Jurnal Fizik Malaysia Volume 39 Issue 2 (2018) pgs 10001-10006 L.G. Yin

Quantum Secure Direct Communication: A Survey of Basic Principle and Recent Development

Liuguo Yin[a,b], Dong Pan[a,c,d] and Gui-Lu Long[a,c,d]

[a]*Tsinghua National Lab of Inform Sci & Tech, Beijing 100084,China*
[b]*School of Inform Sci Techy, Tsinghua University, Beijing 100084, China*
[c]*State Key Lab of Low-dim Quantum Physics and Department of Phys, Tsinghua University, Beijing 100084, China*
[d]*Innovation Center of Quantum Matter, Tsinghua University, Beijing 100084, China*

(Received: 31.1.2018 ; Published: 18.4.2018)

Abstract. Quantum algorithm puts serious threats to information security. Quantum cryptography offers new solutions to this problem. As an important branch of quantum cryptography, quantum secure direct communication (QSDC) transmits secret information directly through a quantum channel. QSDC has no key, no ciphertext, and eliminates the known security loopholes in traditional secure communication. QSDC has changed the structure of secure communication fundamentally. Here we give a survey of QSDC in terms of principle and recent developments.

Keywords: Quantum Secure Direct Communication, Quantum cryptography, Duality Quantum Computing.

I. INTRODUCTION

Secure communication is vitally important in military, national security and everyday life. Classical cryptography protects information security with computational complexity [1]. However, quantum computer [2-4] puts serious threats to classical cryptography, due to its quantum parallelism [5-8]. To resists the quantum attack, one way is to construct post-quantum protocols in classical cryptography [9]. However, its security against quantum attack has not been proven. In particular, development in quantum algorithm is fast, after some slow period [10]. The use of linear combination of unitaries in duality quantum computing [11-14] offers great flexibility in designing quantum algorithm, for instance the recent quantum algorithms [15-18] all use linear combination of unitaries [19-20]. The security of classical protocols against quantum attack is being actively explored.

Another way is to use quantum cryptography. In quantum communication legitimate users can detect eavesdropping on-site. There are three forms of quantum secure communication, quantum key distribution (QKD) [21], quantum secret sharing [22] quantum secure direct communication (QSDC) [23]. QKD has progressed rapidly [24,25]. QKD based secure communication is a two-stage process. In the first stage, a key is established and in the second stage, the key is used to encrypt the message into ciphertext and then be communicated using a classical communication.

In QSDC, information is sent securely through a quantum channel without setting up a prior key [23,26,27]. The secure direct nature of QSDC makes it an important cryptographic primitive. Protocols of quantum signature [28], quantum dialogue [29,30], and quantum direct secret sharing [31] have been constructed based on QSDC. Recent experimental verifications of the

DL04 QSDC protocol [32] with single photons under noisy channel and QSDC protocols with entangled photons [33] have firmly verified the basic principles of QSDC.

II. STRUCTURE OF SECURE COMMUNICATION AND QSDC

FIGURE 1. Structure of Secure Communications. Key is distributed using secure key distribution channel. Then the key is transferred from the key distribution channel to the communication channel at the sender and receiver's sites. Plaintext from sender Alice is encrypted into ciphertext and the ciphertext is transmitted through a public channel to the receiver Bob. Bob decrypts the ciphertext using the key into plaintext.

The structure of a general secure communication is shown in Figure 1. It consists of two channels, one for key distribution and one for ciphertext transmission. There are four possible security loopholes: 1) an eavesdropper can steal key at the key distribution channel; 2) Eve can steal the key while it is transferred from the key distribution to the communication terminal; 3) Eve can steal the key when it is transferred from the key distribution to the communication terminal at the receiver's site; 4) Eve can steal the ciphertext in the public channel. Loopholes at users' sites are ignored usually, but it may turn out to be a serious problem when the sites become complicated and modern eavesdropping technology becomes more sophisticated. Usually, the key is distributed using the RSA protocol, and the ciphertext is encrypted using the AES protocol. Using QKD, the key distribution is guaranteed with security, but the other security loopholes still remain.

In 2000, Long and Liu proposed the first QSDC protocol using EPR pairs [23]. In QSDC, the legitimate users can not only detect eavesdropping, but also avoid the information leakage when Eve is found. This is due to the use of block data transmission technique proposed in [23]. To better understand the process, we describe briefly the procedure of this protocol.

An EPR pair can be in any one of the 4 states:

$$|\psi 1\rangle = \sqrt{\frac{1}{2}}(|00\rangle+|11\rangle),\ |\psi 2\rangle = \sqrt{\frac{1}{2}}(|00\rangle-|11\rangle),\ |\psi 3\rangle = \sqrt{\frac{1}{2}}(|01\rangle+|10\rangle),\ |\psi 2\rangle = \sqrt{\frac{1}{2}}(|01\rangle-|10\rangle)$$

Alice and Bob agree beforehand that $|\psi 1\rangle$,$|\psi 2\rangle$,$|\psi 3\rangle$ and $|\psi 4\rangle$ are encoded as 00,01,10,11 respectively. Alice produces an ordered N EPR pair sequence, which is denoted by $[(P_1(1), P_1(2)), (P_2(1), P_2(2)), \ldots (P_i(1), P_i(2)),\ldots,(P_N(1), P_N(2))]$, where $P_i(1)$ denotes one particle in the i-th EPR pair, and $P_i(2)$ for the other. The order of these N EPR pairs is maintained throughout the QSDC process. The detailed 4 steps are as follows:

(1) Alice produces an ordered N EPR pair sequence, $[(P_1(1), P_1(2)), (P_2(1), P_2(2)), \ldots,(P_i(1), P_i(2)),\ldots, (P_N(1), P_N(2))]$ according to the message bit sequence. The sequence also contains some checking EPR pairs which are inserted into the sequence randomly.

Alice takes one particle from each EPR pair to form the first ordered particle sequence: [$P_1(1)$, $P_2(1)$, $P_3(1)$, ...,$P_N(1)$]. The rest of the EPR particles form the second ordered particle sequence: [$P_1(2)$, $P_1(2)$, $P_3(2)$, ...,$P_N(2)$]. Alice sends Bob the second ordered particle sequence: [$P_1(2)$, $P_2(2)$, $P_3(2)$, ...,$P_N(2)$].

(2) After Bob receives the second particle sequence, he acknowledges the fact to Alice. Alice chooses some of the particles randomly in the first particle sequence from the checking EPR pairs and performs measurement on the particles randomly in the {0,1}-basis or {+, -}-basis. Alice also notifies Bob the positions of these particles, and Bob performs measurement on the corresponding particles by choosing randomly the {0,1} basis or the {+,-}-basis. Bob stores the rest of the particles of his particle sequence.

Then Bob publicly announces the basis and the outcome of his measurement. Based on these information, Alice and Bob can estimate the error rate, and determine if there exists eavesdropping. If the error rate is below a threshold, say 11%, then they go to step (3), otherwise they terminate the process. This is the first security check.

(3) If they are certain that there is no eavesdropping, then Alice sends Bob the first particle sequence: [$P_1(1)$, $P_2(1)$, $P_3(1)$, ...,$P_i(1)$]. Of course, the particles that have been measured are dropped from this particle sequence.

After Bob receives this particle-sequence, he pairs up the particles from the two particle sequences in the right order and performs Bell-basis measurement on them. He records the results of these measurements.

(4) Alice then asks Bob to announce the measurement results of the remaining checking particles to estimate the error rate. If the error rate in this check is below the threshold, then the Bell-basis measurement results are the transmitted message. Then the direct communication is completed. This step is the second security check to ensure the transmission of the first ordered sequence is not eavesdropped so that the information transmitted is correct. In this step, Eve's action can ony destroy, but not steal the transmitted information.

The structure of secure communication with QSDC is given in Figure 2. In QSDC, there is no key distribution, no ciphertext transmission, and all the four security loopholes associated with traditional secure communications are eliminated. In particular, the structure of secure communication has been changed fundamentally. There is only one quantum channel.

Subsequently, other QSDC protocols were proposed, e.g., the two-step QSDC [26], where the information is encoded in quantum operation, and the DL04 QSDC protocol [27], which uses single photons instead of entangled photon pairs.

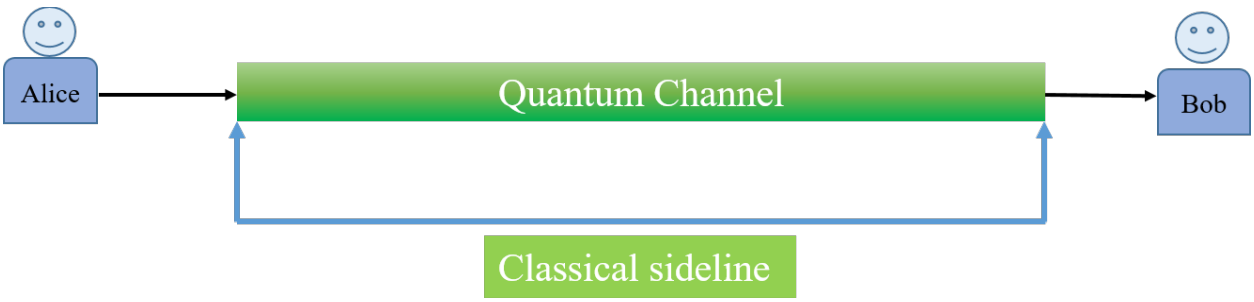

FIGURE 2. Structure of Secure Communication with QSDC. It has fundamentally changed the structure of secure communication. There is no key, no ciphertext. QSDC has eliminated all the four security loopholes in secure communication. The classical sideline is used to exchange the information of the eavesdropping check.

III. CURRENT STATUS AND PERSPECTIVE

Quantum computer attacks of classical cryptography is a big threat. Quantum algorithms with product of unitary operations, represented by the quantum factorization algorithm and quantum search algorithm, have achieved breakthroughs and greatly pushed forward the study of quantum information. However, the restriction of product of unitary operations hindered the use of skills and techniques in classical algorithms design. The duality quantum computing formalism allows the use of linear combination of unitary operations in quantum computing, and it bridges the gap between quantum and classical algorithms, and opens a new way for constructing quantum algorithms. Recent development in quantum algorithms has already shown the power of such formalism. It is expected that it will be extensively used in quantum computers, when practical quantum computers become available.

QSDC has been developed steadily over the past 17 years. Experimental demonstration and implementation of the QSDC protocols are the main focus of current researches. The single-photon based DL04-QSDC protocol has been experimentally demonstrated over the years, firstly with the N=1 special case in ref. [34]. In 2013, the Beijing University of Posts and Telecommunication group [35] has demonstrated a quantum secret sharing scheme [36] which is based on the DL04-QSDC protocol. In 2016, Shanxi University and Tsinghua University joint group has proposed DL04 QSDC protocol with frequency coding, which can resist both loss and error in a noisy environment, and demonstrated it experimentally [37]. Recently, the USTC and Nanjing University of Posts and Telecommunication joint group has just realized the entanglement-based QSDC protocols [23,26] using the state-of-the-arts quantum memory [33]. Last year, another group has just demonstrated the two QSDC protocols [23,26] in long-distance fiber [38]. These experiments have pushed the progress of experimental QSDC greatly. They have been reported not only academic professional websites such as in phys.org [39] and MIT technology review [40], but also by security experts [41,42] and the US national security website [43,44].

It should be pointed out that QSDC can be implemented with the current technology with comparable performance parameters such as communication rate and distance as QKD. Quantum memory is the key device for long-distance QSDC and QKD. As there has been no sophisticated quantum memory, optical fiber delay is the practical substitute for quantum memory. It is estimated that the distance of QSDC using single photons is about a quarter of the distance of the BB84 QKD protocol, and about half of the distance of QKD with entanglement. Practical implementation of QSDC will be the major task in the near future. Theoretically, security proof with explicit threshold of errors are also important subject of study.

IV. CONCLUSION

QSDC is a new form of secure communication. It is distinctive of three “No”s and one “new”: it has No secret keys, No ciphertext, No known security loopholes, and it establishes a new structure of secure communication. Because it does not use key, the security loophole in the key distribution channel is eliminated, and the security loophole in the key storage and transition is eliminated, and the security loophole in the ciphertext attack is eliminated. Many of the security disasters are because of human errors. QSDC decreases the human factor to a minimum, and it has a big advantage in the security. Meanwhile, as quantum technology, in particular, quantum key distribution, is developing fast and is ready for practical application, it is time to study

QSDC, the new generation of perfect secure communication [40]. Currently, a working prototype of QSDC is being built in Tsinghua. QSDC could be very useful in some special operation tasks [41]. We expect more development in QSDC in the near future.

ACKNOWLEDGMENTS

This work was supported by National Natural Science Foundation of China under Grant Nos. 11175094 and 91221205, and the National Basic Research Program of China under Grant No. 2015CB921001.

REFERENCES

1. R. Rivest, A. Shamir and L. Adleman, *Communications of the ACM*, **21**:120-126 (1978).
2. P. Benioff, *Journal of statistical physics*, **22**(5): 563-591 (1980).
3. M. Yuri. Vychislimoe i nevychislimoe (in Russian), *Sov. Radio*. pp. 1315 (1980).
4. R. P. Feynman, *Int. J. Theor. Phys.*, **21** (6): 467-488 (1982).
5. D. Deutsch, *Proceedings of the Royal Society of London A.*, **400** (1818): 97117 (1985).
6. P. W. Shor, *SIAM review*, **41**(2): 303-332 (1999).
7. L. K. Grover, *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing. ACM*: 212-219. (1996).
8. G. L. Long, *Physical Review A*, **64**(2): 022307 (2001).
9. D. J. Bernstein, J. Buchmann, and E. Dahmen, eds. *Springer Science & Business Media*, (2009).
10. P. W. Shor, *Journal of the ACM (JACM)*, **50**(1): 87-90 (2003).
11. G. L. Long, *Communications in Theoretical Physics*, **45**(5): 825 (2006).
12. G. L. Long and Y. Liu. *Communications in Theoretical Physics*, **50**(6): 1303 (2008).
13. G. L. Long, Y. Liu, C. Wang. *Communications in Theoretical Physics*, **51**(1): 65 (2009).
14. G. L. Long, International Journal of Theoretical Physics, 2011, **50**(4): 1305-1318.
15. A. W. Harrow, A. Hassidim and S. Lloyd, *Physical review letters*, **103**(15): 150502 (2009).
16. A. M. Childs and N. Wiebe, *Quantum Information and Computation*, **12**(11&12), 0901–0924 (2012).
17. D. W. Berry et al., *Physical review letters*, **114**(9): 090502 (2015).
18. S. J. Wei, D. Ruan and G. L. Long, *Scientific Reports*, **6**: 30727 (2016).
19. S. J. Wei and G. L. Long. *Quantum Information Processing*, **15**(3): 1189-1212 (2016).
20. S. J. Wei et al., *2017 IEEE 85th VTC Conference (QCFN)* (2017).
21. C. H. Bennett and G. Brassard, *Int Conf Comp, Syst & Signal Proc*, Bangalore, India, Dec 9-12 (1984).
22. M. Hillery, V. Buzek and A. Berthiaume. *Physical Review A*, **59**(3): 1829 (1999).
23. G. L. Long and X. S. Liu, *Physical Review A*, **65**(3): 032302 (2002).
24. B. Korzh et al., *Nat Photonics*; **9**: 163-168 (2015).
25. S. K. Liao et al., *arXiv preprint* arXiv:1707.00542 (2017).
26. F. G. Deng, G. L. Long and X. S. Liu, *Physical Review A*, **68**(4): 042317 (2003).
27. F. G. Deng and G. L. Long, *Physical Review A*, **69**(5): 052319 (2004).
28. C. S. Yoon et al., *Phys. Scr.*; **90**: 15103-15108 (2015).
29. G. Gao, *Opt. Comm.*, **283**: 2288-2293 (2010).
30. C. Zheng C and G. F. Long, *Sci China-Phys Mech Astron*, **57**:1238-1243 (2014).
31. Z. J. Zhang, *Phys Lett A*, **342**: 60-66 (2005).

32. J. Y. Hu et al., *Light: Science & Applications*, **5**(9): e16144 (2016).
33. W. Zhang et al., *Physical Review Letters*, **118**(22): 220501 (2017).
34. A. Cere, et al., *Physical Review Letters*, **96**(20): 200501 (2006).
35. K. J. Wei, H. Q. Ma and J. H. Yang, *Optics Express*, **21**(14): 16663-16669 (2013).
36. F. G. Deng, H. Y. Zhou and G. L. Long. *Journal of Physics A: Math & Gen*, **39**(45): 14089 (2006).
37. J. Y. Hu et al., *Light: Science & Applications*, **5**(9), e16144 (2016).
38. F. Zhu et al., *Science Bulletin*, **62**(22), 1519 (2017).
39. Lisa Zyga, Physicists use quantum memory to demonstrate quantum secure direct communication. https://phys.org/news/2017-06-physicists-quantum-memory.html
40. Quantum Breakthrough Heralds New Generation of Perfectly Secure Messaging. Mittechnology Review, November 1, 2017. https://www.technologyreview.com/s/609294/quantum-breakthrough-heralds-new-generation-of-perfectly-secure-messaging/
41. Joel Harding, Two things struck me instantly. https://toinformistoinfluence.com/2017/06/14/physicists-use-quantum-memory-to-demonstrate-quantum-secure-direct-communication/
42. R. C. Porter, China has a breakthrough in spy-proof quantum communications. https://fortunascorner.com/2017/11/10/china-breakthrough-spy-proof-quantum-communications/
43. R. C. Porter, 'Unhackable' internet breakthrough as scientists develop new quantum teleportation tests to prevent 'eavesdropping', "China Has A Breakthrough In Spy-Proof Quantum Communications". https://fortunascorner.com/2018/01/06/unhackable-internet-breakthrough-scientists-develop-new-quantum-teleportation-tests-prevent-eavesdropping/
44. Patrick Tucker, China Has A Breakthrough in Spy-Proof Quantum Communications, Defenceone.com (US National Security Website), 9, November, 2017. http://www.defenseone.com/technology/2017/11/china-has-breakthrough-spy-proof-quantum-communications/142415/