bits of the secret message as the second inputs, each user applies XOR operations. After that, they publish their XOR results through a classical channel.

Step 6: Charlie announces the unitary operations that he has performed on the first and the second photons of the information-carrier cluster states in Step 1. That is, if he performs II, IX, XI, XX, he will publish "00", "01", "10", "11", respectively.

Step 7: Each user obtains the counterparty's secret message. Since each user has three kinds of bits: The published bits of Charlie, the published bits of his/her counterparty and the bits which have been obtained in Step 5 as the saved measurement results of the photons. For decoding the messages, each user applies the classical XOR operations on all these bits, bit by bit. For example, if Charlie publishes the bits "01", Alice1 publishes the bits "11" and Bob1 obtains the bits "10" by measuring the photons, the final results will be "00" $(01 \oplus 11 \oplus 10 = 00)$. Thus Bob1 gets Alice1's secret bits "00".

III. Information Leakage Problem

At first glance, eight bits of classical information in all are exchanged at the cost of two four-qubit cluster states. However, if it is considered carefully, one can find that one half of the information is leaked out unconsciously. In the following, we give an example to explain the reason. Without loss of generality, we take the first two cluster states $|o.\rangle_{a_1b_1c_1d_1}$ and $|o.\rangle_{a_2b_2c_2d_2}$ which are used as the information carriers as an example. Suppose that Charlie performs unitary operations on the first and the second photons of these two cluster states, denoted by $X^u_{a_1}$, $X^v_{b_1}$, $X^x_{a_2}$ and $X^y_{b_2}$, respectively. After that, the whole state of these two four-qubit cluster states can be expressed as

$$X^u_{a_1} \otimes X^v_{b_1} \otimes X^x_{a_2} \otimes X^y_{b_2} \, |o.\rangle_{a_1b_1c_1d_1} \otimes |o.\rangle_{a_2b_2c_2d_2}$$

$$= \frac{1}{2} \sum_{i,j=0}^{1} (-1)^{i \cdot j} |i \oplus u, j \oplus v, ij\rangle_{a_1b_1c_1d_1}$$

$$\otimes \frac{1}{2} \sum_{i,j=0}^{1} (-1)^{k \cdot l} |k \oplus x, l \oplus y, kl\rangle_{a_2b_2c_2d_2}$$

In Step 5, all the users should measure his/her two qubits in the B_Z basis. Let Alice1's, Alice2's, Bob1's, Bob2's measurement results be (α_1, α_2), (β_1, β_2), (χ_1, χ_2) and (δ_1, δ_2), respectively. According to the above equation, we know that the following relationships hold.

$$\alpha_1 = \chi_1 \oplus u, \quad \alpha_2 = \chi_2 \oplus x, \; \beta_1 = \delta_1 \oplus v, \; \beta_2 = \delta_2 \oplus y.$$

Assume Alice1's Alice2's, Bob1's, Bob2's two-bit secret message be (k_1, k_2), (l_1, l_2), (m_1, m_2), (n_1, n_2) respectively. Then they will publish two classical bits $(\alpha_1 \oplus k_1, \alpha_2 \oplus k_2)$, $(\beta_1 \oplus l_1, \beta_2 \oplus l_2)$, $(\chi_1 \oplus m_1, \chi_2 \oplus m_2)$, $(\delta_1 \oplus n_1, \delta_2 \oplus n_2)$ respectively in Step 5. After Charlie announces the values of u, v, x, y in Step 6, each user can get the counterpart's two-bit secret. For example, Alice1 can get Bob1's secret (m_1, m_2) by $\alpha_1 \oplus (\chi_1 \oplus m_1) \oplus u = m_1, \alpha_2 \oplus (\chi_2 \oplus m_2) \oplus x = m_2$. However, if considering carefully, we can find that anyone can get some information about the secret messages from the public information that all the users and Charlie announce. It is obvious that everyone knows that $(\alpha_1 \oplus k_1) \oplus (\chi_1 \oplus m_1) \oplus u = k_1 \oplus m_1$, $(\alpha_2 \oplus k_2) \oplus (\chi_2 \oplus m_2) \oplus x = k_2 \oplus m_2$, $(\beta_1 \oplus l_1) \oplus (\delta_1 \oplus n_1) \oplus v = l_1 \oplus n_1$, and $(\beta_2 \oplus l_2) \oplus (\delta_2 \oplus n_2) \oplus y = l_2 \oplus n_2$. That is to say, one half of the secret messages have been leaked out. This is not allowed in a truly secure quantum communication protocol.

IV. The Intercept-Measure-Resend Attack and the CNOT Operation Attack by an Outside Adversary

Indeed, one of the two bases, the B_Z basis and the B_X basis, is randomly used to measure the four-qubit sample cluster states. The method is usually effective because these two bases are conjugated. However, it is useless against the intercept-measure-resend attack by an outside adversary. In the following, we explain the reason. Assume Eve is the outside adversary who will make the intercept-measure-resend attack. After Charlie sends the four sequences, the A-sequence, the B-sequence, the C-sequence and the D-sequence out, Eve catches the A-sequence and the B-sequence (or the C-sequence and D-sequence), measures each sequence with the B_Z basis photon by photon, and then prepares a new fake sequence according to the results. Then Eve sends these two fake sequences to Alice1 and Alice2 (or Bob1 and Bob2) respectively. Obviously, if a sample four-qubit cluster state is intended to be measured by the B_Z basis, no error will be introduced because Eve prepares the fake sequences in the B_Z basis as well according to the measurement results. One may hope that there is a positive probability to detect this kind of attack when a sample four-qubit cluster state is intended to be measured by the B_X basis. However, we find that the users cannot detect the attack, even if this basis is used. In the following, we explain the reason in detail. As we know,

$$|o.\rangle_{a_ib_ic_id_i} = \frac{1}{2}(|0000\rangle + |0101\rangle + |1010\rangle - |1111\rangle)_{a_ib_ic_id_i}$$

$$\frac{1}{1} \sum_{1}^{1}$$

$$= \frac{1}{4}\{|+\rangle|+\rangle|+\rangle|+\rangle + |+\rangle|-\rangle|+\rangle|+\rangle + |-\rangle|+\rangle|+\rangle|+\rangle$$
$$- |-\rangle|-\rangle|+\rangle|+\rangle + |+\rangle|+\rangle|-\rangle|+\rangle - |+\rangle|-\rangle|-\rangle|+\rangle$$
$$+ |-\rangle|+\rangle|-\rangle|+\rangle + |-\rangle|-\rangle|-\rangle|+\rangle + |+\rangle|+\rangle|+\rangle|-\rangle$$
$$+ |+\rangle|-\rangle|+\rangle|-\rangle - |-\rangle|+\rangle|+\rangle|-\rangle + |-\rangle|-\rangle|+\rangle|-\rangle$$
$$- |+\rangle|+\rangle|-\rangle|-\rangle + |+\rangle|-\rangle|-\rangle|-\rangle + |-\rangle|+\rangle|-\rangle|-\rangle$$
$$+ |-\rangle|-\rangle|-\rangle|-\rangle\}_{a_i b_i c_i d_i}, \quad (3)$$

$$= \frac{1}{4}\sum_{i,j,k,l=0}^{4} (-1)^{i\cdot j+k\cdot l}\,|i \oplus u, k \oplus x, j \oplus v, l \oplus y\rangle_{a_1 a_2 b_1 b_2}$$
$$\otimes |ikjl\rangle_{c_1\ c_2 d_1 d_2} \quad (2)$$

so there are sixteen possible measurement results in all and each result has the same probability to appear if a four-qubit cluster state $|o.)_{a_i b_i c_i d_i}$ is measured by using the B_X basis. When this four-qubit cluster state is replaced with one of the four-qubit states in the B_Z basis ($|0000)_{a_i b_i c_i d_i}$,$|0101)_{a_i b_i c_i d_i}$, $|1010)_{a_i b_i c_i d_i}$ and $|1111)_{a_i b_i c_i d_i}$), and all the users utilize the B_X basis to measure this state, there are also sixteen possible results of which each has the same probability to appear. That is, the two distributions about the respective measurement results are identical. As a result, Eve's attack cannot be detected by the users. For the four-qubit cluster states which are used as information carriers, all the users utilize the B_Z basis to measure them. This means that Eve can obtain Alice1's and Bob1's measurement results in Step 5. After Charlie publishes the information about the random operations performed on these states, Eve can get all the users' results in Step 5, and thus she can gain all the secret messages.

In fact, Eve can make another attack, the so-called CNOT operation attack, to steal the secret messages without being detected. As for the CNOT attack, Eve prepares two ancilla sequences, the E-sequence and the F-sequence, in which all the states stay in $|0)$. After Charlie sends the four sequences, the A-sequence, the B-sequence, the C-sequence and the D-sequence out, Eve captures the A-sequence and the B-sequence (or the C-sequence and D-sequence), and makes CNOT operations on the A-sequence and the E-sequence, as well as on the B-sequence and the F-sequence (or on the C-sequence and the E-sequence, and on the D-sequence and the F-sequence) with photons from the A-sequence and the B-sequence being the control qubits (or with photons from the C-sequence and the D-sequence being the control qubits). Then Eve resends the A-sequence and the B-sequence to Alice1 and Alice2, and measures the E-sequence and the F-sequence with the B_Z basis. If the i-th four-qubit cluster state is a sample, the whole state will be

$$|o.)_{a_i b_i c_i d_i e_i f_i} = \frac{1}{2}(|0000)|00) + |0101)|01) + |1010)|10) - |1111)|11))_{a_i b_i c_i d_i e_i f_i}, \quad (4)$$

after a CNOT operation is performed on the photon a_i and the ancilla e_i as well as on the photon b_i and the ancilla f_i. After Eve measures the ancillas e_i and f_i with the B_Z basis, this four-qubit cluster state is replaced with one of the four-qubit states in the B_Z basis ($|0000)_{a_i b_i c_i d_i}$,$|0101)_{a_i b_i c_i d_i}$, $|1010)_{a_i b_i c_i d_i}$ and $|1111)_{a_i b_i c_i d_i}$). Obviously, no error will be introduced if this sample state will be intended to be measured in the B_Z basis. If the users utilize the B_X basis to measure this state, the situation is the same as that in the intercept-measure-resend attack. So they cannot find any exception.

If the i-th four-qubit cluster state is an information carrier, Eve can obtain the secret bits the users transmit. Assume the unitary operations Charlie performs on the first and the second photons of this state are X_a^u ^{b_i} and X^v ^{i} becomes

$$CNOT_{a\,e}\;{}_{b\,f}\;{}^{u}\;{}^{v}\;X \otimes X\;|o.)\;|0)\;|0)$$
$$\;{}^{i}\;{}_{i}CNOT_{i}\;(\;)$$
$$\frac{1}{2}\;{}^{1}\;{}_{i}\;{}_{a_i}\;{}_{b_i}\;{}_{a_i b_i c_i d_i}\;{}_{e_i}\;{}_{f_i}$$
$$= \frac{1}{2}\sum_{i,j=0}(-1)^{i\cdot j}\;|i \oplus u, j \oplus v, ij)_{a\,b\,c\,d}\,|i \oplus u, j \oplus v)_{e\,f}. \quad (5)$$

That is, Eve copies Alice1's and Alice2's measurement results on photons a_1 and b_1 by measuring the ancilla e_i and f_i, respectively. After Charlie publishes the information about the random unitary operations performed on this cluster state, Eve can get all the users' measurement results. As a result, Eve can gain all the secret messages without being detected.

V. The Different Initial State Attack by the Controller

Charlie is the controller and the reference node who prepares the four-qubit cluster states, so he should be prevented from stealing some information without being detected. However, in the original CBQSDC protocol, if Charlie is dishonest, he can successfully attack the protocol and steal all the information the users want to send with the different initial state attack. The attack strategy is as follows.

The δ numbers of sample cluster states used for eavesdropping check are chosen by Charlie, so he knows which four-qubit cluster states are used as information carriers. To make an efficient attack, Charlie prepares each information-carrier cluster state in the fake state $|o.)_{a_i b_i c_i d_i e_i f_i}$ instead of $|o.)_{a_i b_i c_i d_i}$, where e, f are two ancilla photons which will be kept in Charlie's laboratory. Then the dishonest controller acts as an honest controller would, i.e., he performs the random unitary operations I or X on the first and the second photons of these fake states. After that, he sends all the particles a, b, c and d to Alice1, Alice2, Bob1 and Bob2 respectively, but keeps the ancillas e and f in his laboratory. For a sample state, Charlie complies with the protocol. Obviously, the dishonest Charlie's action cannot be discovered by the users because he only takes actions on what are information carriers but he performs the same actions as an honest controller when a state is used for eavesdropping check.

To steal the messages the users intend to exchange, Charlie measures ancillas e and f in the B_Z basis and saves the results. It is obvious that Charlie's measurement results of particles e and f are identical to those of the particles c and d. Since the random unitary operations on the particles a and b are determined by him, he can extract all the users' secret messages when they publish the XOR results in Step 5.

VI. Conclusion

In summary, the multi-user CBQSDC network protocol based on classical XOR operation and quantum entanglement is analyzed. It is shown that this protocol has the information leakage problem, that is, one half of the information the users transmit is leaked out unconsciously. Furthermore,

respectively.

it is also weak against the intercept-measure-resend attack

After a CNOT operation on the qubits a_i and e_i, as well as on the qubits b_i and f_i respectively, the whole state

and the CNOT operation attack from an outside adversary. Additionally, a dishonest controller can make the different

initial state attack to obtain the users' secret messages without being detected.

REFERENCES

[1] Z. Fu, X. Sun, Q. Liu, L. Zhou, and J. Shu, "Achieving efficient cloud search services: Multi-keyword ranked search over encrypted cloud data supporting parallel computing," *IEICE Trans. Commun.*, vol. E98-B, no. 1, pp. 190–200, Jan. 2015.

[2] Z. Fu, F. Huang, X. Sun, A. Vasilakos, and C.-N. Yang, "Enabling semantic search based on conceptual graphs over encrypted outsourced data," *IEEE Trans. Services Comput.*, to be published, doi: 10.1109/TSC.2016.2622697.

[3] Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, "Enabling personalized search over encrypted outsourced data with efficiency improvement," *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 9, pp. 2546–2559, Sep. 2016.

[4] Z. Fu, X. Wu, C. Guan, X. Sun, and K. Ren, "Toward efficient multi-keyword fuzzy search over encrypted outsourced data with accuracy improvement," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 12, pp. 2706–2716, Dec. 2016.

[5] Q. Liu, W. Cai, J. Shen, Z. Fu, X. Liu, and N. Linge, "A speculative approach to spatial-temporal efficiency with multi-objective optimization in a heterogeneous cloud environment," *Secur. Commun. Netw.*, vol. 9, no. 17, pp. 4002–4012, Nov. 2016.

[6] Z. Xia, X. Wang, X. Sun, and Q. Wang, "A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data," *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 2, pp. 340–352, Jan. 2016.

[7] Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren, "A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 11, pp. 2594–2608, Nov. 2016.

[8] Y. Kong, M. Zhang, and D. Ye, "A belief propagation-based method for task allocation in open and dynamic cloud environments," *Knowl.-Based Syst.*, vol. 115, pp. 123–132, Jan. 2017.

[9] X. Chen, S. Chen, and Y. Wu, "Coverless information hiding method based on the chinese character encoding," *J. Internet Technol.*, vol. 18, no. 2, pp. 313–320, Mar. 2017.

[10] C. Yuan, Z. Xia, and X. Sun, "Coverless image steganography based on SIFT and BOF," *J. Internet Technol.*, vol. 18, no. 2, pp. 435–442, Mar. 2017.

[11] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput., Syst. Signal Process.*, Bangalore, India, Dec. 1984, pp. 175–179.

[12] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145–195, Mar. 2002.

[13] H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nature Photon.*, vol. 8, no. 8, pp. 595–604, Jul. 2014.

[14] L. Gui-lu, D. Fu-guo, W. Chuan, L. Xi-Han, W. Kai, and W. Wan-Ying, "Quantum secure direct communication and deterministic secure quantum communication," *Frontiers Phys. China*, vol. 2, no. 3, pp. 251–272, 2007.

[15] X.-H. Li, "Quantum secure direct communication," (in Chinese), *Acta Phys. Sinica*, vol. 64, no. 16, p. 0160307, Aug. 2015.

[16] B. A. Nguyen, "Quantum dialogue," *Phys. Lett. A*, vol. 328, no. 1, pp. 6–10, Jul. 2004.

[17] F. Gao, F. Guo, Q. Wen, and F. Zhu, "Revisiting the security of quantum dialogue and bidirectional quantum secure direct communication," *Sci. China G, Phys. Mech. Astron.*, vol. 51, no. 5, pp. 559–566, May 2008.

[18] Y.-G. Tan and Q.-Y. Cai, "Classical correlation in quantum dialogue," *Int. J. Quantum Inf.*, vol. 6, no. 2, pp. 325–329, Apr. 2008.

[19] Z. Liu, H. Chen, and W. Liu, "Cryptanalysis of controlled quantum secure direct communication and authentication protocol based on five-particle cluster state and quantum one-time pad," *Int. J. Theor. Phys.*, vol. 55, no. 10, pp. 4564–4576, Oct. 2016.

[20] Z.-H. Liu, H.-W. Chen, and W.-J. Liu, "Information leakage problem in high-capacity quantum secure communication with authentication using Einstein–Podolsky–Rosen pairs," *Chin. Phys. Lett.*, vol. 33, no. 7, p. 070305, Jul. 2016.

[21] T.-Y. Ye, "Fault-tolerant authenticated quantum dialogue using logical Bell states," *Quantum Inf. Process.*, vol. 14, no. 9, pp. 3499–3514, Sep. 2015.

[22] T.-Y. Ye, "Quantum secure direct dialogue over collective noise channels based on logical Bell states," *Quantum Inf. Process.*, vol. 14, no. 4, pp. 1487–1499, Apr. 2015.

[23] F. Zarmehi and M. Houshmand, "Controlled bidirectional quantum secure direct communication network using classical XOR operation and quantum entanglement," *IEEE Commun. Lett.*, vol. 20, no. 10, pp. 2071–2074, Oct. 2016.

[24] Z.-H. Liu, H.-W. Chen, D. Wang, and W.-Q. Li, "Cryptanalysis and improvement of three-particle deterministic secure and high bit- rate direct quantum communication protocol," *Quantum Inf. Process.*, vol. 13, no. 6, pp. 1345–1351, Jun. 2014.

[25] Z.-H. Liu and H.-W. Chen, "Cryptanalysis and improvement of quantum broadcast communication and authentication protocol with a quantum one-time pad," *Chin. Phys. B*, vol. 25, no. 8, p. 080308, Aug. 2016.

[26] C. A. Yen, S. J. Horng, H. S. Goan, T. W. Kao, and Y. H. Chou, "Quantum direct communication with mutual authentication," *Quantum Inf. Comput.*, vol. 9, nos. 5–6, pp. 376–394, May 2009.