Received: 12 August 2019 | Accepted: 26 September 2019

DOI: 10.1002/que2.26

Check for updates

ORIGINAL PAPER

WILEY

Security of quantum secure direct communication based on Wyner's wiretap channel theory

Jiawei Wu[1] | **Zaisheng Lin**[2,3] | **Liuguo Yin**[2,3] | **Gui-Lu Long**[1,3,4,5]

[1]State Key Laboratory of Low-Dimensional Quantum Physics and Department of Physics, Tsinghua University, Beijing, China

[2]School of Information and Technology, Tsinghua University, Beijing, China

[3]Beijing National Research Center for Information Science and Technology, Tsinghua University, Beijing, China

[4]Innovative Center of Quantum Matter, Beijing, China

[5]Beijing Academy of Quantum Information Science, Beijing, China

Correspondence
Zaisheng Lin, School of Information and Technology, Tsinghua University, Beijing 100084, China.
Email: bazingalzs137@mail.tsinghua.edu.cn

Funding information
China Aerospace Science and Technology Corporation; National Basic Research Program of China, Grant/Award Number: 2017YFA0303700 and 2015CB921001; National Natural Science Foundation of China, Grant/Award Number: 61727801, 61871257, and 11774197; Key R&D Program of Guangdong Province, Grant/Award Number: 2018B030325002; Beijing Advanced Innovation Center for Future Chip (ICFC)

Summary

Quantum secure direct communication (QSDC) transmits secret messages directly over a quantum channel without the prior distribution of a key. Here, we apply Wyner's wiretap channel theory to analyze the security of QSDC protocols. The ideal protocol is treated as the main channel, and the effect of eavesdropping is treated as the wiretap channel. Entanglement-based QSDC protocols are analyzed in detail at first. We calculated the channel capacity of the wiretap channel, and hence, the secrecy channel capacity of the protocol. The security of single-photon–based QSDC protocols is studied through the equivalence between the entanglement-based protocols and single-photon–based protocols. We present a modified version of the single-photon-based DL04 protocol, which gives a higher secrecy capacity.

KEYWORDS

quantum cryptography, quantum secure direct communication, wiretap channel

1 | INTRODUCTION

In traditional cryptography, distributing a secret key is a vulnerable process. Quantum key distribution (QKD)[1] can ensure the information-theoretic security of the distributed key based on the principle of quantum mechanics, thus ensuring the security of the message transmitted in the classic channel with one-time-pad encryption. An alternative way is to transmit the message in quantum channels directly. Such an idea has motivated a batch of protocols called quantum secure direct communication (QSDC), including the entanglement-based two-step protocols[2,3] and the single-photon–based DL04 protocol,[4] and attracts widespread attention. Multistep QSDC with Greenberger-Horne-Zeilinger state and

 © 2019 John Wiley & Sons, Ltd.

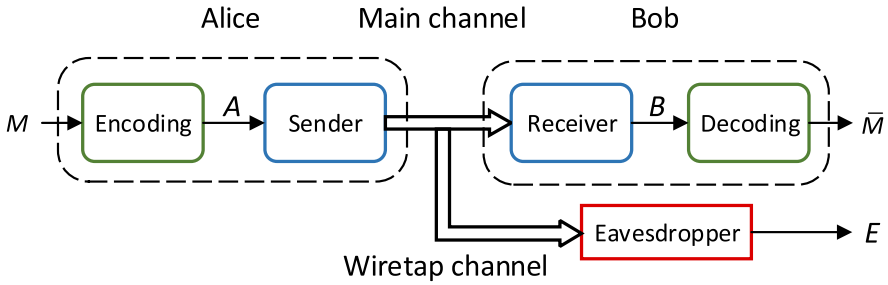

FIGURE 1 The framework of wiretap channel model. The whole quantum part is composed of two channels: the main channel and the wiretap channel. Message M enters the sender's entry after encoding and restore to $\overline{M}$ after the receiver's output and decoding

high-dimension QSDC with superdense coding have been proposed.[5,6] Lum et al explored the use of quantum data locking in QSDC.[7] Massa et al proposed a QSDC protocol where the direction of transmission is anonymous.[8] Shapiro et al investigated the use of quantum low probability of intercept to realize high rate QSDC.[9] Furthermore, the measurement-device-independent protocols for QSDC, which could eliminate security loopholes with imperfect measurement devices, have been proposed.[10-12] Device-independent QSDC protocol, which could eliminate all possible security loopholes associated with imperfect devices, has also been proposed quite recently.[13]

In recent years, there has been remarkable progress in practical realization of QSDC. In 2016, Hu et al completed the first experimental demonstration of DL04 protocol with faint laser, validating the feasibility of QSDC in a noisy environment.[14] The two-step protocol was realized over 0.5-km optical fiber, showing the potential of its long-distance transmission.[15] Zhang et al demonstrated the application of atomic quantum memory in the entanglement-based protocol.[16] However, practical quantum memory is far from available. Sun et al solved the problem by proposing a practical scheme without quantum memory based on classical coding theory.[17]

In contrast to QKD, whose security has been proven over the last two decades,[18-24] the security analysis of QSDC protocols has only recently debuted.[25,26] Qi et al[26] analyzed the security of DL04 QSDC protocol using Wyner's wiretap channel theory,[27] and set up a practical prototype, which can send secure messages directly at a distance of over 1.5 km with a transmission rate of 50 bps.

Since QSDC transmits secret messages directly over quantum channels, post-processing is not possible. Therefore, the security analysis of QSDC is completely different from that of QKD. Fortunately, there are many powerful tools in information theory that can help to complete this task. Wyner's wiretap channel theory proves that there exist coding schemes that can ensure the secure transmission of the messages if the secrecy capacity is greater than zero. The wiretap channel model includes a main channel from Alice to Bob and a wiretap channel from Alice to Eve, as shown in Figure 1. The model gives a secrecy capacity, which is the maximal secure transmission rate between Alice and Bob.

The whole communication process of the two-step protocol[3] includes the quantum part and the classical part. In the quantum part, Alice prepares N Einstein-Podolsky-Rosen (EPR) pairs and sends each half of them to Bob. On receiving the particles, Bob checks the error rates by sampling some of the qubits and measuring them in the σ_x or σ_z bases. Alice encodes her classical bit sequence A on the EPR pairs using dense coding and sends the remaining halves to Bob. Bob decodes the EPR pairs to get sequence B, which is the message received by Bob. The whole quantum part can be treated in a wiretap channel model, in which Alice sends some messages to Bob, while an eavesdropper tries to eavesdrop it. In the classical part, the information of eavesdropping checking is transmitted in a public channel where Eve can get all the information. The secrecy capacity, which is the maximal difference between the capacity of the main channel and the wiretap channel, can be calculated using the parameters from eavesdropping checking. This is in sharp contrast to classical communication where it is almost impossible for legitimate users to acquire the capacity of the wiretap channel. The quantum channel provides a powerful tool to probe eavesdropping, thus gives a tight estimation of the channel capacity.

In the following, we give a proof of the security of two-step QSDC based on the wiretap channel theory and calculate its secrecy capacity. We find that this capacity is slightly smaller than that obtained from the entanglement distillation scheme,[18,19] which is expected because of the complicated quantum processing involved. Wyner's theory is more appealing for practical applications as it does not use the complicated quantum operations as in the quantum distillation process. Moreover, the secrecy capacity of generic single-photon–based QSDC protocols is also obtained through the equivalence between entanglement-based protocols and single-photon–based protocols. Based on the result, we propose some modification on DL04 protocol to increase its secrecy capacity.

This paper is organized as follows. In Section 2, we describe the detailed process of two-step protocol. Then, we estimate the information leakage in the quantum part and give the secrecy capacity of the channel. In Section 3, the security of

DL04 protocol is given. By modifying the DL04 protocol, we can get a larger secrecy capacity. In Section 4, we give a concise summary.

2 | SECURITY ANALYSIS OF THE TWO-STEP QSDC PROTOCOL

The two-step QSDC works as follows.[3]

(1) *Prepare EPR pairs.* Alice prepares $2n$ maximally entangled EPR pairs $|\psi^-\rangle^{\otimes 2n}$, where $|\psi^-\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$. Alice sends each half of the EPR pairs to Bob, which is called system B.
(2) *Eavesdropping checking.* Bob randomly chooses n qubits as check bits and measures them in the bases of σ_z or σ_x randomly. Then, Bob tells Alice the positions of the qubits and measurement bases he has chosen. Alice does the same measurement and shares her results with Bob. They can obtain quantum bit error rates (QBERs) in the two measured bases, ϵ_x and ϵ_z. If the QBERs exceed some threshold, which will be given later, the protocol aborts.
(3) *Dense coding.* Alice applies one of the following four unitary operations to her qubits to encode 00, 01, 10, 11, respectively,

$$\begin{aligned} U_{00} &= I = |0\rangle\langle 0| + |1\rangle\langle 1|, \\ U_{01} &= \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|, \\ U_{10} &= \sigma_x = |1\rangle\langle 0 + |0\rangle\langle 1|, \\ U_{11} &= \sigma_x\sigma_z = |1\rangle\langle 0| - |0\rangle\langle 1|. \end{aligned} \tag{1}$$

Then, she sends them to Bob.
(4) *Decode message.* On receiving the qubits from Alice, Bob combines the two halves of EPR pairs and measures them with Bell basis to obtain the message.

The degree of eavesdropping can be estimated through the QBER. It is worth noting that classical privacy amplification,[28] which is used in QKD, is unsuitable for direct communication because part of intelligible information may be lost. In practical application, forward coding will be implemented.[26] However, we will not go into the details here. In this section, we will estimate the lower bound of the secrecy capacity of two-step protocol.

In a general sense, any secret communication protocol can be treated in a wiretap channel model. For a QSDC protocol, the transmission of messages in the quantum channel between Alice and Bob is modeled as a main channel and the eavesdropping and environmental noises are modeled as a wiretap channel. Then, according to Wyner's wiretap channel theory,[27,29,30] there exists a coding method that allows the secure transmission of information at a rate lower than the secrecy capacity, provided that the secrecy capacity is positive. The secrecy capacity can be calculated as follows:

$$C_s = C_M - C_W, \tag{2}$$

where C_M and C_W are the capacity of the main channel and the wiretap channel, respectively.

To estimate the wiretap channel capacity, we need to analyze the detailed process of eavesdropping. Our analysis follows the method of Renner et al.[21] Firstly, we assume Eve performs a coherent attack. Specifically, Eve attaches her auxiliary system $|E\rangle$ to system B and performs a unitary operation U_{BE}, then she sends system B to Bob. The entire state of system B before the operation is the direct product of independent and identically distributed (i.i.d.) systems, $\rho_B = [(|0\rangle\langle 0| + |1\rangle\langle 1|)/2]^{\otimes 2n}$. If a randomized permutation is applied to the qubits, the joint state of B and E, ρ_{BE}, can be seen as a direct product of i.i.d. subsystems ρ_{BEsub} asymptotically, according to quantum De Finetti theorem.[31] In other words, we can construct a state ρ_{BEsub} to approximate ρ_{BE}: $\rho_{BEsub}^{\otimes 2n} \to \rho_{BE}$. It is sufficient to consider Eve's operation U_{BE} on every subsystem separately, which is the case of collective attack. For convenience, subscript *sub* is neglected in the following discussion.

After the operation of Eve, the state of EPR pair becomes

$$\rho_{AB} = Tr_E(U_{BE}|E\rangle|\psi^-\rangle\langle\psi^-|\langle E|U_{BE}^{\dagger}). \tag{3}$$

To simplify the effect of the attack on the system, we introduce an additional operation that Alice and Bob both apply the same transformation chosen randomly from $I, \sigma_x, \sigma_z, \sigma_x\sigma_z$. Such operation can eliminate all the nondiagonal elements

of ρ_{AB} in Bell basis,[22] then it has the following matrix form in the basis $\{|\psi^-\rangle, |\psi^+\rangle, |\phi^-\rangle, |\phi^+\rangle\}$:

$$\rho_{AB} = \begin{bmatrix} \lambda_1 & 0 & 0 & 0 \\ 0 & \lambda_2 & 0 & 0 \\ 0 & 0 & \lambda_3 & 0 \\ 0 & 0 & 0 & \lambda_4 \end{bmatrix}. \tag{4}$$

Consider a purification $|\psi_{ABE}\rangle$ of state ρ_{AB}

$$|\psi_{ABE}\rangle = \sum_{i=1}^{4} \sqrt{\lambda_i} |\Phi_i\rangle |E_i\rangle, \tag{5}$$

where $|\Phi_i\rangle$ is the Bell state of system AB and $\{|E_i\rangle\}$ is a set of orthogonal states of Eve's auxiliary system. The parameters λ_i are constrained by QBER ε_x and ε_z: $\varepsilon_z = \lambda_3 + \lambda_4, \varepsilon_x = \lambda_2 + \lambda_4$. The state after the dense coding of Alice is $U_a|\psi_{ABE}\rangle$, where $U_a \in \{U_{00}, U_{01}, U_{10}, U_{11}\}$.

Finally, Eve intercepts all the qubits from Alice in the last step to obtain maximal information about the message and measure them, ie, Eve acquires system AE. Tracing out system B from system ABE, we get

$$\rho_{AE} = Tr_B(|\psi_{ABE}\rangle\langle\psi_{ABE}|) = \frac{1}{2}(P_{|\psi_1\rangle} + P_{|\phi_1\rangle}), \tag{6}$$

where $P_{|\psi\rangle}$ is the projection operator of state $|\psi\rangle$ and we have defined

$$\begin{aligned} |\psi_1\rangle \equiv |0\rangle_A \left(\sqrt{\lambda_3}|E_3\rangle + \sqrt{\lambda_4}|E_4\rangle\right) \\ + |1\rangle_A \left(\sqrt{\lambda_2}|E_2\rangle - \sqrt{\lambda_1}|E_1\rangle\right), \\ |\phi_1\rangle \equiv |0\rangle_A \left(\sqrt{\lambda_1}|E_1\rangle + \sqrt{\lambda_2}|E_2\rangle\right) \\ + |1\rangle_A \left(\sqrt{\lambda_4}|E_4\rangle + \sqrt{\lambda_3}|E_3\rangle\right). \end{aligned}$$

The encoded states are

$$\begin{aligned} \rho_{AE,00} &= U_{00}\rho_{AE}U_{00}^\dagger = \frac{1}{2}(P_{|\psi_1\rangle} + P_{|\phi_1\rangle}), \\ \rho_{AE,01} &= U_{01}\rho_{AE}U_{01}^\dagger = \frac{1}{2}(P_{\sigma_x|\psi_1\rangle} + P_{\sigma_x|\phi_1\rangle}), \\ \rho_{AE,10} &= U_{10}\rho_{AE}U_{10}^\dagger = \frac{1}{2}(P_{\sigma_z|\psi_1\rangle} + P_{\sigma_z|\phi_1\rangle}), \\ \rho_{AE,11} &= U_{11}\rho_{AE}U_{11}^\dagger = \frac{1}{2}(P_{\sigma_x\sigma_z|\psi_1\rangle} + P_{\sigma_x\sigma_z|\phi_1\rangle}). \end{aligned}$$

Eve can measure all the subsystems $\rho_{AE,a}$ jointly. However, the information acquired from one subsystem on average in adjoint measurement cannot exceed that in single measurement of one subsystem. To explain this, consider the situation when the classical bit string $\tilde{A}$ is encoded in some manner and assume $\tilde{A} = a_1 a_2 \cdots a_m = \{a_i\}$, with a distribution $p_{\tilde{A}}$, where a_i is a two-bit word. Applying Holevo bound,[32] we get

$$\begin{aligned} I(\tilde{A} : \tilde{E}) &\leq S\left(\sum_{\tilde{A}} p_{\tilde{A}} \rho_{AE,\tilde{A}}\right) - \sum_{\tilde{A}} p_{\tilde{A}} S\left(\rho_{AE,\tilde{A}}\right) \\ &\leq m\left[S\left(\sum_a p_a \rho_{AE,a}\right) - 1\right], \end{aligned} \tag{7}$$

where $\rho_{AE,\tilde{A}}$ is system AE encoded with bit string $\{a_i\}$ and we have assumed each word a_i has the same distribution p_a. Therefore, it is sufficient to estimate the maximum of $I(A : E)$ by analyzing one subsystem. The upper bound on $I(A : E)$

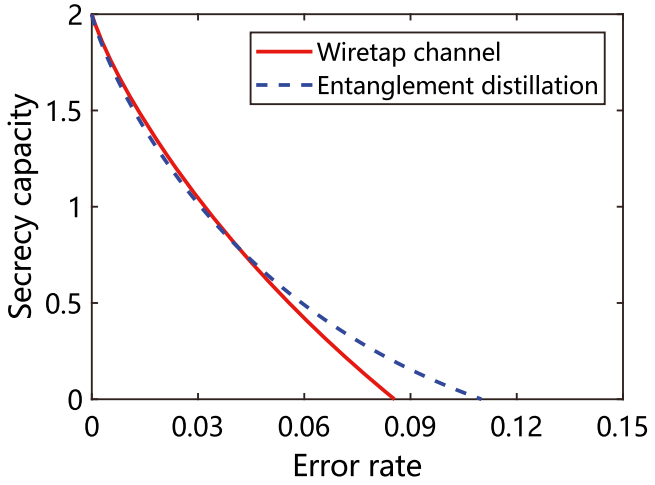

FIGURE 2 Comparison of secrecy capacity between different methods. The horizontal coordinate is the error rate of eavesdropping check, corresponding to the parameter $p/2$ in the depolarizing channel. Note the reception rates Q_B and Q_E are set to 1 in order to simplify the result. The capacity of the wiretap channel method is slightly larger than that of the entanglement distillation method at a low error rate but falls to zero rapidly as the error rate increases. The error rate threshold of the wiretap channel method is 0.086 while that of the entanglement distillation method is 0.110

gives the wiretap channel capacity (see Appendix A for details)

$$C_W = \max I(A : E) \leq h(\varepsilon_x) + h(\varepsilon_z). \tag{8}$$

The capacity of the main channel C_M depends on the bit error rate between classical information A and B. We can reasonably assume that the main channel is a symmetric channel, and then, considering the channel loss, the lower bound of the secrecy capacity is

$$C_s \geq Q_B \left[2 - h_4(\mathbf{e})\right] - Q_E \left[h(\varepsilon_x) + h(\varepsilon_z)\right], \tag{9}$$

where $h_4(\mathbf{e})$ is four-array Shannon entropy, Q_B and Q_E are the reception rates of the main channel and the wiretap channel, respectively, and $\mathbf{e}$ is the error rate distribution of the main channel. The error distribution $\mathbf{e}$ can be obtained through the decoding process.

In addition, the random permutation to reduce coherent attack to collective attack and random local operation to eliminate nondiagonal elements of ρ_{AB} can be removed from the protocol. From the perspective of Alice and Bob, any random operation on system AB will introduce an external auxiliary system. Since the details of the operation are transmitted in the public channel, the auxiliary systems can be utilized by Eve and may increase her power. If the operations above are removed, the secrecy capacity above remains a lower bound.

Another method to ensure security is entanglement distillation originated from the works of Lo and Chau[18] and Shor and Preskill.[19] After the distribution of EPR pairs, they do an additional operation of entanglement distillation according to the result of eavesdropping checking. The achievable efficiency of entanglement distillation is $1-h(\varepsilon_x)-h(\varepsilon_z)$, then the secrecy capacity is $C_s = [1-h(\varepsilon_x)-h(\varepsilon_z)][2-h_4(\mathbf{e})]$, where the second item is the classical capacity between Alice and Bob after entanglement distillation. To make comparison, we can reasonably assume the qubits of each EPR pair go through the same quantum channel independently without loss. If the quantum channel is modeled as a lossless depolarizing channel $\mathcal{E} : \rho \mapsto pI/2 + (1-p)\rho$, the error rates of σ_x and σ_z measurement in eavesdropping checking are $p/2$. After both qubits of an EPR pair pass the channel, the depolarizing probability is $2p - p^2$.[33] The secrecy capacities are plotted in Figure 2. The secrecy capacity of the wiretap channel method has less tolerance for error rate, but it can utilize practical classical coding, while the entanglement distillation method requires a quantum computer.

3 | SECURITY OF THE SINGLE-PHOTON QSDC PROTOCOL

Generally speaking, single-photon–based protocols are more practical than entanglement-based protocols. Therefore, we construct a generic single-photon–based QSDC protocol and prove its security through the equivalence between the two kinds of protocols.

Firstly, we need to construct an equivalent two-way entanglement-based protocol. The protocol works as follows: (1) Bob prepares the EPR pairs in state $|\psi^-\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$. (2) Bob sends each half of the pairs to Alice and does

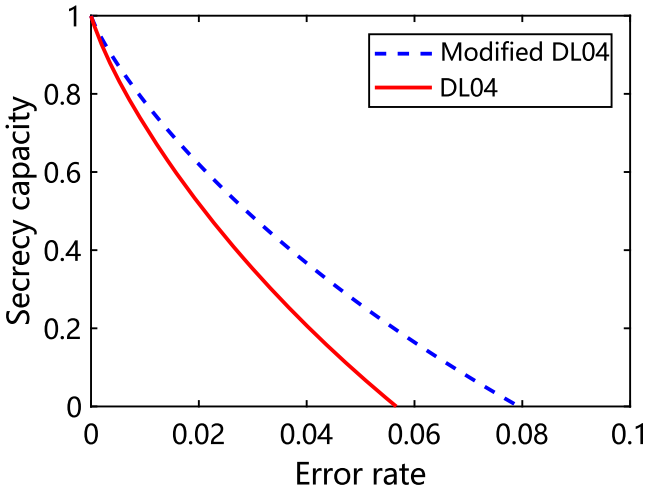

FIGURE 3 Comparison of secrecy capacity between DL04 protocol and modified DL04 protocol under lossless depolarizing channel. The secrecy capacity of modified DL04 protocol is remarkably larger when the error rate is under the threshold. The error rate threshold of DL04 is 0.057 while that of modified DL04 is 0.079

parameter estimation. (3) Alice applies encoding operation U_k on her halves and sends them to Bob. (4) Bob measures the pairs to decode. It is easy to find the equivalence between this two-way protocol and the original two-step protocol. Additionally, if Alice abandons dense coding and uses two operations, eg, I and σ_x, to encode the message, Bob simply needs to measure the two qubits separately to decode.

The generic two-way single-photon–based protocol is constructed as follows: (1) Bob prepares each qubit randomly in state $|\varphi_j^i\rangle$ and sends them to Alice, where $i \in \{0, 1\}$ and $\{|\varphi_j^0\rangle, |\varphi_j^1\rangle\}$ forms the basis of operator σ_j. (2) After Alice receives the qubits, they do parameter estimation by selecting some pairs randomly and measuring some observables such as σ_x or σ_z. (3) They sift out the qubits that cannot be effectively encoded by Alice. For example, if Alice is to apply $U_k \in \{I, \sigma_x\}$ to encode, they sift out the qubits in σ_x basis since the states remain unchanged under σ_x operation. (4) Alice applies encoding operation U_k and sends them to Bob. (5) Bob measures the qubits in the basis in which they are prepared to decode.

Next, we prove the equivalence between the two protocols above. For the generic two-way single-photon–based protocol, Eve interacts with the qubits sent by Bob and gets the state $U_{AE}|\varphi_j^i\rangle|E\rangle$. After the encoding operation of Alice, Eve intercepts all the qubits and gets the state $|\Phi_j^{i,k}\rangle_{AE} = U_k U_{AE}|\varphi_j^i\rangle|E\rangle$. For the two-way entanglement-based protocol without dense coding, the state of the whole system after the interaction of Eve and the encoding of Alice is $|\Phi^k\rangle_{ABE} = U_k U_{AE}|\psi^-\rangle|E\rangle$. Then, Bob measures his qubits in basis σ_j. If the measurement result is $\bar{i}$, we can verify $|\Phi_j^{i,k}\rangle_{AE} = \langle\varphi_j^{\bar{\xi}}|\Phi^k\rangle_{ABE}$, neglecting the normalization factor.

Based on the equivalence, the lower bound of the secrecy capacity of the typical two-way single-photon–based QSDC protocol, ie, the DL04 protocol,[4] can be obtained (see Appendix B for details)

$$C_s \geq Q_B[1 - h(e)] - Q_E h(\varepsilon_z + \varepsilon_x), \tag{10}$$

where e is the bit error rate of the binary main channel. This capacity is the same as the previous result.[26] However, a higher capacity can be reached if the eavesdropping checking part is modified. The modified DL04 protocol works as follows: (1) Bob prepares qubits $|\varphi_j^i\rangle$ randomly in basis σ_x, σ_y, or σ_z and sends them to Alice. (2) Bob tells Alice which qubit is prepared in basis σ_y, then Alice measures those qubits in basis σ_y to get an error rate ε_y. (3) Alice applies encoding operation I, σ_y on the remaining qubits and sends them to Bob. (4) Bob measures the returned qubits in the basis in which he prepares them to decode. The lower bound of the secrecy capacity of this modified DL04 protocol is

$$C_s \geq Q_B[1 - h(e)] - Q_E h(\varepsilon_y). \tag{11}$$

The performance of DL04 protocol and modified DL04 protocol under lossless depolarizing channel is shown in Figure 3.

In a general form, when they check the error rate in σ_u $(u = x, y, z)$ basis and Alice uses $\{I, \sigma_u\}$ as encoding operation, the secrecy capacity is $C_s = Q_B[1 - h(e)] - Q_E h(\varepsilon_u)$. Actually, the secrecy capacity is only constrained by the error rate of the corresponding basis of encoding operation.

4 | CONCLUSION

We have applied the wiretap channel theory on security analysis of QSDC. The security of two-step protocol against coherent attack is proven with the secrecy capacity

$$C_s \geq Q_B[2 - h_4(\mathbf{e})] - Q_E[h(\varepsilon_x) + h(\varepsilon_z)]. \tag{12}$$

Our analysis is completed under the following assumptions. (1) There exist noise and loss in the quantum channel. (2) The entanglement source and measurement device are perfect. (3) The EPR pairs transmitted in a round are infinite. Compared with the method of entanglement distillation, the error rate threshold based on the wiretap channel theory is slightly smaller. This result implies the superiority of quantum coding to some extent since one-way entanglement distillation is equivalent to quantum error correction code.[34]

Furthermore, we have established the equivalence between entanglement-based QSDC protocols and single-photon–based QSDC protocols, thus obtaining the secrecy capacity of the latter ones. Specifically, we have analyzed and modified the DL04 protocol to get a higher secrecy capacity

$$\begin{aligned} &\text{DL04: } C_s \geq Q_B[1 - h(e)] - Q_E h(\varepsilon_x + \varepsilon_z), \\ &\text{Modified DL04: } C_s \geq Q_B[1 - h(e)] - Q_E h(\varepsilon_y). \end{aligned} \tag{13}$$

An in-depth analysis indicates that the eavesdropping capability of Eve can be fully described by the error rate in the basis of the encoding operator or, in other words, the phase error rate. The reason for the high performance of modified DL04 is that it can estimate Eve's eavesdropping capability more accurately.

The application of Wyner's wiretap channel theory to the security of QSDC provides a quantitative analysis of security for transmitting information deterministically. QSDC requires a forward coding scheme, which is different from QKD where only random numbers are transmitted. Forward coding has been studied in information theory, typical example was presented in the work of Tyagi and Vardy.[30] As QSDC is the direct transmission of meaningful message rather than random strings, there exist potential wide applications in communication. The analysis presented here is a step toward the practical application of QSDC in realistic conditions.

ACKNOWLEDGEMENTS

This work was supported by China Aerospace Science and Technology Corporation; by the National Basic Research Program of China under grants 2017YFA0303700 and 2015CB921001; by the National Natural Science Foundation of China under grants 61727801, 61871257, and 11774197; and by the Key R&D Program of Guangdong Province under grant 2018B030325002. This work is supported in part by the Beijing Advanced Innovation Center for Future Chip (ICFC).

ORCID

Jiawei Wu https://orcid.org/0000-0001-7340-7846
Liuguo Yin https://orcid.org/0000-0002-4441-9490
Gui-Lu Long https://orcid.org/0000-0002-9023-1579

REFERENCES

1. Bennett CH, Brassard G. Quantum cryptography: public key distribution and coin tossing. *Theor Comput Sci*. 2014;560:7-11.
2. Long G-L, Liu XS. Theoretically efficient high-capacity quantum-key-distribution scheme. *Phys Rev A*. 2002;65(3):032302.
3. Deng F-G, Long G-L, Liu X-S. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. *Phys Rev A*. 2003;68(4):042317.
4. Deng F-G, Long G-L. Secure direct communication with a quantum one-time pad. *Phys Rev A*. 2004;69(5):052319.
5. Wang C, Deng F-G, Long G-L. Multi-step quantum secure direct communication using multi-particle Green–Horne–Zeilinger state. *Opt Commun*. 2005;253(13):15-20. http://dx.doi.org/10.1016/j.optcom.2005.04.048
6. Wang C, Deng F-G, Li Y-S, Liu X-S, Long G-L. Quantum secure direct communication with high-dimension quantum superdense coding. *Phys Rev A*. 2005;71(4):044305.

7. Lum DJ, Howell JC, Allman MS, et al. Quantum enigma machine: experimentally demonstrating quantum data locking. *Phys Rev A*. 2016;94:022315. http://dx.doi.org/10.1103/PhysRevA.94.022315
8. Massa F, Moqanaki A, Del Santo F, Dakic B, Walther P. Experimental two-way communication with one photon. Paper presented at: 2018 Conference on Lasers and Electro-Optics Pacific Rim (CLEO-PR); 2018; Hong Kong.
9. Shapiro JH, Boroson DM, Dixon PB, Grein ME, Hamilton SA. Quantum low probability of intercept. *J Opt Soc Am B*. 2019;36(3):B41-B50. http://dx.doi.org/10.1364/JOSAB.36.000B41
10. Niu P-H, Zhou Z-R, Lin Z-S, Sheng Y-B, Yin L-G, Long G-L. Measurement-device-independent quantum communication without encryption. *Science Bulletin*. 2018;63(20):1345-1350. http://dx.doi.org/10.1016/j.scib.2018.09.009
11. Zhou ZR, Sheng YB, Niu PH, Yin LG, Long GL, Hanzo L. Measurement-device-independent quantum secure direct communication. *Sci China-Phys Mech Astron*. 2020;63. No. 230362. https://doi.org/10.1007/s11433-019-1450-8
12. Gao Z, Li T, Li Z. Long-distance measurement-device-independent quantum secure direct communication. *Europhysics Letters*. 2019;125(4):40004. http://dx.doi.org/10.1209/0295-5075/125/40004
13. Zhou L, Sheng Y-B, Long G-L. Device-independent quantum secure direct communication. *Science Bulletin*. 2019. https://doi.org/10.1016/j.scib.2019.10.025
14. Hu J-Y, Yu B, Jing M-Y, et al. Experimental quantum secure direct communication with single photons. *Light Sci Appl*. 2016;5(9):e16144. http://dx.doi.org/10.1038/lsa.2016.144
15. Zhu F, Zhang W, Sheng Y, Huang Y. Experimental long-distance quantum secure direct communication. *Science Bulletin*. 2017;62(22):1519-1524. http://dx.doi.org/10.1016/j.scib.2017.10.023
16. Zhang W, Ding D-S, Sheng Y-B, Zhou L, Shi B-S, Guo G-C. Quantum Secure Direct Communication with Quantum Memory. *Phys Rev Lett*. 2017;118:220501. http://dx.doi.org/10.1103/PhysRevLett.118.220501
17. Sun Z, Qi R, Lin Z, Yin L, Long G, Lu J. Design and implementation of a practical quantum secure direct communication system. Paper presented at: 2018 IEEE Globecom Workshops (GC Wkshps); 2018; Abu Dhabi, UAE.
18. Lo H-K, Chau HF. Unconditional security of quantum key distribution over arbitrarily long distances. *Science*. 2050;283(5410):1999.
19. Shor PW, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys Rev Lett*. 2000;85(2):441-444.
20. Mayers D. Unconditional security in quantum cryptography. *J ACM*. 2001;48(3):351-406. http://dx.doi.org/10.1145/382780.382781
21. Renner R, Gisin N, Kraus B. Information-theoretic security proof for quantum-key-distribution protocols. *Phys Rev A*. 2005;72(1):012332.
22. Kraus B, Gisin N, Renner R. Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication. *Phys Rev Lett*. 2005;95(8):080501.
23. Scarani V, Bechmann-Pasquinucci H, Cerf NJ, Lütkenhaus N, Peev M. The security of practical quantum key distribution. *Rev Md Phys*. 2009;81(3):1301-1350.
24. Lu H, Fung C-HF, Ma X, Cai Q. Unconditional security proof of a deterministic quantum key distribution with a two-way quantum channel. *Phys Rev A*. 2011;84(4).
25. Hu J, Jing M, Zhang P, et al. Security proof of the two-way quantum secure direct communication with channel loss and noise. arXiv e-prints: arXiv:1706.03234; 2017.
26. Qi R, Sun Z, Lin Z, et al. Implementation and security analysis of practical quantum secure direct communication. *Light Sci Appl*. 2019;8(1):22.
27. Wyner AD. The wire-tap channel. *Bell Syst Tech J*. 1975;54(8):1355-1387. http://dx.doi.org/10.1002/j.1538-7305.1975.tb02040.x
28. Bennett CH, Brassard G, Crépeau C, Maurer UM. Generalized privacy amplification. *IEEE Trans Inf Theory*. 1995;41(6):1915-1923.
29. Thangaraj A, Dihidar S, Calderbank AR, McLaughlin SW, Merolla J-M. Applications of LDPC codes to the wiretap channel. *IEEE Trans Inf Theory*. 2007;53(8):2933-2945. http://dx.doi.org/10.1109/TIT.2007.901143
30. Tyagi H, Vardy A. Universal hashing for information-theoretic security. *Proc IEEE*. 2015;103(10):1781-1795. http://dx.doi.org/10.1109/JPROC.2015.2462774
31. Renner R. Symmetry of large physical systems implies independence of subsystems. *Nature Physics*. 2007;3(9):645-649.
32. Holevo AS. Bounds for the quantity of information transmitted by a quantum communication channel. *Probl Peredachi Inf*. 1973;9(3):3-11.
33. Beaudry NJ, Lucamarini M, Mancini S, Renner R. Security of two-way quantum key distribution. *Phys Rev A*. 2013;88(6):062302.
34. Bennett CH, DiVincenzo DP, Smolin JA, Wootters WK. Mixed-state entanglement and quantum error correction. *Phys Rev A*. 1996;54(5):3824-3851.
35. Jozsa R, Schlienz J. Distinguishability of states and von Neumann entropy. *Phys Rev A*. 2000;62. https://doi.org/012301. http://dx.doi.org/10.1103/PhysRevA.62.012301

How to cite this article: Wu J, Lin Z, Yin L, Long G-L. Security of quantum secure direct communication based on Wyner's wiretap channel theory. *Quantum Engineering*. 2019;e26. https://doi.org/10.1002/que2.26

APPENDIX A

THE DETAILED CALCULATION OF SECRECY CAPACITY OF TWO-STEP PROTOCOL

Firstly, we calculate the upper bound of mutual information $I(A:E)$. Remind that, in Equation (7), we have the average mutual information on one subsystem between Alice and Eve

$$I(A:E) \leq S\left(\sum_a p_a \rho_{AE,a}\right) - 1. \tag{A1}$$

Since p_a is the distribution of each word, we can reasonably assume $p_a = 1/4$ for all a. Then, the Gram matrix method is used to calculate the entropy of $\sum_a p_a \rho_{AE,a}$ (refer to the work of Jozsa and Schlienz[35] for Gram matrix method). The Gram matrix of $\sum_a p_a \rho_{AE,a}$ is symmetric

$$\mathbf{G} = \frac{1}{8}\begin{bmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{B}^{\mathsf{T}} & \mathbf{A} \end{bmatrix},$$

where

$$\mathbf{A} = \begin{bmatrix} 1 & \lambda_1+\lambda_2-\lambda_3-\lambda_4 & 0 & 0 \\ & 1 & 0 & 0 \\ \vdots & & 1 & \lambda_1+\lambda_2-\lambda_3-\lambda_4 \\ & \cdots & & 1 \end{bmatrix},$$

$$\mathbf{B} = \begin{bmatrix} 0 & 0 & -\lambda_1+\lambda_2-\lambda_3+\lambda_4 & \lambda_1-\lambda_2-\lambda_3+\lambda_4 \\ 0 & 0 & -\lambda_1+\lambda_2+\lambda_3-\lambda_4 & \lambda_1-\lambda_2+\lambda_3-\lambda_4 \\ -\lambda_1+\lambda_2-\lambda_3+\lambda_4 & \lambda_1-\lambda_2-\lambda_3+\lambda_4 & 0 & 0 \\ -\lambda_1+\lambda_2+\lambda_3-\lambda_4 & \lambda_1-\lambda_2+\lambda_3-\lambda_4 & 0 & 0 \end{bmatrix}.$$

If we define

$$\begin{aligned} A &= \lambda_1+\lambda_2-\lambda_3-\lambda_4, \\ B &= \lambda_1-\lambda_2+\lambda_3-\lambda_4, \\ C &= \lambda_1-\lambda_2-\lambda_3+\lambda_4, \end{aligned}$$

the eigenvalues of Gram matrix $\mathbf{G}$ are

$$\frac{1}{8}\times\begin{pmatrix} 1+A+B+C \\ 1+A+B+C \\ 1+A-B-C \\ 1+A-B-C \\ 1-A+B-C \\ 1-A+B-C \\ 1-A-B+C \\ 1-A-B+C \end{pmatrix}.$$

Then, we have

$$\begin{aligned} S\left(\sum_a p_a \rho_{AE,a}\right) &= S(\mathbf{G}) \\ &\leq 1 + h\left(\frac{1}{2}(1+A)\right) + h\left(\frac{1}{2}(1+B)\right) \\ &= 1 + h(\varepsilon_z) + h(\varepsilon_x), \end{aligned}$$

noting that $\varepsilon_z = \lambda_3+\lambda_4, \varepsilon_x = \lambda_2+\lambda_4$. This entropy reaches its maximum when $C = AB$.

Similarly, we get the entropy of $\rho_{AE,a}$, ie, $S(\rho_{AE,a}) = 1$ for all a. The upper bound on the mutual information between Alice and Eve is

$$\begin{aligned} I(A:E) &\leq S\left(\sum_a p_a \rho_{AE,a}\right) - \sum_a p_a S\left(\rho_{AE,a}\right) \\ &\leq h(\varepsilon_z) + h(\varepsilon_x). \end{aligned} \tag{A2}$$

The capacity of wiretap channel satisfies

$$C_W \leq h(\varepsilon_z) + h(\varepsilon_x).$$

If we assume the main channel is a quaternary symmetric channel, the capacity of the main channel is

$$C_M = 2 - h_4(\mathbf{e}), \tag{A3}$$

where $\mathbf{e}$ is the error rate distribution of the main channel. The lower bound of the secrecy capacity of two-step protocol is

$$C_s \geq 2 - h_4(\mathbf{e}) - h(\varepsilon_x) - h(\varepsilon_z).$$

Considering the channel loss, it becomes

$$C_s \geq Q_B[2 - h_4(\mathbf{e})] - Q_E[h(\varepsilon_x) + h(\varepsilon_z)]. \tag{A4}$$

APPENDIX B

THE DETAILED CALCULATION OF THE SECRECY CAPACITY OF DL04 PROTOCOL AND MODIFIED DL04 PROTOCOL

In the entanglement version of modified DL04 protocol, there are two encoded states

$$\rho_{AE} = \frac{1}{2}(P_{|\psi_1\rangle} + P_{|\phi_1\rangle}),$$
$$\sigma_y \rho_{AE} \sigma_y = \frac{1}{2}(P_{\sigma_x\sigma_z|\psi_1\rangle} + P_{\sigma_x\sigma_z|\phi_1\rangle}).$$

Similarly, the Gram matrix method is used to calculate the entropy of $\sum_a p_a \rho_{AE,a}$, where $p_a = 1/2$ for all a. The Gram matrix is

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & \lambda_1 - \lambda_2 - \lambda_3 + \lambda_4 \\ 0 & 1 & -\lambda_1 + \lambda_2 + \lambda_3 - \lambda_4 & 0 \\ 0 & -\lambda_1 + \lambda_2 + \lambda_3 - \lambda_4 & 1 & 0 \\ \lambda_1 - \lambda_2 - \lambda_3 + \lambda_4 & 0 & 0 & 1 \end{bmatrix}.$$

Noticing that $\lambda_1 - \lambda_2 - \lambda_3 + \lambda_4 = 1 - 2\varepsilon_y$, the eigenvalues of the Gram matrix are

$$\frac{1}{4} \times \begin{pmatrix} 1 + (1 - 2\varepsilon_y) \\ 1 + (1 - 2\varepsilon_y) \\ 1 - (1 - 2\varepsilon_y) \\ 1 - (1 - 2\varepsilon_y) \end{pmatrix}.$$

It is easy to get the entropy $S(\sum_a p_a \rho_{AE,a}) = 1 + h(\varepsilon_y)$. Then, we have the mutual information

$$\begin{aligned} I(A:E) &\leq S\left(\sum_a p_a \rho_{AE,a}\right) - \sum_a p_a S\left(\rho_{AE,a}\right) \\ &\leq h(\varepsilon_y), \end{aligned}$$

and secrecy capacity of modified DL04 protocol

$$C_s \geq Q_B[1 - h(e)] - Q_E h(\varepsilon_y), \tag{B1}$$

where $1 - h(e)$ is the main channel capacity.

For DL04 protocol, the only difference is that the parameters acquired in the eavesdropping checking process are ε_x and ε_z instead of ε_y. Hence, we need to estimate the upper bound of ε_y through ε_x and ε_z. According to the constraint

$$\begin{aligned} \varepsilon_x &= \lambda_2 + \lambda_4, \\ \varepsilon_z &= \lambda_3 + \lambda_4, \\ \varepsilon_y &= \lambda_2 + \lambda_3, \\ \lambda_i &\geq 0, \forall i, \end{aligned} \tag{B2}$$

the worst situation is $\lambda_4 = 0$, then we have $\max \varepsilon_y = \varepsilon_x + \varepsilon_z$. The secrecy capacity of DL04 protocol is obtained by substituting this result into Equation (B1)

$$C_s \geq Q_B[1 - h(e)] - Q_E h(\varepsilon_x + \varepsilon_z). \tag{B3}$$