A Letters Journal Exploring the Frontiers of Physics

January 2020

EPL, **129** (2020) 10004
doi: 10.1209/0295-5075/129/10004

www.epljournal.org

Security proof of the two-way quantum secure direct communication with channel loss and noise

Jian-Yong Hu, Liu Yang, Shu-Xiao Wu, Rui-Yun Chen, Guo-Feng Zhang, Cheng-Bing Qin, Lian-Tuan Xiao[a] and Suo-Tang Jia

State Key Laboratory of Quantum Optics and Quantum Optics Devices, Institute of Laser Spectroscopy, and Collaborative Innovation Center of Extreme Optics, Shanxi University - Taiyuan 030006, China

received 31 October 2019; accepted in final form 15 January 2020
published online 14 February 2020

PACS 03.67.Hk – Quantum communication
PACS 03.67.-a – Quantum information
PACS 03.67.Dd – Quantum cryptography and communication security

Abstract – Quantum secure direct communication is one of the major branches of quantum cryptography, which sends secret information through a quantum channel directly without setting up a prior key. Over the past decade, numerous protocols have been proposed, and some of them have been experimentally demonstrated. The two-way protocol is seen as one of the most practical protocol; in this paper, we present the security proof of the two-way quantum secure direct communication protocol when the noisy and lossy channel is taken into account.

Introduction. – Quantum communication enables two remote parties to share secret information securely over a long distance [1]. Since the pioneering protocol was presented by Bennett and Brassard [2], different modes of quantum communication have been developed, such as quantum key distribution (QKD), quantum secret sharing, quantum secure direct communication (QSDC), quantum teleportation, quantum dense coding, and so on [2–6].

QSDC is one of the important modes of the quantum communication; in contrast to QKD, QSDC sends secret information directly through a quantum channel without setting up a prior key, which eliminates further security loopholes associated with key management and ciphertext attacks [7]. Since the first QSDC protocol was proposed [4], it has become one of the hot research topics in quantum communication over the past decade [8–19]. To the entanglement carriers, in 2003, Deng, Long and Liu proposed the two-step QSDC protocol where the criteria for QSDC were explicitly stated [20]. QSDC protocols based on high-dimensional entanglement, multipartite entanglement, and hyperentanglement were developed [21–25]. To the single-photon carriers, the first QSDC protocol was proposed in ref. [26], the so-called DL04 protocol; its feasibility had been demonstrated in [27–29]. Wei Zhang *et al.* carried out a QSDC experiment with quantum memory [30]. Ruoyang Qi *et al.* implemented the experiment with the help of low-density parity-check code [31]. In addition, protocols of quantum signature, quantum dialogues, and quantum direct secret sharing have been constructed based on QSDC [32–34].

In the practice, the channel loss and noise would cause errors of the information when each information bit is encoded in an individual photon [35]. Therefore, the QSDC protocol which uses a block transmission technique was proposed by Long and Liu, in which the quantum information carrier such as single-photons or Einstein-Podolsky-Rosen entanglement pairs are transmitted in blocks [4]. However, if the quantum channel is a noisy channel, Eve can always gain a certain number of qubits by hiding her presence in the channel noise. The information leakage may be eliminated by using quantum privacy amplification [36]. Unfortunately, quantum privacy amplification ruins the direct communication picture as it involves the merger and order reshuffling of qubits.

An efficient way to implement QSDC in the noisy and lossy channel is to use the forward error correction (FEC) code. In previous works, a FEC code, named frequency coding scheme, was used in the two-way QSDC [37–42] to overcome the channel loss and noise [27,43]. In this work, we present a security proof of the two-way QSDC protocol.

Modified two-way QSDC protocol. – Suppose that Alice is going to send a secret message $\boldsymbol{M}$ to Bob. The modified two-way QSDC protocol works as follows.

[a]E-mail: xlt@sxu.edu.cn

1) Qubits preparation. Bob prepares a block of qubits, each of them is randomly in one of the four states $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|-\rangle$, where $|0\rangle$ and $|1\rangle$ are the eigenstates of the Pauli $\boldsymbol{Z}$ operator, and $|\pm\rangle = (|0\rangle \pm |1\rangle)/2$ are the eigenstates of the Pauli $\boldsymbol{X}$ operator. Then Bob sends the qubits to Alice, Alice acknowledges this fact.

2) Encoding. Alice randomly selects part of the qubits for attack detection (control mode). Alice measures the qubits by randomly choosing the $\boldsymbol{X}$ or $\boldsymbol{Z}$ bases. Then the measurement bases and results are announced through a public channel. Alice and Bob throw away the cases if different bases were used. The remaining cases are kept for estimating the error rate. If the error rate is higher than the pre-set threshold, they will abort the communication. Otherwise, the remaining qubits are used for encoding (encoding mode). Alice firstly executes data compression for the secret message, then encodes the message on a codeword with a FEC code [44], and sends it to Bob. The coding scheme is pre-negotiated and properly designed according to the error rate measured in the control mode. Here, bit 0 is encoded with the identity operation $I = |0\rangle\langle 0| + |1\rangle\langle 1|$ and bit 1 with $U = i\sigma_{\rm y} = |0\rangle\langle 1| - |1\rangle\langle 0|$.

3) Decoding. Bob measures the qubits on the same basis he used for preparing the qubits and decodes the message.

In this modified two-way protocol, before encoding the secret message on qubits, Alice firstly executes data compression, and the FEC code is used for encoding. We will show that they are necessary for the security of transmission.

Security analysis. – The security analysis in this section draws on the work in refs. [45–48].

In step 1) of the above protocol, the state Bob prepared is a complete mixed state, the density operator $\rho^{\rm B} = (|0\rangle\langle 0| + |1\rangle\langle 1|)/2$. To know Alice's encoding operation, Eve has to figure out the quantum state before and after the encoding. Therefore, Eve has to attack the qubits on both the channel M_1 (Bob→Alice) and M_2 (Alice→Bob). Eve's most general operation can be described by a unitary operation together with an ancilla

$$\begin{aligned} U|0\rangle|\varepsilon\rangle &= c_{00}|0\rangle|\varepsilon_{00}\rangle + c_{01}|1\rangle|\varepsilon_{01}\rangle, \\ U|1\rangle|\varepsilon\rangle &= c_{11}|1\rangle|\varepsilon_{11}\rangle + c_{10}|0\rangle|\varepsilon_{10}\rangle, \\ U|+\rangle|\varepsilon\rangle &= c_{++}|+\rangle|\varepsilon_{++}\rangle + c_{+-}|-\rangle|\varepsilon_{+-}\rangle, \\ U|-\rangle|\varepsilon\rangle &= c_{--}|-\rangle|\varepsilon_{--}\rangle + c_{-+}|+\rangle|\varepsilon_{-+}\rangle, \end{aligned} \tag{1}$$

where c_{ij}, $(i,j = 0,1,+,-)$ are non-negative real numbers, $|\varepsilon\rangle$ represents Eve's ancillary state. After Eve's attack in the main channel M_1, the joint state of the qubits and Eve's ancillas is

$$\rho_{M_1}^{BE} = U(\rho^B \otimes |\varepsilon\rangle\langle\varepsilon|)U. \tag{2}$$

In the encoding mode, instead of encoding random numbers on the qubits just like QKD, in QSDC, secret information is encoded on the qubits directly, which may decrease the entropy of the qubits. For instance, the maximum entropy of a 26 character source is $H_{\max} = \log_2(1/26) = 4.7\,\text{bit/symbol}$. However, the English language makes uneven use of characters. The entropy $H \approx 4.2$ bit/character, therefore the efficiency of the alphabet is around 0.89. In our protocol, we assume that Alice encodes 0 and 1 on qubits with probability P_0 and $1 - P_0$, respectively. The joint state of the encoded qubits and Eve's ancillas becomes

$$\rho^{ABE} = P_0|0\rangle\langle 0| \otimes \rho_{M_1}^{BE} + (1 - P_0)|\rangle\langle 1| \otimes U\rho_{M_1}^{BE}U^\dagger. \tag{3}$$

According to Shannon's information theory, in the asymptotic scenario, one can always find a coding scheme for data compression to make P_0 arbitrarily approach 1/2. As we described in step 2), data compression is implemented before encoding, therefore, without loss of generality, here we assume $P_0 = 1/2$. After Alice's encoding operation, the encoded qubits are sent back to Bob. The security capacity $C_{\rm s}$ is bounded by the conditional entropy of qubits that Alice sends to Bob given the quantum information of Eve, $C_{\rm s} = S(\rho^{\rm A}|\rho^{\rm BE})$, where $S(\rho^{\rm A}|\rho^{\rm BE}) = S(\rho^{\rm ABE}) - S(\rho^{\rm BE})$. Given that, the secrecy capacity per qubit is

$$C_{\rm s} = 1 - h(\xi), \tag{4}$$

where $\xi = c_{++}^2 - c_{01}^2$, and $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the binary Shannon entropy function. Here we assume that $c_{++}^2 = c_{--}^2$, $c_{01} = c_{10}$ and $c_{00}^2 = c_{11}^2$.

For practical quantum channels, channel loss and noise should be considered. In the control mode, Alice and Bob estimate the error rate in the main channels M_1. Here we assume that the error rate in the main channel M_2 is the same as in the channel M_1. Actually, since the main channels M_1 and M_2 could be the same fiber link, the polarization drift would be compensated automatically, therefore the error rate at Bob's side should be even smaller. In the asymptotic scenario, the secrecy capacity per qubit is

$$C_{\rm s} \leq \{t(1 - h(e)) - t_1 h(\xi)\}, \tag{5}$$

where $t_1 = 10^{-\alpha L/10}$ is the transmittance of the main channel M_1, α is the fiber attenuation coefficient, L is the length of the main channel $M_1 \cdot t = t_1 \cdot t_2$, and $t_2 = t_1$ is the transmittance of the channel M_2. Figure 1 presents the relationship of the secrecy capacity and the communication distance for different error rates. It shows that, in the two-way QSDC protocol, the communication distance is sensitive to the error rate measured in control mode, the maximum communication distance decreases rapidly with the increase of the error rate.

Discussion. – According to Shannon's information theory once the secrecy capacity $C_{\rm s} > 0$, Alice can always find out a code scheme to transmit a secret message over the quantum channel with security and reliability.

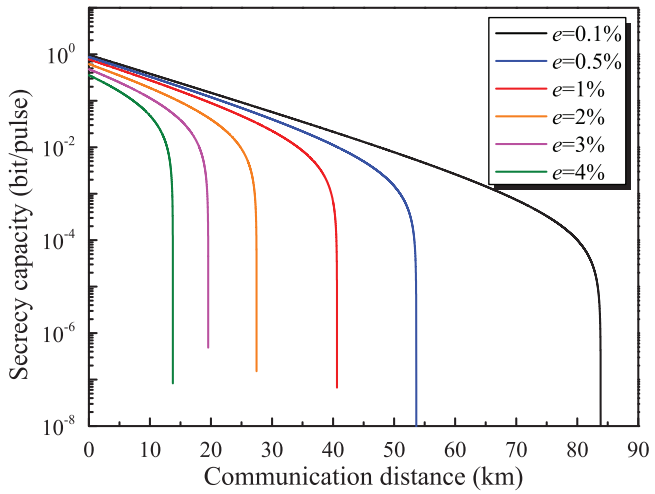

Fig. 1: Secrecy capacity *vs.* communication distance. Here we set the fiber attenuation coefficient $\alpha = 0.2\,\mathrm{dB/km}$.

In step 2) of the protocol, after the data compression, Alice collects K bits $\boldsymbol{M}$ out of the data stream. Then she maps $\boldsymbol{M}$ onto a codeword $\boldsymbol{X}$ of length $N(N > K)$. Assume the main channel is a binary symmetric channel with crossover probability $p_{(1|0)} = p_{(0|1)} = q$ and also a binary erasure channel with erasure probability $1 - t$. If the encoded qubits are lost during the transmission, Bob knows nothing about Alice's encoding operation. Therefore, after the transmission of the main channel, the entropy per qubit is

$$H_B = t[-q\log q - (1-q)\log(1-q)] + (1-t). \tag{6}$$

The codeword $\boldsymbol{X}$ is constructed by N qubits, which can be seen as a point in an N-dimensional Hamming space. At the receiving end, it changes to a Hamming sphere $\boldsymbol{Y}$ because of channel loss and noise. Only 2^K vectors out of 2^N possible vectors are used as typical codewords. Properly choosing the codewords could detect and even correct the error bits. In order to decode the message correctly, the Hamming distance d of each codeword should be bigger than NH_B; in addition,

$$2^{NH_B} \cdot 2^{NR} \leq 2^N. \tag{7}$$

That is

$$0 \leq R \leq C \equiv 1 - H_B, \tag{8}$$

where $R = K/N$ is the transmission efficiency, C is the channel capacity. Intuitively, in a very high dimensional binary space, while two spheres of radius r whose centers are a distance d apart have a non-zero volume of intersection for any r greater than $d/2$, the fractional overlap is vanishingly small provided that $r < d$. According to the noisy-channel coding theorem, when $N \to \infty$, if $R < C$, there always exists a coding scheme such that the information can be transmitted over the channel with an arbitrarily small frequency of errors.

Because of channel noise of the main channel M_1, part of the qubits may leak to Eve as we discussed above. Therefore, Eve can be seen as a receiver connected by a channel with erasure probability $1 - t_E$, which means Eve knows $N \cdot t_E$ qubits of information. To consider the worst case, Eve uses a channel without noise and loss. The amount of information about the qubit sequence that Eve can get is limited by the error rate in the control mode. The Hamming radius of her Hamming sphere is $NH_E/2$, where $H_E = 1 - t_E$, and the Hamming radius of Bob's Hamming sphere is $NH_B/2$. To transmit information securely and reliably, the Hamming distance between each codeword that Alice used for encoding must be bigger than NH_B. To transmit information securely, the following condition must be satisfied:

$$\frac{N \cdot H_E}{N \cdot H_B} > 2. \tag{9}$$

The condition of eq. (9) assures the secret bit rate could be positive.

When the radius of Eve's Hamming sphere is three times that of Bob's, Eve cannot distinguish adjacent typical codewords; here the adjacent typical codewords means the typical codewords which has the shortest Hamming distance. Although the maximum transmission capacity of the main channel is NR, to guarantee the security of information transmission only one bit of the secret message could be encoded on the block, and the information bit should be encoded on the adjacent typical codewords. With the increase of the radius of Eve's Hamming sphere, more information bits could be encoded on the block of qubits. The mean secrecy capacity per qubit is

$$C_{\mathrm{s}} = H_E - H_B. \tag{10}$$

The highest efficiency could be achieved when t_E =0 and $t = 1$. If $t < 1$, the security of information transmission is guaranteed at the expense of encoding efficiency. This is similar to the privacy amplification in the QKD.

Comparing with quantum key distribution. Compared with the QKD protocol, the QSDC protocol shows some advantages and disadvantages. Firstly, in the QSDC protocol, a FEC code is needed for secure information transmission; here, the FEC code can also be seen as one of the privacy amplification methods. The difference of FEC code with the privacy amplification method used in the previous QKD protocol is that the FEC code combined the privacy amplification, error correction and one time pad all together. For ideal cases, the error rate could be set to zero, and one time pad would not change the security capacity, therefore the security capacity of the two-way QKD protocol and two-way QSDC protocol with FEC code should be the same. Secondly, all the QSDC protocols could be used as QKD protocols, one just need to replace the secret message with a sequence of random numbers. However, not all the QKD protocols can be used as a QSDC protocol, which means QSDC has the potential to perform the task the QKD cannot do, for example building up the full quantum network. Furthermore,

QSDC does not need complicated key management and also post processing. Nevertheless, there are also some disadvantages for QSDC compared with QKD. For example, in QSDC, a FEC code is needed which may not be easier than the post processing in QKD. Besides, in QKD, one just needs to care about the qubits that are detected by the receiver; the lost qubits would not be used to generate key, therefore the mutual information between Alice and Eve decreases with the length of the communication distance just like the mutual information between Alice and Bob. However, in QSDC, since the secret message is encoded on the qubits, one should care about the encoded qubits that are sent out. For instance, the channel M_1 and M_2 is a noisy and lossy channel, which means the mutual information I(A;B) would decrease with the length of the channel; however, Eve's channel could be a lossless channel, that is, the mutual information between Alice and Eve would not change with the length of channel M_2. This would make the secrecy capacity of QSDC decline faster than QKD with the increasing of the length of the channel. From this perspective, QKD may have longer communication distance than QSDC.

Conclusion. – In this paper, the security proof of the two-way QSDC protocol is given. It shows that data compression and a FEC code are necessary steps for practical QSDC. Our work could be extended to other QSDC protocols.

* * *

This work is supported by the Natural Science Foundation of China (Nos. 61527824, 11374196, and 61675119) and PCSIRT (No. IRT 13076).

REFERENCES

[1] Yin H.-L. *et al.*, *Phys. Rev. Lett.*, **117** (2016) 190501.
[2] Bennett C. H. and Brassard G., in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York) 1984, pp. 175–179.
[3] Hillery M., Bužek V. and Berthiaume A., *Phys. Rev. A*, **59** (1999) 1829.
[4] Long G.-L. and Liu X.-S., *Phys. Rev. A*, **65** (2002) 032302.
[5] Bennett C. H. *et al.*, *Phys. Rev. Lett.*, **70** (1993) 1895.
[6] Bennett C. H. and Wiesner S. J., *Phys. Rev. Lett.*, **69** (1992) 2881.
[7] Long G.-L., Wang C., Li Y.-S. and Deng F.-G., *Sci. Sin. Phys. Mech. Astron.*, **41** (2011) 332.
[8] Long G.-L. *et al.*, *Front. Phys. China*, **2** (2007) 251.
[9] Zhu Z.-C., Hu A.-Q. and Fu A.-M., *Int. J. Theor. Phys.*, **53** (2014) 1495.
[10] Zhou L., Sheng Y.-B. and Long G.-L., *Sci. Bull.*, **65** (2020) 12.
[11] Cui Z. X., Zhong W., Zhou L. and Sheng Y.-B., *Sci. China Phys. Mech. Astron.*, **62** (2019) 110311.
[12] Niu P.-H. *et al.*, *Sci. Bull.*, **63** (2018) 1345.
[13] Chen S.-S., Zhou L., Zhong W. and Sheng Y.-B., *Sci. China Phys. Mech. Astron.*, **61** (2018) 090312.
[14] Zhu F., Zhang W., Sheng Y.-B. and Huang Y.-D., *Sci. Bull.*, **62** (2017) 1519.
[15] Wu J.-W., Lin Z.-S., Yin L.-G. and Long G.-L., *Quantum Eng.*, **1** (2019) e26.
[16] Gao Z.-K., Li T. and Li Z.-H., *EPL*, **125** (2019) 40004.
[17] Sheng Y.-B. and Zhou L., *Sci. Bull.*, **62** (2017) 1025.
[18] Sheng Y.-B. and Zhou L., *Phys. Rev. A*, **98** (2018) 052343.
[19] Sun Z. *et al.*, in *2018 IEEE Globecom Workshops (GC Wkshps), Abu Dhabi, United Arab Emirates* (Institute of Electrical and Electronic Engineers) 2018, pp. 1–6.
[20] Deng F.-G., Long G.-L. and Liu X.-S., *Phys. Rev. A*, **68** (2003) 042317.
[21] Wang C. *et al.*, *Phys. Rev. A*, **71** (2005) 044305.
[22] Gao Z.-K., Li T. and Li Z.-H., *EPL*, **125** (2019) 40004.
[23] Wang C., Deng F.-G. and Long G.-L., *Opt. Commun.*, **253** (2005) 15.
[24] Li Y.-B., Song T.-T., Huang W. and Zhan W.-W., *Int. J. Theor. Phys.*, **54** (2015) 589.
[25] Zarmehi F. and Houshmand M., *IEEE Commun. Lett.*, **20** (2016) 10.
[26] Deng F.-G. and Long G.-L., *Phys. Rev. A*, **69** (2004) 052319.
[27] Hu J.-Y. *et al.*, *Light: Sci. Appl.*, **5** (2016) e16144.
[28] Cerè A., Lucamarini M., Giuseppe G. D. and Tombesi P., *Phys. Rev. Lett.*, **96** (2006) 200501.
[29] Hu J.-Y. *et al.*, *Opt. Express*, **26** (2018) 20835.
[30] Zhang W. *et al.*, *Phys. Rev. Lett.*, **118** (2017) 220501.
[31] Qi R.-Y. *et al.*, *Light: Sci. Appl.*, **8** (2019) 22.
[32] Yoon C. S., Kang M. S., Lim J. I. and Yang H. J., *Phys. Scr.*, **90** (2015) 15103.
[33] Gao G., *Opt. Commun.*, **283** (2010) 2288.
[34] Zhang Z.-J., *Phys. Lett. A*, **342** (2005) 60.
[35] Cai Q.-Y., *Phys. Rev. Lett.*, **91** (2003) 109801.
[36] Deng F.-G. and Long G.-L., *Commun. Theor. Phys.*, **46** (2006) 443.
[37] Cai Q.-Y. and Li B.-W., *Chin. Phys. Lett.*, **21** (2004) 601.
[38] Lucamarini M. and Mancini S., *Theor. Comput. Sci.*, **560** (2014) 46.
[39] Han Y.-G. *et al.*, *Sci. Rep.*, **44** (2014) 4936.
[40] Shaari J. S., Lucamarini M. and Mancini S., *Quantum Inf. Process*, **13** (2014) 1139.
[41] Henao C. I. and Serra R. M., *Phys. Rev. A*, **92** (2015) 052317.
[42] Lu H., *Quantum Inf. Process*, **14** (2015) 3827.
[43] Hu J.-Y. *et al.*, *Photon. Res.*, **3** (2015) 24.
[44] Tang J., Wen H., Zeng K., Hu L. and Chen S.-L., in *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall), Toronto, ON* (Institute of Electrical and Electronic Engineers) 2017, pp. 1–5.
[45] Lu H., Fred Fung C.-H., Ma X.-F. and Cai Q.-Y., *Phys. Rev. A*, **84** (2011) 042344.
[46] Fred Fung C.-H., Ma X.-F., Chau H. F. and Cai Q.-Y., *Phys. Rev. A*, **85** (2012) 032308.
[47] Lu H., Fred Fung C.-H. and Cai Q.-Y., *Phys. Rev. A*, **88** (2013) 044302.
[48] Beaudry N. J., Lucamarini M., Mancini S. and Renner R., *Phys. Rev. A*, **88** (2013) 062302.