International Journal of Security and Its Applications
Vol. 9, No. 3 (2015), pp. 267-274
http://dx.doi.org/10.14257/ijsia.2015.9.3.20

Quantum Secure Communication Protocol Based on Single-photon

Guoan Zhao[1]

[1]*School of Network Education, Beijing University of Posts and Telecommunications, Beijing 100876, China*
zga@bupt.edu.cn

Abstract

Two-way quantum secure communication protocol and one-way quantum secure communication protocol based on single photon sequence and the XOR operation have been proposed, one-way communication can confuse the eavesdroppers and two-way communication only a single authentication and there is not visible to eavesdropping and delayed photon attack Trojan horse attack. The new agreement the use of single photon sequence and no regularity not only to achieve unconditional security, and semantics confuse eavesdroppers and has a high transmission efficiency, easy implementation, especially suitable for use in noisy channels.

Keywords**:** *quantum secure communication, single photon, one-way communication, two-way communication*

1. Introduction

Quantum communication is one of the main focuses in the quantum information research. It has a good application prospect. In 1984, Bennett, a scientist of IBM, and Brassard of University De Montreal, put forward Quantum Key Distribution Protocol (short for BB84) based on two groups of encoded photons in orthogonal polarization state. In BB84 Protocol, quantum key distribution is carried out through a quantum channel, that is to say, random key sequence in binary system is transmitted by a quantum channel and the secret message encrypted by the random key is transmitted by a classics channel. The preparation and measurement of quantum signals in the protocol is relatively simple, but needs ideal single-photon source to realize the security in the noisy channel [1]. In 1991, Ekert first brought out Quantum Key Distribution Protocol based on entangled particles, short for Ekert 91 [2]. In 1992, Bennett proposed a brief Quantum Key Distribution Scheme based on a group of non-orthogonal states, short for B92 [3]. These researches and references [4-10] have discussed the branches of Quantum Key Distribution (QKD). Among them, the branches of quantum communication also conclude: Quantum Secret Sharing (QSS) [11-16], Quantum Secure Communication [17-28], Quantum Encryption Algorithm, Quantum Authentication and Signature, Quantum Network Communication Protocol and so on. Different from classics secret sharing, QSS shares not only classics information, but also quantum information. While the first Quantum Secret Sharing Protocol [11] (HBB Protocol) has used quantum means to achieve the share of classics information, and QSS designed in References [12-16] is focused on secret messages sharing in certain field. After being encrypted by a set of code, secret message is transmitted through a quantum channel in DSQC, and the key is transmitted by a classics channel after ensuring the security of the quantum channels by both parties in the communication, thus the receiver can read out the secret message. This can be regarded as a deformation of communication system based on quantum key distribution. In the noisy

ISSN: 1738-9976 IJSIA

condition, DSQC has a good adaptability, because many pieces of classics message are exchanged in the communication after the security of the channel is assured, and the secret message needn't to be transmitted.

QSDC differs from QKD, QSS and DSQC. In QSDC, the secret message is directly transmitted by a quantum channel, and some auxiliary message to the security check is transmitted by a classics channel. Similarly, the security of QSDC is also based on quantum no-cloning principle, quantum uncertainty principle, and the association and non-locality of the entangled particles. In 2002, Boström and Felbinger explored the ideas of quantum entanglement and quantum dense coding to propose "Ping-pong" Protocol [21], though it is proved insecure in the noise channel, QSDC becomes a branch preferred by the researchers in the quantum communication field. In 2003, Deng Guofu and Long Guilu utilized block transmission thought and based on dense coding theory and entanglement pair to put forward Two-step Quantum Security Direct Communication Scheme [22], and discuss the standard of quantum secure communication scheme. In 2004, Yan Fengli used quantum teleportation to conduct quantum direct communication and brought out the relative scheme. In 2005, Wang Chuan proposed high dimension QSDC Scheme [23] with quantum dense coding; Zhu Aidong put forward QSDC Protocol [24] based on particle order rearrangement; Wang Jian brought out multi-party controlled QSDC Protocol [25] based on single-photon order rearrangement; then appeared QSDC Protocol [26] with X entangled state and protocol [27] with identity authentication to improve the security of QSDC. Hence, QSDC becomes one of the research focuses and Long Guilu [29] overviewed the basic theory and recent dynamic development of QSDC.

The security of the quantum communication has been guaranteed by the quantum no-cloning principle and quantum uncertainty principle. Single particle again becomes one of the ideal information carriers in the quantum communication loved by the researchers and wins wider application for the merit of economic utility, high efficiency, realization simplicity, simple operation and so forth. BB84 [1] Protocol first set a precedent for the researches on single-particle QKD, then followed many researches on quantum communications based on single-particle, such as QKD Scheme in B92 [3]; Quantum Key Distribution Scheme with measuring base encryption by Hwang [30]; Multi-party Quantum Secret Sharing [31] Scheme based on a disposable pad protocol expension of the single-photon; Security Quantum Communication Scheme [20] based on single-photon and confirmation of non-maximally entangled state by Li Xihan. Recently, Quan Dongxiao and Pei Changxing have brought up a new Quantum Security Communication Protocol (QPLZ Protocol) [28] in which the single-photon is used as information source and one-way communication is conducted, with the help of the logistics of the send sequence and test of the check sequence, *i.e.,* send sequence is formed by the XOR operation on the secret information sequence and random sequence.

It is well-known that a crucial issue of secret communication is its security. The security of quantum communication is based on the theory of quantum mechanics to prevent the unconditional attack of eavesdroppers, *i.e.,* the technique of eavesdroppers is only confined by the laws of quantum mechanics. The importance of QSDC or DSQC Protocol is more important than that of QKD, because they transmit secret messages by a quantum channel, other than a private key. Therefore, how to test the existence of eavesdroppers faster and more exactly and guarantee the effective transmission of secret messages are the research direction for QSDC and DSQC Protocol, but the necessary auxiliary information is only transmitted by a classics channel at the public and non-altered basis. From that, based on single-photon sequence and XOR operation, we propose unidirectional quantum security

communication protocol that confuses eavesdroppers in the paper. We also propose bidirectional quantum security communication protocol that only needs single check without invisible eavesdropping or Trojan horse attack of delay photon attack. The eavesdropping test is first conducted and the necessary auxiliary messages are published by a classics channel, then the protocol is comprehensively analyzed. The encoding rule of communication protocol in the paper has adopted: Z based: $|H\rangle = |0\rangle = 0$, $|V\rangle = |1\rangle = 1$, X based: $|u\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = 0$, $|d\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = 1$. In the paper, we first review the quantum communication protocol. Next, we propose and analyze unidirectional quantum security communication protocol. Then, we propose and analyze bidirectional quantum security communication protocol. At last, we draw a conclusion to the protocol.

2. Unidirectional Quantum Security Communication Protocol based on Single-photon

In order to work out more secure and practical unidirectional quantum security protocol, the communication process of the new-designed one based on single-photon is described as follows:

(1) Alice utilizes random number generator to generate random sending photon sequence, randomly chooses Z based and X based to carry out random coding, and sends these random photon sequence to Bob;

(2) After receiving the photon sequence, Bob simply conducts delay storage and records the position of the receiving photon, and randomly selects partial received photon (as random check sequence) to choose Z based and X based randomly to test and record the outcomes of his measurements. Then, he sends the position of the photon and measuring result to Alice;

(3) After she receives the collected message from Bob, Alice compares the measuring result of the check sequence chosen by Bob and works out the error rate. If the error rate is higher than threshold value, that means the channel is not secure, and the communication is halted. Even though Eve had got the random photon sequence without code information, he hasn't obtained any secret message. If the channel is safe, the following operation will be continued to carry out. In the condition of secure channel, Alice conducts the bitwise XOR operation according to Bob's feedback on the photon sequence received by Bob (not including random check sequence or second check sequence) and code classics sequence, encodes the secret messages, and publishes all the measurement matrix of the photon sequence except the check sequence and the condition and value of the second check sequence. In the midst, we can use sequence 010… 1 stands 1 position Z based, 2 position X based, 3 position Z based… final position X based as measuring base sequence to be published and transmitted, the code classics sequence is got by the bitwise XOR operation to the codes in the actual code sequence and random photon sequence. She transmits the codes in the above-mentioned code classics sequence and measuring base sequence by the classics channel to Bob;

(4) After getting the measuring base information of every position declared by Alice through the classics channel, Bob conducts measurement to the received photon sequence (not including random check sequence) in the corresponding measuring base, checks the security of the channel for the second time, and performs the bitwise XOR operation to the result sequence and the received code classics sequence, then obtains the encrypted secret messages. The detail of the protocol procedures are drawn as Figure 1.

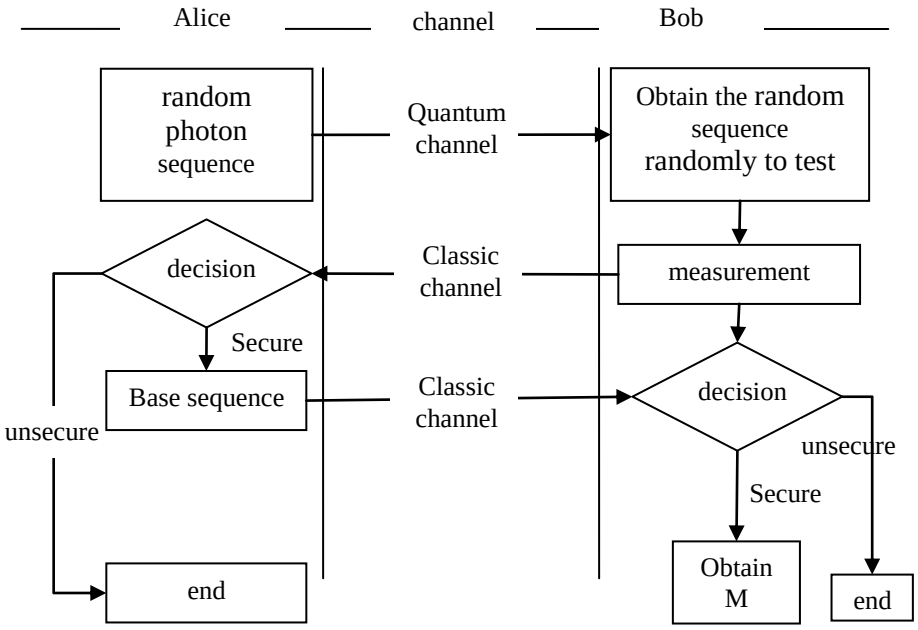

Figure 1. The Proposed Unidirectional Transmission Protocol

The protocol in the paper is based not only on quantum no-cloning principle and quantum uncertainty principle to guarantee the security of quantum communication, but also on the uncertainty or confusion of the random sequence. It has inherited the main thought of QPLZ Protocol, so common interception-retransmission attack; auxiliary particle attack and refuse services attack are not effective to the protocol. It has also improved QPLZ Protocol. In the protocol, it is suggested that the codes base of the information sequence and check sequence are published at the same time, because the information sequence has already been encrypted before. Even though the channel is not secure, the eavesdropper only gets the ciphertext, *i.e.*, Eve is easy to obtain the ciphertext, that means the security of the channel is guaranteed by means of encryption, not by the quantum mechanics theory, the essence of the security in quantum communication. And that depends on the encryption with one-time pad and the random number generator becomes essential. How to overcome the factual difficulty that complete random generator cannot be made in the classics cryptography is not mentioned, so that brings certain hidden danger to the protocol. Though we don't need to judge the security of the channel by measuring the photon in certain position [28], the security of QPLZ Protocol must be reduced to the grade of classics encryption communication. Therefore, the security of the transmitted messages by a quantum channel must be guaranteed by utilizing quantum mechanics theory as much as possible, and that constructs the basis of the quantum communication. According to the new protocol in this paper, the security of a quantum channel is checked first, then the secret message is encoded and transmitted after the confirmation of the security of the transmission sequence in a quantum channel. Even though the transmission by a quantum channel is not random sequence, the quantum loss led by the noise of the channel is random and that guarantees the nondeterminacy of the random sequence. At the same time, the information is checked for the second time, which fatherly ensures the security and detectability of the channel. After being conducted XOR operation, the random sequence may previously be encoded to produce classics code. The classics code and some simple random sequence with certain rules can form the semantic information irrelative to the secret message, and that will confuse the eavesdroppers to believe it is the

secret message. However, common Trojan horse attacks, including invisible eavesdropping [32] and delay photon attack [33], have no effect on the unidirectional quantum communication. As for encoding, it is the same as that of QPLZ Protocol, and it owns certain security merits compared to BB84 Protocol [34] based on delay measurement. But to reduce information volume of classics communication, QPLZ Protocol adopts the way of only publishing the position of the photon in the X based code, thus unluckily increases the information volume of the classics communication. In the case of equal probability, Z based and X based codes are used, to N/2 photon X based, the number that message in every position needs classics bitwise is $log_2 \frac{N}{2}$, then at least needs N/2×$log_2 \frac{N}{2}$ classics information position. While the protocol in the paper is under certain agreement by both parties based on N classics information position needed in the transmission to specify the specific position by Z based and X based code. When N≤8, N/2×$log_2 \frac{N}{2}$≤N, the particle within 8 cannot be transmitted every time in the quantum communication, so the new protocol has obvious advantage to the classics information transmission, but how to use the way, such as compression coding to streamline, cannot fatherly be discussed. Besides, the new protocol has the following advantages, for example, easy to realize, high transmission efficiency and double communication distance compared to the bidirectional communication.

The new protocol is similar to Deng Guofu's BB84 Protocol based on delay measurement and Li Xihan's Quantum Security Communication Protocol based on any d dimenssion single-photon. Compared to that of Li Xihan's [20], the operation is different, but they have equally satisfactory results. While in this paper, after-encoding strategy is put forward. Even if Eve has intercepted partial photons, that is only photon itself, because the code base of these photons hasn't been declared and they themselves are random unmeaningful codes. Under the circumstances of multidimentional (d>2), the efficiency of Reference [20] is higher. In Reference [20], the necessary auxiliary information is announced after ensuring the security of quantum channels, so the randomly selected photon with certain position is measured and tested. We can see that just like BB84 [1] Protocol, the unidirectional communication protocol based on single-photon has adopted random measurement to the security test. Differently, the protocol has only selected partial photons to the random test, increasing the capacity of communication system, but Bob needs furtherly storing the received photons. Hence, to increase the practicability of the protocol, we can expand the random test scope of the second step in the protocol to all the photons, the same as Reference [1] and that can make the protocol easy to come true. Also, the protocol has used the thought of second check to ensure its security furtherly.

Besides, the ideas of unidirectional quantum security communication in the paper has some common with that of the bidirectional, but the requirement for the capacity of storing is lowered, even that may be applied to the bidiretional communication protocol. The code idea of the protocol in the paper is that the security of the quantum channel is confirmed first, then the transmitted information is encoded. It has common with the bidirectional communication, but omits the code operation of the second check and fill to make it easy to come true in the protocols, such as QPLZ. To the party with low capacity of storage, it can even omit the storing link, only to lower the use rate of photon, that is to say, Bob needs only to carry out random measurement to all the received photons, similar to the way of BB84 [1], and this has reduced the requirement for Bob's storage capacity. In the noisy channel, only certain amount of effective photon is guaranteed, then check and further code can be carried out to them, without increasing the problems of mistaken code, *e.g.*, later fill. In conclusion, the new protocol in the paper is not only safe, semantic confusion, but also well applied in the noisy channel.

3. Bidirectional Quantum Security Communication Protocol based on Single-photon

According to the above unidirectional quantum security communication protocol, we can work out a safe and practical one, the process is described as follows:

(1) Alice utilizes random number generator to generate random sending photon sequences, randomly chooses Z based and X based to carry out random coding, and sends these random photon sequences to Bob;

(2) After receiving the photon sequence, Bob simply conducts delay storage and records the position of the received photon, and randomly selects partial received photon (as random check sequence) to choose Z based and X based randomly to test and record the outcomes of the measuring. Then, he sends the position of the photon and measuring result to Alice;

(3) After she receives the collected message from Bob, Alice compares the measuring result of the check sequence chosen by Bob and works out the error rate. If the error rate is higher than the threshold value, that means the channel is not secure, and the communication is terminated. Even though Eve had got the random photon sequence without code information, he hasn't got any secret messages. If the channel is safe, the following operation will be then carried out. In the case of secure channel, according to Bob's feedback, Alice conducts the bitwise XOR operation to the photon sequence received by Bob, not including all the test base of the check sequence and the position and value of the second check sequence. In the midst, we can use the sequence 010… 1 stands 1 position Z based, 2 position X based, 3 position Z based… final position X based as measuring base sequence to be declared and transmitted. The above measuring base sequence together with the position and value of the second check sequence are transmitted by a classics channel to Bob;

(4) After he gets the measuring base information of every position announced by Alice through a classics channel, Bob conducts measurement to the received photon sequence (not including random check sequence) in the corresponding measuring base, compares the second check sequence to make sure the security of the channel, at the same time, conducts XOR operation to the result sequence and the secret message code sequence to be sent, then sends the secret message to Alice by a classics channel;

(5) After receiving the secret message, Alice carries out XOR operation to it with her own random code, and gets the secret message.

The new protocol is not only based on quantum no-cloning principle, and uncertainty principle to guarantee the security of the quantum communication, but also applied the uncertainty or confusion of the random sequence. It has inherited the main thought of the above unidirectional protocol, so the common eavesdropping-retransmission attacks, auxiliary particle attack, refuse service attack, *etc.*, are all not effective. Besides, the code design in the protocol first confirms the security of the quantum channel, and the transmitted messages are encoded. The quantum information is only transmitted once, and the code operation of second error correction and fillment in QPLZ Protocol are omitted and made it easier to achieve. To the party with lower storing capacity, the storage link may even omitted, only reducing the use rate of the photons, that is to say, Bob conducts random test to all the received photons, and reduces the requirements for Bob's storing capacity similar to BB84 [1]. After receiving the random code sequence, Bob carries out classics code to it and then transmits the classics codes to Alice, which has realized the aim of the bidirectional communication without increasing extra equipment and provided a kind of new thought for the bidirectional communication protocol. The invisible eavesdropping [32] in the common Trojan horse attack and delay photon attack [33] are incapable to the bidirectional communication protocol designed by the new method and ideas. Furthermore, compared to

other bidirectional quantum communication protocol, in this protocol, the quantum channel is only used once and it is favorable to apply it in the channel with worse noise. In a word, the protocol in this paper has tried to overcome the shortcomings of the previous protocols, combined many new thoughts based on the new theory, and provided a feasible way to the noise channel.

4. Conclusion

In conclusion, the unidirectional and bidirectional quantum security communication protocols based on single-photon in the paper have not only inherited the advantages of QPLZ, such as easy to realize, high transmission efficiency, double communication distance and so on, but also overcome some shortcomings. Furthermore, the new protocol has brought out some new ideas for realizing bidirectional protocol to guarantee the unconditional security. It has improved the strategy of coding to reduce code amount of information and made the quantum communication easier to realize. It has transmitted some irrelative content to the secret messages in terms of random code to confuse the eavesdroppers to reach the target of semantic safety. It needn't test Trojan horse attack and has advantage in the noise channel.

References

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing", Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing Bangalore, India, **(1984)** December, pp. 175-179.
[2] A. K. Ekert, Phys. Rev. Lett., vol. 67, no. 661, **(1991)**.
[3] C. H. Bennett, Phys. Rev. Lett., vol. 68, **(1992)**, pp. 3121-3124.
[4] C. H. Bennett, G. Brassard and N. D. Mermin, Phys. Rev. Lett., vol. 68, no. 557, **(1992)**.
[5] N. Gisin, *et al.*, Rev. Mod. Phys., vol. 74, no. 145, **(2002)**.
[6] G. L. Long and X. S. Liu, Phys. Rev. A, vol. 65, no. 032302, **(2002)**.
[7] F. G. Deng and G. L. Long, Phys. Rev. A, vol. 68, no. 042315, **(2003)**.
[8] X. B. Wang, Phys. Rev. A, vol. 72, no. 012322, **(2005)**.
[9] G. Q. He, Z. Yi, J. Zhu and G. H. Zeng, Acta Phys. Sin., vol. 56, no. 6427, **(2007)**. (in Chinese)
[10] Y. B. Zhao, M. Heid, J. Rigas and N. Lütkenhaus, Phys. Rev. A, vol. 79, no. 012307, **(2009)**.
[11] M. Hillery, V. Bužek and A. Berthiaume, Phys. Rev. A, vol. 59, no. 1829, **(1999)**.
[12] V. Karimipour and A. Bahraminasab, Phys. Rev. A, vol. 65, no. 042320, **(2002)**.
[13] L. Xiao, G. L. Long, F. G. Deng and J. W. Pan, Phys. Rev. A, vol. 69, no. 052307, **(2004)**.
[14] X. H. Li, *et al.*, J. Phys. B, vol. 39, no. 1975, **(2006)**.
[15] Z. X. Man, Y. J. Xia and N. B. An, Eur. Phys. J. D, vol. 42, no. 333, **(2007)**.
[16] J. Bogdanski, N. Rafiei and M. Bourennane, Phys. Rev. A, vol. 78, no. 062307, **(2008)**.
[17] A. Beige, B. G. Englert, C. Kurtsiefer and H. Weinfurter, Acta.Phys. Pol. A, vol. 101, no. 357, **(2002)**.
[18] F. L. Yan and X. Zhang, Eur. Phys. J. B, vol. 41, no. 75, **(2004)**.
[19] Z. X. Man, Z. J. Zhang and Y. Li, Chin. Phys. Lett., vol. 22, no. 18, **(2005)**.
[20] X. H. Li, F. G. Deng, C. Y. Li, Y. J. Liang, P. Zhou and H. Y. Zhou, J. Korean Phys. Soc., vol. 49, no. 1354, **(2006)**.
[21] K. Boström and T. Felbinger, Phys. Rev. Lett., vol. 89, no. 187902, **(2002)**.
[22] F. G. Deng, G. L. Long and X. S. Liu, Phys. Rev. A, vol. 68, no. 042317, **(2003)**.
[23] C. Wang, F. G. Deng and Y. S. Li, Phys. Rev. A, vol. 71, no. 044305, **(2005)**.
[24] A. D. Zhu, Y. Xia, Q. B. Fan and S. Zhang, Phys. Rev. A, vol. 73, no. 022338, **(2006)**.
[25] J. Wang, H. Q. Chen, Q. Zhang and C. J. Tang, Acta. Phys. Sin., vol. 56, no. 673, **(2007)**. (in Chinese)
[26] S. Lin, Q. Y. Wen, F. Gao and F. C. Zhu, Phys. Rev. A, vol. 78, no. 064304, **(2008)**.
[27] M. J. Wang and W. Pan, Chin. Phys. Lett., vol. 25, no. 3860, **(2008)**.
[28] D. X. Quan, C. X. Pei, D. Liu and N. Zhao, Acta. Phys. Sin., vol. 59, no. 2493, **(2010)**. (in Chinese)
[29] G. L. Long, C. Wang, Y. S. Li and F. G. Deng, Sci Sin Phys Mech Astron, vol. 41, pp. 332-342. (in Chinese)
[30] W. Y. Hwang, I. G. Koh and Y. D. Han, Phys. Lett. A, vol. 244, **(1998)**, pp. 489–494.
[31] Z. J. Zhang, Y. Li and Z. X. Man, Phys. Rev. A, vol. 71, no. 044301, **(2005)**.
[32] Q. Y. Cai, Phys. Lett. A, vol. 351, no. 23, **(2006)**.

[33] N. Gisin, *et al.*, Rev. Mod. Phys., vol. 74, no. 145, **(2002)**.
[34] F. G. Deng, G. L. Long, Y. Wang and L. Xiao, Chin. Phys. Lett., vol. 21, no. 2097, **(2004)**.

Authors

Zhao Guoan, was born in Heilongjiang Province of China on February 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 worked in the University he has been engaged in several research and development programs involving communication, systems design, and management information system.

