International Journal of Security and Its Applications
Vol.9, No.10 (2015), pp.333-340
http://dx.doi.org/10.14257/ijsia.2015.9.10.30

Quantum Secure Direct Communication Using Checking Sequence Coded

Zhao Guoan[1], Su Geng[2], Ning Fan[3], and Gao Zehua[4]

[1] *School of Network Education, Beijing University of Posts and Telecommunications, Beijing 100876, China*
[2] *China Academy of Telecommunication Research of MIIT, Beijing 100191, China*
[3] *Key Laboratory of Universal Wireless Communications, Ministry of Education, Beijing University of Posts and Telecommunications, Beijing 100876, China*
[4] *School of Information and Communication Engineering, Laboratory of Network System Architecture and Convergence, Beijing University of Posts and Telecommunications, Beijing 100876, China*
zga@bupt.edu.cn

Abstract

The checking sequence of the schemes of quantum secure direct communication based on a secret transmitting order of particles is only checked for security, which is limited quantum resource and is not made the best. The checking sequence is only checked for security by analyzing quantum secure direct communication proposed before. The novel protocol codes the checking sequence which is added the certain meaning in addition to security checks, named the protocol of the sub-step secret transmitting order of particles using the checking sequence coded. Through analysis by synthesis the novel protocol has higher security and reliability.

Keywords: *checking sequence coded, QSDC, secure transmitting order, quantum communication, sub-step*

1. Introduction

Quantum secure direct communication (short for QSDC) attracts many researchers' attention in quantum communication area. On 2000, a high efficiency two step QSDC scheme is first proposed by Long G. L. and Liu X. S.. in QSDC scheme[1], both quantum un-cloneable theory and quantum un-predictable theory are considered. By utilizing Bell status, the maximum quantum entangled state between particles, a novel encoding and decoding scheme is proposed based on EPR non-locality. The two-step scheme divides each pair of entangled state particles to two parts. Firstly, one part generates a sequence and transmits through a quantum channel. After the transmission, a secure behavior is operated in order to promise the quantum channel is safe. Secondly, after the secure checking, the other part generates a new sequence and operates the quantum photon transmission. In 2003, the concept of quantum secure transmission is proposed in Ref. [2] and [3]. To implementation the concept, an approximate security quantum direct communication scheme is proposed[4], which both considers the quantum entangled state and dense coding. In Ref. [5], a two-step QSDC scheme based on the intensive coding method is proposed by Deng F. G. in 2003. At the meantime, a novel quantum re-arrangement based QSDC scheme is proposed, which the quantum re-arrangement method is using the characteristics of the quantum to reset the original sequence of the particles in order to protect the information privacy. The introduction for the rest schemes and related solutions can be found in <china science> published in 2011. In

ISSN: 1738-9976 IJSIA

generals, the basic idea of two-step scheme is using block transmission, sub-step transmission and sequence re-arrangement to promise the information privacy without generating a security keys during the transmission.

As a production by combining security and quantum mechanics, quantum secret key distribution becomes a main research area in quantum communications. In 1984, Bennett from IBM and Brassard from Montréal University proposed a two pair cross-polarization based quantum secret key distribution scheme for single quantum photon communication (BB84)[8]. According to the BB84, the quantum secret key generates a random binary secret key through a quantum channel to distribute. However, the classical channel is used to transmit an encrypted secure information. Considering the complexity, the generating and measuring of the quantum signal proposed in this scheme is in a simply way. However, an ideally single quantum photon is assisted in a noise channel in order to promise the security. In 1992, a pair of non-cross-polarization quantum secret key distribution scheme is proposed by Bennett, also known as B92[9]. Ekert proposed an entangled quantum photon based quantum secret key distribution scheme, known as Ekert91[10]. After that, QSDC appears and becomes more and more popular.

Considering the development of the information technology, an entangled quantum photon based QSDC protocols is proposed in this paper. By re-arranging the quantum photon sequence and sequence re-encoding for secure checking, a new security strategy for quantum security communication is established. The analysis reveals the proposed protocol can promise the security of the information sequence in a high efficiency ways.

2. QSDC Protocol

As known to all, security is the top considered for a secret communication. The security of quantum communications is based on the quantum mechanics development. Therefore, the constraints of the quantum mechanics also limits the quantum secure communications. In general, the protocol of secret information transmitted by quantum channel is more important than the protocol of secret keys transmission.

An EPR pair can be each one of the 4 Bell status (bell basic status):

$$|\Psi^{\pm}\rangle=\frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B\pm|1\rangle_A|0\rangle_B), \quad (1)$$

$$|\Phi^{\pm}\rangle=\frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B\pm|1\rangle_A|1\rangle_B)。 \quad (2)$$

Where $|0\rangle$ and $|1\rangle$ represents the two Eigen states in the two-level energy systems, which means the horizontal polarization and vertical polarization separately. For example, self-rotations along the z-axis, the Eigen states represent the self-rotation symbol σ_z. A and B represent a pair of two quantum photons. Two quantum photons in an entangled status are well connected and non-locality, which is proved by many quantum experiments [11-17]. Therefore, Bell-status only focuses on pair of two quantum photon entangled status. Furthermore, the entangled status for Bell-status is the maximum entangled status. To promise the consistence in this paper, only the maximum entangled status is considered. Considering a pair of AB quantum photons in entangled status $|\Psi^{-}\rangle=\frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B-|1\rangle_A|0\rangle_B)$, if photon A is measured and the results is $|0\rangle_A$, then the quantum states of the original pair of AB collapses to direct product space $|0\rangle_A|1\rangle_B$. In this case, the quantum states of quantum B would equals and only equals to $|1\rangle_B$. According the quantum mechanics theory, the connection is constant and won't change according to the distance change. Meanwhile, only if the quantum photons are entangled, the connection of the measurement is existing. This is a characteristic for non-locality of entangled quantum.

A four binary operations are deployed in this communication protocols, which are U_0=I, U_1= σ_z, U_2= σ_x, U_3= $i\sigma_y$, a more specific details are defined as follow:

$U_0=|0\rangle\langle 0|+|1\rangle\langle 1|$, $U_1=|0\rangle\langle 0|-|1\rangle\langle 1|$, $U_2=|0\rangle\langle 1|+|1\rangle\langle 0|$, $U_3=|0\rangle\langle 1|-|1\rangle\langle 0|$, such definitions represent the two bits classical information 00, 11, 01, 10 respectively.

Based on this physical characteristic, a proposed procedures is described as follow:

1) Alice prepares EPR, then Alice selects a suitable sized subset for check sequence, the rest EPR pairs are set to secret information sequences. The check sequence and secret information sequences are both EPR pairs instead of single quantum photons. The size of checking sequence is decided both by the size of the secret information sequence and by the re-arrangement method of secret information sequence. Then, Alice uses the four binary operations ending the secret message in set M, also checks the encoded message in set C. (The coding check messages is disrupted the secret of EPR corresponding relations between particles)

To simplify, defined there are N pairs of EPR pairs entangled quantum photons: $P_1(1,1')$, $P_2(2,2')$,…,$P_j(j,j')$…$P_N(N,N')$. Assuming the checking message chosen by Alice is (0100101101…11), then first choose varies suitable EPR pairs in order to compose set C. Then, encodes 01 on $P_1(1,1')$, 00 on $P_2(2,2')$, 10 on $P_3(3,3')$…11 on $P_c(C,C')$ till the end. It is import that the number of 0 and the number of 1 must be equal in the checking message.

Alice transmits disordered message composed by the initial states of check sequence set C and quantum channel encoded set C to bob through a classical channel. The sequence of set C should set in a disordered sequence, and the secret message set M re-arranges according to the new order shown in sequence set C.

The disorder sequence set C is like this: $P_1(1')$ …$P_2(2)$ …$P_3(3')$… $P_3(3)$……$P_c(C')$…$P_1(1)$ … $P_c(C)$ …$P_2(2')$.

The message of the check sequence set C means that the message sequence is ordered like this: the first 0 personifies $P_{c+1}(C+1)$'s place, the first 1 personifies $P_{c+2}(C+2)$, the second 0 personifies $P_{c+1}(C+1')$'s place which compose a group with the first 0, the third 0 personifies $P_{c+3}(C+3)$'s place, the second 1 personifies $P_{c+2}(C+2')$'s place, and so on. If the length of checking sequence is short of the message, then checking sequence's message is recycled in turn. The define message of the check sequence is shown as Figure 1.

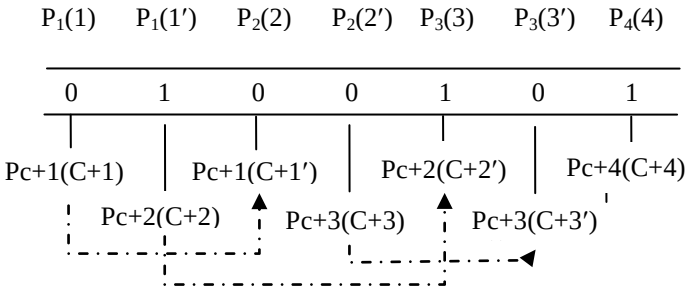

Figure 1. The Meaning of the Check Sequence

2) Bob receives the check sequence set C through a quantum channel, also receives an initial state of check sequence set C through a classical channel. By using the defined binary operations to measure the EPR contained in the check sequence set C. The measurement result stores in local storage and the feedback sends to Alice.

3) Alice compares the value between the originals and the one receives from Bob in order to detect the potential eavesdropper eve. If the channel is secure, Alice re-arranges the set M according to the information provided by the check sequence as showed in Figure 1, then transmits the message as a single quantum photons through a quantum channel to the receiver Bob. Otherwise, Alice terminates this communication and starts the next one.

4) Once Bob receives the sequence M, a decoding mechanism is operated. By using a match entangled states provided by the check sequence, Bob can decoded and received the information transmitted by Alice successfully.

The procedures described cannot only detect the eavesdroppers Eve, but also decrease the communication times. Furthermore, even the eavesdroppers Eve can sounding the quantum channel, the eavesdroppers Eve cannot receive a desired message from a single disordered quantum photon. By using this method, both privacy and performance of a quantum communication can be promised.

3. Comprehensive Analysis of the Protocol

This protocol is based on the combination of EPR pairs, and the step-by-step transmission and block transmission, ordering up security strategy, but also the integrated use of the code and other technical in order to promise the transmission security, make this protocol not only meets the higher security requirements, but also reduces the number of communication, namely to improve the whole communication efficiency, rational use of limited resources and to increase the stability of the whole communication system.

The details of analysis listed as follow:

Firstly, the proposed protocol is based on the EPR pair. Therefore, similar entangled photon based schemes in Ref. [4], Ref. [18-19] are already proved the security. Furthermore, a detailed introduction is given in Ref. [5].

Secondly, the security strategy of the proposed protocol is based on the inherent of the disorder of the check sequence C and disorder of the message sequence M. If Alice and Bob detect non eavesdroppers Eve during the transmission, eavesdroppers Eva can only sounding the signals but cannot decoded the information by Bell measurement. This protocol confidential information of M sequences EPR to separate for each single photon and disrupt the sort, the eavesdropper Eve if the check sequence in C transmission eavesdropping is found, the corresponding relationship in the check sequence C transmission is completed will grasp the actual EPR particles in M sequence, cannot obtain secret information available also. However, this protocol uses disorder examination sequence C transmission security and secret in formation of M sequences are simply that this agreement is in a safe condition. Therefore, this protocol is absolutely safe in an ideal channel.

Finally, the protocol of EPR based transmission in Ref. [7] mentioned, though the quantum communication transmitted only once a time, it seems to decrease the possibility of eavesdropping. However, in fact, once the value in the quantum communication is higher than the threshold and captured by the eavesdroppers Eve, the whole communication would terminated. Meanwhile, this is a trade-off between communication security and communication continuity. The protocol proposed in this paper can overcome this problem. Because, the checking sequence C and secret message sequence M is transmitted separately. Once the check sequence C detect the eavesdropping, the communication terminated. Besides, the transmission of secret message sequence M is canceled in order to promise an absolutely secure. On the other possibilities, there is no eavesdropping detected by the check sequence C, the communication continuous with secure permission. The eavesdroppers Eve cannot decoded the secret messages even has the secret messages sequence only.

The detail of the protocol procedures are drawn as follow Figure 1.

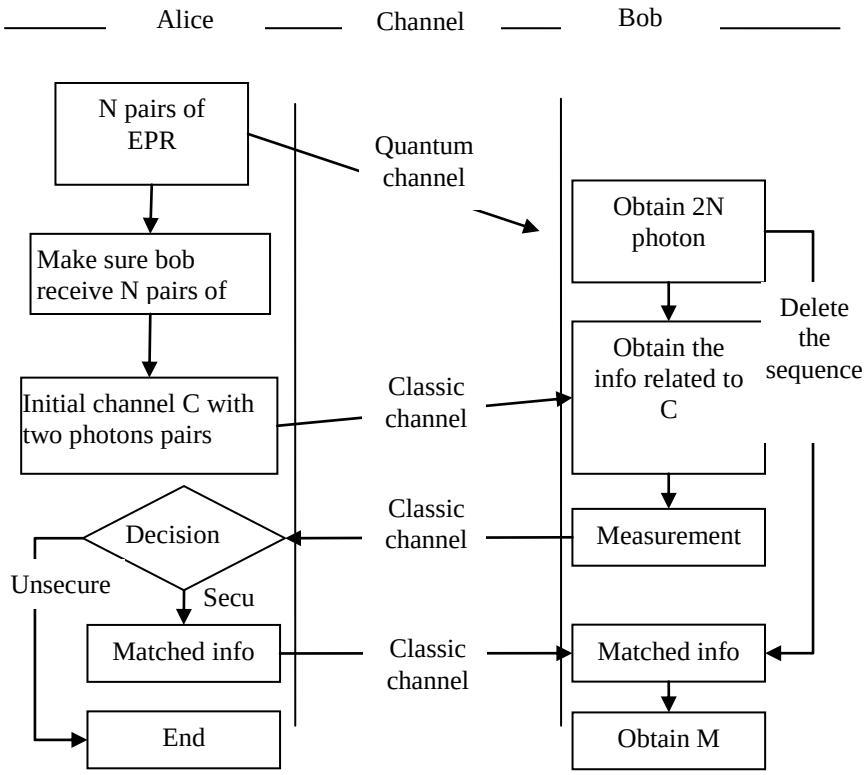

Figure 2. Quantum Photon based One-step Transmission Protocol

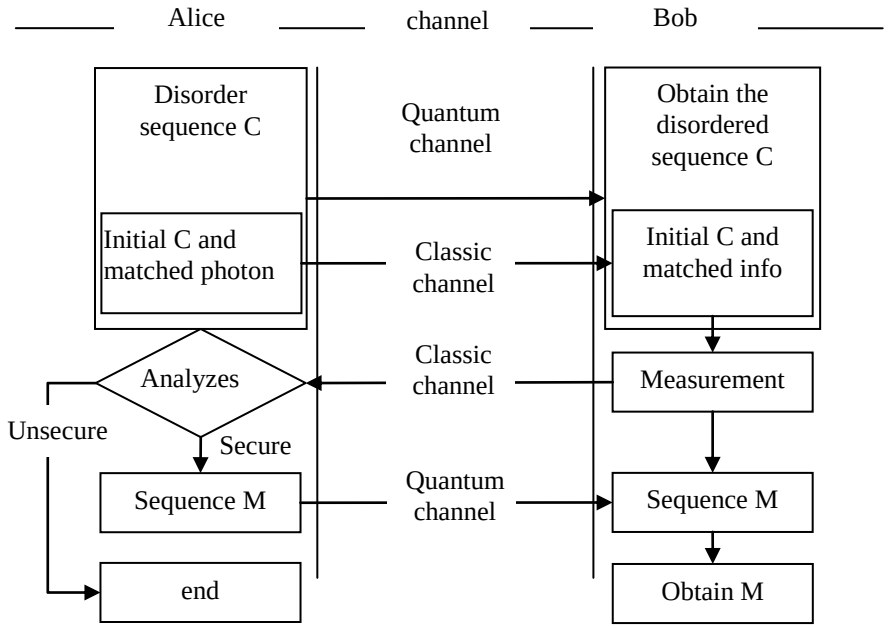

Figure 3. The Proposed Two-step Transmission Protocol

As shown in Figure 2 and Figure 3, the proposed protocol both using the quantum channel and classic channel twice, the total communication happens third times. First communication both happens on quantum channel and classic channel, which based on the protocol described in Ref. [7]. Particle secret transmission of step transmission protocol process based on Ref. [7], which is using the quantum channel at one time, and using a classical channel three times, both sides of the protocol of the communication

were conducted for four interactions in total, the first time an initiator of communication enable only the quantum channel, the classical channel is in the idle state. Obviously, this protocol reduces the communication times compared with Ref. [7], rational distribution of data using the strategy and full uses of communication infrastructure resources, especially the communication channel, the throughput rate of the whole system is improved, and ensures the stability of the system.

To be considered the in real channel scenario, the checking sequence can be considered some redundancy coding message. This strategy can reduce the secondary communication traffic information content, but the balance of the redundancy rate is not constant base of the real channel scenario. The effectiveness also need to be consider and tested.

Based on the previous consideration, the proposed QSDC using checking sequence coded scheme not only promise the secure, but also increase the transmission efficiency by decrease the unnecessary transmission times. So, we can go on study the application about other cases.

4. Summary

Both single-direction and double-direction quantum communication are secure in an ideal channel scenario based on the analysis mentioned above. However, the noise exists in real channel scenario. Therefore, it become a severe threat in quantum communication area. To make a trade-off between optimal and reality, increase the error threshold in a weak noise scenario is worth of considering. Therefore, the proposed protocol can still be used in noise channel scenario.

At the same time, quantum communication in the 8-10 literature, once the eavesdropper is being detected, the whole communication is terminated, the secret information is discarded. Therefore the information cannot be stolen. However, for QSDC, it is different with the reference 8-10 QKD protocol. The quantum channel in QSDC direct transmission of secret information, if be bugged does not mean just waste news, but the secret information has been leaked; while the QKD protocol transmission is a key, even if the key information for eavesdroppers to obtain will not reveal the secret information, even in consideration of the safety key can be passed in the legal and communications between the two sides the new generation. For the purposes of this agreement, the secret information hidden in the quantum sequence disorder, and the corresponding relation between the secret sequences also hidden in the check sequence, sequence checking transmission is disordered. Eve accesses to the particle set in time, but does not know a particle sequence and correct correspondences, so she cannot obtain the secret information effectively, this time in addition to communication starts eavesdropping case, Alice needs to immediately stop the communication, otherwise the communication safe can be conditional, it will not lead to the disclosure of secret information, the secret information can continue to use in the legal users.

Generally, based on encoding check sequence and sub step method, a novel protocol is proposed in this paper. For some similar protocol, these secure strategies not only promise the quantum secure, but also increase the QSDC transmission efficiency. The analysis proves that the proposed protocol is absolute secure in a noise-free channel scenario. The main advantages of the proposed protocol are encoding the check sequence with a certain meaning. Therefore, the full extension of the secure check sequence, distribute-step transmission and quantum sequential transmission strategy fully guarantee the security of quantum communication.

But the method of the checking sequence coded is not the end in the quantum secure communication. Sometimes the method can be used to other quantum secure

communication, for example, which is designed in Ref. [20]. So we can do a lot of researches about the application for its effectiveness.

Acknowledgements

We thank Li Baoxun & Zhao Xiuli for reading the text and giving us suggestions. The study is supported by the project “the study of continue education brand effect”.

References

[1] Long G L, Liu X S. Phys Rev A., 65 032302 **(2002)**
[2] Beige A, Englert B G, Kurtsiefer C, Weinfurter H Acta. Phys. Pol. A. 101 357–368 **(2002)**
[3] Beige A, Englert B G, Kurtsiefer C, Weinfurter H J. Phys. A-Math Gen 35 L407–L413 **(2002)**
[4] Boström K, Felbinger T Phys.Rev.Lett. 89 187902 **(2002)**
[5] Deng F G, Long G L, Liu X S Phys. Rev. A 68 042317 **(2003)**
[6] Deng F G, Long G L. Phys. Rev. A 68 042315 **(2003)**
[7] Ai-Dong Zhu, Yan Xia, Qiu-Bo Fan, and Shou Zhang Phys. Rev. A 73 022338 **(2006)**
[8] Bennett C H, Brassard G 1984 In: Proceedings of IEEE International Conference on Computers, System and Signal Processing. Bangalore, India: IEEE 175–179
[9] Bennett C H. 1992 Phys. Rev. Lett. 68 3121–3124 **(1992)**
[10] Ekert A K. 1991 Phys. Rev. Lett. 67 661–663 **(1991)**
[11] Tapster PR,Rarity JG and Owens PCM. Phys. Rev. Lett. 73 1923–1926. **(1994)**
[12] Tittel W, Brendel J, Zbinden H et al Phys. Rev. Lett. 81 3563–3566. **(1998)**
[13] Tittel W, Brendel J, Gisin B et al Phys. Rev. A. 81 3229–3232. **(1998)**
[14] Shih Y and Kim YH Found Phys. 29 1849–1861. **(1999)**
[15] Pan JW, Bouwmeester D, Daniell M et al Nature 403 515–519. **(2000)**
[16] Kuzmich A, Walmsley IA and Mandel L Phys. Rev. A. 64 063804. **(2001)**
[17] Pittman TB and Franson JD Phys. Rev. Lett. 90 240401 **(2003)**
[18] H. Inamori, L. Rallan, and V. Vedral J. Phys. A. 34 6913-6918. **(2001)**
[19] Edo Waks, Assaf Zeevi, and Yoshihisa Yamamoto Phys. Rev. A. 65 05231 **(2002)**
[20] Zhao, G.. Quantum Secure Communication Protocol Based on Single-photon. International Journal of Security & Its Applications, 9(3). **(2015)**

Authors

Zhao Guoan, B.S. is an engineer. He was born in Heilongjiang Province of China on Feb 6, 1980. He received the B.S. degree in Communication and Information systems from the University of Beijing University of Posts and Telecommunications in 2006. Then he works in the University and has been engaged in several research and his research interests include development programs involving communication, systems design, management information system and education system.

Su Geng, Ph.D. is an engineer of China Academy of Information and Communication Technology, a member of ITU-R WP5D group. He has been active in communication area, provides contribution in China IMT-2020 Promotion Group. He awarded the PhD degree in EECS from Queen Mary University of London in 2013.

Ning Fan, Ph.D. is an Associate Professor. She was born in Liaoning Province of China in 1962. She received the B.S. degree & D.C. degree in Communication and Information systems from the University of Beijing University of Posts and Telecommunications. Then she works in the University and has been engaged in several research and development programs involving communication, systems design and so on.

Zehua Gao, Ph.D. Associate Professor School of Information and Communication Engineering Laboratory of Network System Architecture and Convergence Beijing University of Posts and Telecommunications (BUPT) Postal Add.: P.O. Box 128#, BUPT, Beijing 100876, P. R. China.