One Division-Multiplexed of Control Code Based on Quantum Secure Direct Communication

Jinlong Liu, Zhilu Wu(✉), and Jianbo Zhao

School of Electronics and Information Engineering, Harbin Institute of Technology,
Harbin 150006, China
{yq20,wuzhilu,zhaojianbo}@hit.edu.cn

Abstract. As a subject of the quantum information science, Quantum Secure Direct Communication (QSDC) has been different from Quantum Key Distribution (QKD), QSDC makes the cryptograph to be transmitted directly in the quantum channel. Quantum non-cloning theorem and the indeterminacy principle insure its security. So QSDC has an important research value for the quantum communication. This letter proposed one division-multiplexed of the control code based on QSDC, the simulation is realized, utilizes the division-multiplexed of the control code to encrypt the quantum subsequence, and further improves the security. Two steps of the quantum communication are optimized to be one step. The division-multiplexed of the control code improves the efficiency of QSDC.

Keywords: QSDC · Division-multiplexed · Control code
Order-rearrangement

1 Introduction

Long and Liu firstly proposes Quantum Secure Direct Communication: Efficient two-step-quantum-QSDC, then the scientists take the advantage of Single-Photon, Polarization-entangled twin photons, Quantum teleportation is proposed for QSDC [1]. The literatures on Quantum Secure Direct Communication in recent five years are summarized and analyzed, the theoretical research of QSDC towards system utility, how to simplify the procedure and how to improve the efficiency become the innovation and the research focus, so how to solve these two problems is the key method for QSDC. The researchers on the study propose Measuring-Base-Encryption Quantum Key Distribution (MBE-QKD) and Quantum Key Distribution based on the controlled order rearrangement encryption (CORE-QKD) [2–6]. The core concepts of two methods both are that how to use the control code, this paper proposes one division-multiplexed of the control code on the architecture of Quantum Secure Direct Communication.

1.1 Advantages of Using QSDC

QSDC directly transmits both the secret key and the cryptograph in the quantum channel to achieve a higher security, but QKD only sends the quantum key with quantum

C. Li and S. Mao (Eds.): WiCON 2017, LNICST 230, pp. 396–404, 2018.
https://doi.org/10.1007/978-3-319-90802-1_35

channel, the cryptograph transmission also depends on the classical electromagnetic channel. The research based on quantum secure direct communication can break away from the current situation that QKD is subject to the classical security communication. QSDC is fit for transmitting confidential information in some emergencies, for example, the power grid where is an attack needs the secure and instant communication. QSDC is beneficial to simplify Distributed Blind Quantum Computation (DBQC).

1.2 Measuring Base Encryption-QKD

Measuring-Base-Encryption Quantum Key Distribution (MBE-QKD) of Hwang, Koh and Han improved BB84-QKD, as both communication sides, Alice and Bob first create a bunch of random binary number password as the control code, the code-length was N_k. Under the action of the control node, both Alice selects the measurement basic to encrypt the polarization states, Bob also selects the same measurement basic to demodulate these polarization states. Therefore, under the environment of noise-free and no eavesdropping, Bob can accurately receive the encrypted message from Alice [7–9]. Because Eve doesn't know the composition of the control code, so there is no way to judge the measurement basic which Alice selects to encrypt the polarization states, Eve only selects the random measurement basic to eavesdrop the cryptograph. Whether Eve selects any measurement basic, he cannot obtain the accurate information. The principle of MBE-QKD was shown in Fig. 1.

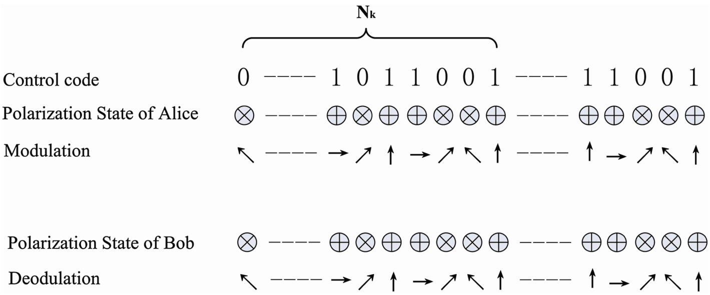


Fig. 1. The principle of MBE-QKD

Whether Eve selects any measurement basic, it cannot obtain the accurate information,so the control code becomes a key of secure communication between Alice and Bob. Before Alice and Bob compare the results by the classical channel, Eve cannot decode any message of the key with the control code. Alice and Bob reuse their control code, Eve can only obtains less than 50% of the cryptograph. If Eve taps the process of the quantum communication, by comparing the quantum bit error rate (QBER) between Alice and Bob, the two parties easily detect Eve, so Alice and Bob get up this transmission, Eve never obtains the useful information of the key with the control code. Due to MBE-QKD and BB84-QKD contain exactly the same coding method, so Hwang proves that this scheme of MBE-QKD is secure. For Alice and Bob, the control code is a secure key of QSDC to detect Eve.

1.3 Controlled-Order-Rearrangement-Encryption-QKD

Before Einstein-Podolsky-Rosen (EPR) enters into the quantum channel, Alice changes the particle transport order of the entanglement with Controlled Order Rearrangement Encryption (CORE), so the chronological locations of the two quantum photons which are located in the upper channel and the lower channel are not one-to-one, and the two quantum photons do not come from the identical EPR. The control code and the order rearrangement are the key technology in CORE-QKD. One bunch of the keys which are shared by Alice and Bob is the control code, for Eve, the control code is one bunch of the random binary sequence [10]. Figure 2 shows the principle of CORE-QKD.

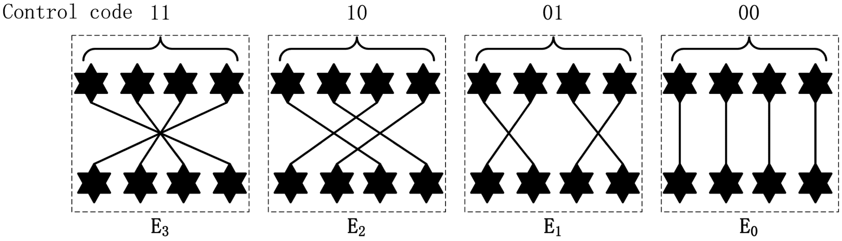


Fig. 2. The principle of CORE-QKD

Alice and Bob can transfer the effective and secure information in the quantum channel after they determines the order rearrangement of EPR, when they begin to assign the quantum key. The encryption and the decryption both utilize the order rearrangement of the control code. As shown in Fig. 2, the two quantum photons which are connected with the straight lines for one EPR. The four EPR contained 24 (4!) kinds of the order rearrangement. For example, Alice and Bob choose four kinds of the order rearrangements to transfer every EPR, they are E_0, E_1, E_2 and E_3. 2 bits of binary values of the control code are 00, 01, 11, and 10, the four binary numbers are respectively corresponded to E_0, E_1, E_2 and E_3.

1.4 Division-Multiplexed of Control Code

Through the analyses of the control code in the methods of MBE-QKD and CORE-QKD, the researchers conclude that the control code is the key technology for the two methods. The control code is used to select the same measurement basic in MBE-QKD; to select the mode of the order rearrangement [11]. Based on the key technology of the control code in MBE-QKD and CORE-QKD, this letter proposes one division-multiplexed of the control code (DMCC) on Quantum Secure Direct Communication-architecture, this method not only makes the control code to select the measurement basic, but also to select the mode of the order rearrangement, in the communication process of QSDC.

2 Establish Model on Division-Multiplexed of the Control Code

In the signal generator, Alice uses the polarization controller (Line-Conjugate-base $\oplus$, Diagonal-Conjugate-base $\otimes$) to modulate the quantum particles, Line-Conjugate-base $\oplus$ modulates the horizontal polarization state "→" and the vertical polarization state "↑", Diagonal-Conjugate-base $\otimes$ modulates the 45° polarization state "↗" and the −45° polarization state "↘", the horizontal polarization state "→" and the vertical polarization state "↑" encode the quantum bit (Qbit) 0, the 45° polarization state "↗" and the −45° polarization state "↘" encode Qbit 1.

The double multiplexing function is that the two parties determine the order rearrangement and select the polarization conjugate base. The sequence of the control code is one string of data bits of binary system, the string of data bits and the code block of the single photon cryptograph contain the same length cryptograph, the cryptograph sequence contains k single photons, the control code sequence is denoted by N_k.

When N_k performs the control function, "0" in N_k selects the polarization $\oplus$ to modulate the horizontal polarization state "→" and the vertical polarization state "↑", "1" in N_k selects the polarization $\otimes$ to modulate the 45° polarization state "↗" and the −45° polarization state "↘". When N_k performs the rearrangement, the binary value range divides the interval to map the rearrangement of E_m. Assumes $k = 8$, the binary value range of N_8 is {00000000-11111111}, N_8 contains eight equal intervals: {E_1, E_2, E_3, E_4, E_5, E_6, E_7, E_8}, Table 1 shows the corresponding relation, Fig. 3 shows the geometric rearrangement of E_m (For example: E_5 and E_8).

Table 1. Interval of N_8

Model of rearrangement	Section of N_8
E_1	00000000-00011111
E_2	00100000-00111111
E_3	01000000-01011111
E_4	01100000-01111111
E_5	10000000-10001111
E_6	10100000-11011111
E_7	11000000-11011111
E_8	11100000-11111111

Alice first executes the rearrangement based on E_m which the binary value range of N_k selects, when Alice modulates the quantum particles. Then Alice chooses the polarization to code the cryptograph with "0" and "1" from N_k. Figure 4 shows the modulation mode of Alice. Bob uses the same method to demodulate the photons sequence which it receives.

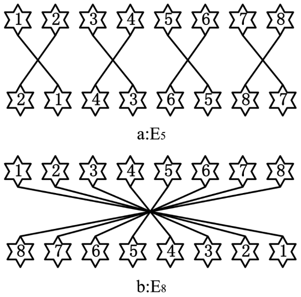
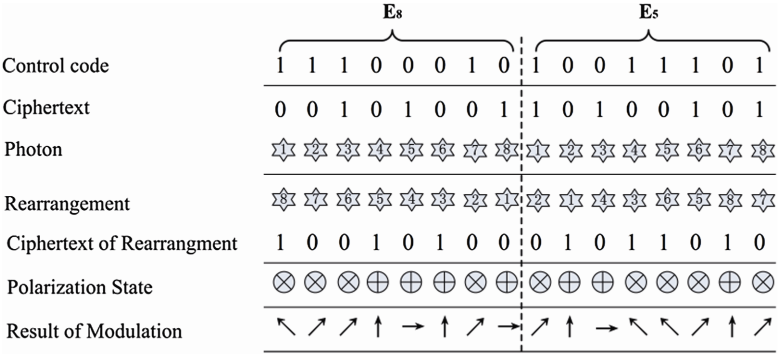


Fig. 3. The order rearrangement E_5 and E_8



	E8								E5							
Control code	1	1	1	0	0	0	1	0	1	0	0	1	1	1	0	1
Ciphertext	0	0	1	0	1	0	0	1	1	0	1	0	0	1	0	1
Photon	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
Rearrangement	8	7	6	5	4	3	2	1	2	1	4	3	6	5	8	7
Ciphertext of Rearrangment	1	0	0	1	0	1	0	0	0	1	0	1	1	0	1	0
Polarization State	⊗	⊗	⊗	⊕	⊕	⊕	⊗	⊕	⊗	⊕	⊕	⊗	⊗	⊗	⊕	⊗
Result of Modulation	↖	↗	↗	↑	→	↑	↗	→	↗	↑	→	↖	↖	↗	↑	↗

Fig. 4. The modulation mode of Alice

3 Experimental Results

The program flow chart of the principle based on DMCC is as shown in Fig. 5. According to the flow chart, Alice (the transmitting end) first prepares the random matrices $\{a_k\}$ and $\{b_k\}$, Bob (the receiving end) prepares the random matrices $\{c_k\}$, the random matrices $\{a_k\}$, $\{b_k\}$ and $\{c_k\}$ values “0” or “1”, $k = 1, 2, \ldots, n$. Alice transmits the quantum states $\{|\varphi a_k b_k>\}$ to Bob, in accordance with an evaluation of the random matrices $\{a_k\}$ and $\{b_k\}$, there are four kinds of the quantum states. The evaluation of random matrices $\{a_k\}$ expresses the cryptograph, if $b_k = 0$, the orthonormal basis I modulates the quantum states of Alice; if $b_k = 1$, the orthonormal basis Z modulates the quantum states of Alice. After Bob receives the quantum states, according to the evaluation of the random matrices $\{c_k\}$, if $c_k = 0$, Bob makes the orthonormal basis I to demodulate the quantum states; if $c_k = 1$, makes the orthonormal basis H to demodulate the quantum states.

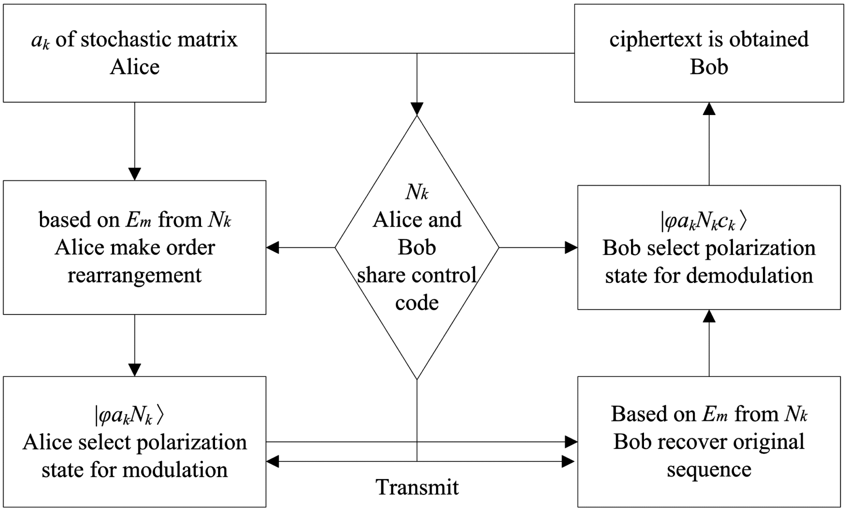


Fig. 5. The program flow chart of the principle based on DMCC

3.1 The Simulation of the Division-Multiplexed Based on the Control Code

As shown in, Alice (the transmitting end) prepares the random matrices $a_k = [1\ 1\ 0\ 1\ 0\ 0\ 1\ 0]$ in Fig. 6, Alice and Bob share the division-multiplexed of the control code $b_k = [1\ 0\ 0\ 0\ 0\ 0\ 1\ 1]$. Because the decimalism of b_k is: m = 131, so Alice selects the fifth rearrangement interval E_5.

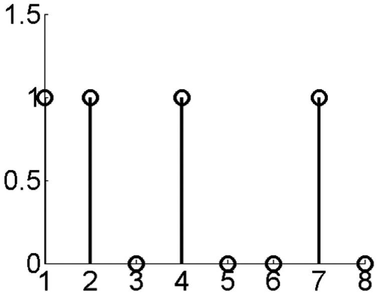


Fig. 6. Alice prepare the random matrices a_k

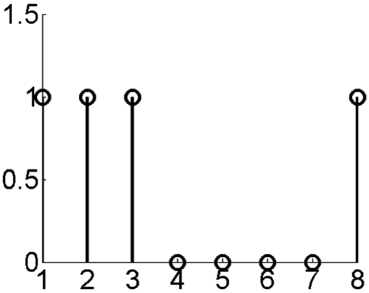


Fig. 7. The result of rearrangement

Alice first executes the order rearrangement, exchanges the first quantum photon and the second quantum photon; exchanges the third quantum photon and the fourth quantum photon; exchanges the fifth quantum photon and the sixth quantum photon; exchanges the seventh quantum photon and the eighth quantum photon, Fig. 7 shows the result of rearrangement.

After the rearrangement, if $b_k = 0$, Alice selects the orthonormal basis I to modulate the quantum; if $b_k = 1$, the orthonormal basis Z to modulate quantum. Figure 8 shows the result of the modulation. Then, Alice transmits the cryptograph of the modulation to Bob, according to the division-multiplexed of the control code, as shown in Fig. 9. Bob recovers the original marshalling sequence of the quantum, then demodulates the final cryptograph, Fig. 10 shows the result of the cryptograph.

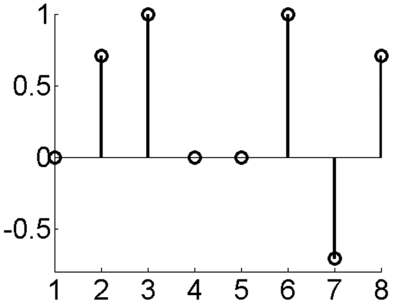


Fig. 8. The result of the modulation

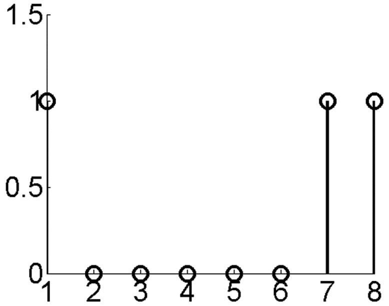


Fig. 9. The control code shared

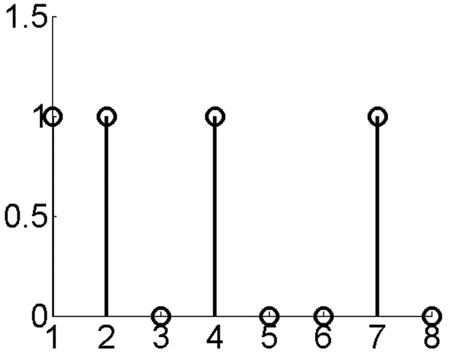


Fig. 10. The cryptograph which Bob demodulates

3.2 Compare QBER

There are eavesdrop-retransmission attacks, Trojan horse attacks, photon-number-splitting attacks, quantum channel noise and channel attenuation in the quantum communication, all reasons also can break the security for QSDC. In the experiments, QBER is employed to compare the security between DMCC and other algorithms, [10] chooses 0.13 as the threshold value. If the threshold value less than 0.13, the eavesdropping, the noise/attenuation cannot be differentiated.

QBER from all 1000 times experiments are more than 0.29 in DMCC, DMCC can detect the eavesdropping effectively. QBER from 118 times experiments are lower than 0.13 in the other algorithm, it cannot differentiate between the eavesdropping and the other reasons in the quantum channel. The comparison between the proposed DMCC and the other algorithm is shown in Table 2.

Table 2. The comparison between the proposed DMCC and another algorithm

QSDC	QBER	Less than 0.13	0.13–0.25	0.25–0.33	More than 0.33
The proposed DMCC	Frequency occurrence	0	0	16	984
Another algorithm	Frequency occurrence	118	280	0	602

4 Conclusion

This letter proposes one division-multiplexed of the control code based on the quantum secure direct communication, the experiments are done, according to the analysis of the simulation result, the proposed algorithm can select the polarization conjugate base to encrypt the quantum, and can execute the order rearrangement. This approach can effectively detect the eavesdropping.

Above all, this paper puts forward one kind of the transmission method in the field of quantum secure direct communication, the main innovative points as follows:

(1) Establish one theory model which put the control code into the block to select the polarization conjugate base.
(2) Design the approach of the order rearrangement based on the control code.
(3) Propose one division-multiplexed of the control code after summarizing the advantages of the control code from MBE-QKD and CORE-QKD.
(4) According to the analysis of the simulation result, this paper proves that the process of division-multiplexed of the control code can effectively detect the eavesdropping.

Acknowledgement. This work is supported by the Professor Zhilu Wu of School of Electronics and Information Engineering in Harbin Institute of Technology.

References

1. 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 **68**(4), 042317 (2003)
2. Yadav, P., Srikanth, R., Pathak, A.: Two-step orthogonal-state-based protocol of quantum secure direct communication with the help of order-rearrangement technique. Quantum Inf. Process. **13**, 2731–2743 (2014)
3. Zhu, C., Hu, Q., Fu, M.: Cryptanalysis and improvement of the controlled quantum secure direct communication by using four particle cluster states. Int. J. Theor. Phys. **53**, 1495–1501 (2015)
4. Xun, R.Y., Wen, P.M., Dong, S.S.: Efficient three-party quantum secure direct communication with EPR pairs. J. Quantum Inf. Sci. **3**, 1–5 (2013)
5. Chen, W., Han, Z.F., Zhang, T.: Field experimental "star type" metropolitan quantm key distribution network. IEEE Photonics Technol. Lett. **21**(9), 575–577 (2009)

6. Liu, D., Pei, C., Quan, D.X.: A new quantum secure direct communication scheme with authentication. Chin. Phys. Lett. **27**(5), 503–506 (2010)
7. Liu, X.Y., Nie, M.: Satellite quantum communication system based on quantum repeating. In: 2011 International Conference on Consumer Electronics, Communications and Networks, pp. 2574–2577 (2011)
8. Jiang, L.N., Zhang, J.L., Ma, J., Yu, S.Y.: Entanglement dynamics between two atoms within different W-like initial states. Int. J. Theor. Phys. **53**(3), 942–951 (2014)
9. Ma, J., Jiang, L.N., Yu, S.Y.: Entanglement dynamics of the mixed two-qubit system in different noisy channels. Int. J. Theor. Phys. **53**(11), 3843–3855 (2014)
10. Guoan, Z., Geng, S., Fan, N.: Quantum secure direct communication using checking sequence coded. Int. J. Secur. Appl. **9**, 333–340 (2015)
11. Zhang, W., Ding, D.S., Sheng, Y.B., Zhou, L.: Quantum secure direct communication with quantum memory. Phys. Rev. Lett. **118**(22), 1–4 (2017)