Advanced Science and Technology Letters
Vol.74 (ASEA 2014), pp.96-100
http://dx.doi.org/10.14257/astl.2014.74.18

One-way Quantum Secure Communication Protocol based on Single-photon

Zhao Guoan[1]

[1]School of Network Education, Beijing University of Posts and Telecommunications, Beijing 100876, China

Abstract. 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 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

1 Introduction

Quantum communication is one of the main focuses in the quantum information research. It has a good application prospect. In 1984, Bennett put forward Quantum Key Distribution Protocol (short for BB84). 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. In 1991, Ekert first brought out QKD Protocol based on entangled particles. In 1992, Bennett proposed a brief QKD Scheme based on a group of non orthogonal states, short for B92. These and references[4-10] have discussed QKD. Among them, quantum communication also concludes: Quantum Secret Sharing[12-16],Quantum Secure Communication [17-28],Quantum Encryption Algorithm, Quantum Authentication and Signature, Quantum Network Communication Protocol and so on. In 2002, Bostrom and Felbinger explored the ideas of quantum entanglement and quantum dense coding to propose “Ping-pong” Protocol[21]. In 2003, Deng and Long utilized block transmission thought and based on dense coding theory and entanglement pair to put forward Two-step QSDC Scheme[22]. In 2004, Yan brought out the relative scheme. In 2005, Wang proposed high dimension QSDC Scheme[23] with quantum dense coding; Zhu put forward QSDC Protocol[24] based on particle order rearrangement; Wang brought out multi-party controlled 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 QSDC.

ISSN: 2287-1233 ASTL

Single particle again becomes one of the ideal information carriers in the quantum communication 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, such as QKD Scheme in B92[3]; QKD Scheme with measuring base encryption by Hwang; Multi-party QSS[32] Scheme based on a disposable pad protocol expension of the single-photon; Quantum Communication Scheme[20] based on single-photon and confirmation of non-maximally entangled state. Recently, Quan and Pei have brought up a new Quantum Security Communication Protocol (QPLZ)[28] in which 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 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. Therefore, how to test the existence of eavesdroppers faster and more exactly and guarantee the effective transmission of secret messages are the research direction, but the necessary auxiliary information is only transmitted by a classics channel. From that, based on single-photon sequence and XOR operation, we propose unidirectional quantum security communication protocol that confuses eavesdroppers. The encoding rule of communication protocol has adopted: Z based: $|H\rangle = |0\rangle = 0$, $|V\rangle = |1\rangle = 1$, X based: $|u\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = 0$, $|d\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = 1$.

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 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 o 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 protocol 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, 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, 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[33] and delay photon attack[34], 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[35] 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.

The new protocol is similar to Deng’s BB84 Protocol based on delay measurement and Li’s Quantum Security Communication Protocol based on any d dimenssion single-photon. Compared to that of Li’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 further 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 further.

3 Conclusion

In conclusion, the unidirectional quantum security communication protocol based on single-photon has not only inherited the advantages of QPLZ, such as easy to realize, high transmission efficiency, double communication distance and so on, but also overcomed some shortcomings. 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. In conclusion, the protocol is not only safe, semantic confusion.

References

1. Bennett C H, Brassard G. 1984 Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing Bangalore, India, December, 1984 p175-179
2. A. K. Ekert 1991 Phys. Rev. Lett. 67 661
3. C. H. Bennett 1992 Phys. Rev. Lett. 68 3121-3124
4. C. H. Bennett, G. Brassard, and N. D. Mermin 1992 Phys. Rev.Lett. 68 557
5. N. Gisin et al. 2002 Rev. Mod. Phys. 74, 145
6. G. L. Long, X. S. Liu 2002 Phys. Rev. A 65 032302
7. F. G. Deng, G. L. Long 2003 Phys. Rev. A 68 042315
8. Wang X B 2005 Phys. Rev. A 72 012322
9. He G Q, Yi Z, Zhu J, Zeng G H 2007 Acta Phys. Sin. 56 6427(in Chinese)
10. Zhao Y B, Heid M, Rigas J, Lütkenhaus N 2009 Phys. Rev. A 79 012307
11. Hillery M, Bužek V, Berthiaume A 1999 Phys. Rev. A 59 1829
12. Karimipour V, Bahraminasab A 2002 Phys. Rev . A 65 042320
13. L. Xiao, G. L. Long, F. G. Deng, and J. W. Pan 2004 Phys. Rev. A 69 052307
14. X.H. Li et al. 2006 J. Phys. B 39 1975
15. Man Z X, Xia Y J, An N B 2007 Eur. Phys. J. D 42 333
16. Bogdanski J, Rafiei N, Bourennane M 2008 Phys. Rev. A 78 062307
17. Beige A, Englert B G, Kurtsiefer C, Weinfurter H 2002 Acta.Phys. Pol. A 101 357
18. F. L. Yan and X. Zhang 2004 Eur. Phys. J. B 41 75
19. Man Z X, Zhang Z J, Li Y 2005 Chin.Phys.Lett. 22 18
20. Li X H, Deng F G, Li C Y, Liang Y J, Zhou P, Zhou H Y 2006 J. Korean Phys. Soc. 49 1354
21. Boström K, Felbinger T 2002 Phys.Rev.Lett. 89 187902
22. Deng F G，Long G L，Liu X S 2003 Phys. Rev. A 68 042317
23. Wang C，Deng F G，Li Y S 2005 Phys. Rev. A 71 044305
24. Zhu A D，Xia Y，Fan Q B，Zhang S 2006 Phys. Rev. A 73 022338
25. Wang J，Chen H Q，Zhang Q，Tang C J 2007 Acta.Phys. Sin. 56 673 (in Chinese)
26. Lin S，Wen Q Y，Gao F，Zhu F C 2008 Phys. Rev. A 78 064304
27. Wang M J，Pan W 2008 Chin. Phys. Lett. 25 3860
28. Quan D X, Pei C X, Liu D, Zhao N 2010 Acta.Phys. Sin. 59 2493 (in Chinese)