Fault tolerant quantum secure direct communication with quantum encryption against collective noise*

Huang Wei(黄 伟)[a)b)†], Wen Qiao-Yan(温巧燕)[a)], Jia Heng-Yue(贾恒越)[a)], Qin Su-Juan(秦素娟)[a)], and Gao Fei(高 飞)[a)]

[a)] *State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*

[b)] *State Key Laboratory of Integrated Services Network, Xidian University, Xi'an* 710071, *China*

(Received 9 March 2012; revised manuscript received 13 April 2012)

We present two novel quantum secure direct communication (QSDC) protocols over different collective-noise channels. Different from the previous QSDC schemes over collective-noise channels, which are all source-encrypting protocols, our two protocols are based on channel-encryption. In both schemes, two authorized users first share a sequence of EPR pairs as their reusable quantum key. Then they use their quantum key to encrypt and decrypt the secret message carried by the decoherence-free states over the collective-noise channel. In theory, the intrinsic efficiencies of both protocols are high since there is no need to consume any entangled states including both the quantum key and the information carriers except the ones used for eavesdropping checks. For checking eavesdropping, the two parties only need to perform two-particle measurements on the decoy states during each round. Finally, we make a security analysis of our two protocols and demonstrate that they are secure.

Keywords: quantum cryptography, quantum secure direct communication, quantum encryption, collective noise

PACS: 03.67.Dd, 03.67.Hk, 03.67.Pp **DOI:** 10.1088/1674-1056/21/10/100308

1. Introduction

Over the last two decades, quantum mechanics has provided some novel ways for processing and transmitting quantum information. Quantum key distribution (QKD) is a remarkable branch of quantum information, in which two remote legitimate users, say Alice and Bob, can establish a shared private random key and thereafter they can use this key to encrypt messages. Since the pioneering work of Bennett and Brassard,[1] much attention has been focused on QKD.[1−20] The QKD protocols proposed in Refs. [1]–[14] are categorized as source-encrypting QKD in Ref. [17], for their ideas are realized by splitting the source into two parts. Specifically, the source is divided into one quantum part and one classical part in Refs. [1]–[10], and two quantum parts in Refs. [11]–[14]. Different from the source-encrypting QKD, the protocols presented in Refs. [17]–[20] are categorized as channel-encrypting (quantum-encrypting) QKD schemes, in which two authorized users first share a sequence of EPR pairs as their reusable quantum key. Then they use their quantum key to encrypt and decrypt the classical bits carried by the travelling states. After that a classical key stream can be established.

In recent years, a novel concept in quantum cryptography, quantum secure direct communication (QSDC), was put forward.[21] Different from QKD, whose task is to generate a private key, the purpose of QSDC is to transmit a secret message directly. Due to its instantaneous nature, QSDC is important in some applications, which has been shown by Deng *et al.*[15,21,22] and Boström *et al.*[23] According to the Deng–Long–Liu criterion,[21,22,24,25] on the one hand, the sender Alice should confirm whether the quantum channel is secure or not before she encodes the mes-

*Project supported by the National Natural Science Foundation of China (Grant Nos. 61170270, 61100203, 60903152, 61003286, and 61121061), the Program for New Century Excellent Talents in University (Grant No. NCET-10-0260), the Specialized Research Fund for the Doctoral Program of Higher Education (Grant No. 20090005110010), the Natural Science Foundation of Beijing (Grant Nos. 4112040 and 4122054), the Foundation of Science and Technology on Communication Security Laboratory (Grant No. 9140C110101110 C1104), and the Fundamental Research Funds for the Central Universities (Grant Nos. BUPT2011YB01, BUPT2011RC0505, 2011PTB-00-29, and 2011RCZJ15).

†Corresponding author. E-mail: E-mail: huangwei096505@yahoo.cn

© 2012 Chinese Physical Society and IOP Publishing Ltd

sage on the quantum information carriers transmitted as the messages cannot be discarded in QSDC.[15,21,22] On the other hand, the security of quantum cryptographic protocols is based on the error rate analysis with the theories in statistics.[15,21,22] Therefore the quantum states in QSDC schemes should be transmitted in a quantum data block.[21] While this is not a necessary condition in QKD since the error rate analysis is just a postprocessing step, and the states transmitted can be abandoned as they do not carry information about the secret message.[15,21,22,25] QSDC has been actively studied by several groups.[21−48] For example, in 2002, Long and Liu presented the first QSDC protocol with Einstein–Podolsky–Rosen (EPR) photon pairs and introduced the concept of a quantum data block into QSDC for checking eavesdropping perfectly.[21] Then Boström and Felbinger proposed the QSDC protocol, later referred to as the ping–pong protocol.[23] However, it has been revealed to be insecure in a noisy channel.[26] In 2003, Deng *et al.*[15] put forward a two-step QSDC protocol using a block of EPR pairs. Later, in 2004, Deng and Long[22] proposed another QSDC protocol using only a sequence of single photons. In 2005, Wang *et al.*[29] proposed a multi-step QSDC protocol using blocks of multi-particle maximally entangled states as a quantum channel and introduced a high-dimensional QSDC protocol[30] with quantum superdense coding. In the period from 2008 to 2010, a few groups[44−46,49] proposed some QSDC protocols over noisy channels. Very recently, Gu *et al.* proposed a robust quantum one-time-pad scheme[38] over a collective noise and a two-step QSDC protocol[37] with hyperentanglement.

Although there are many schemes for QSDC,[21−48] they are all source-encrypting protocols. Till now, there has been only one channel-encrypting QSDC protocol, which was proposed by Li[50] in 2007. However, this protocol was designed in ideal conditions. In experiment, the uncontrollable interaction between transmitted qubits and the environment decreases the fidelity of the transmitted qubits. At present, it is always supposed that the noise in a quantum channel is a collective one.[51] That is, the noise fluctuation is slow in time. If several photons transmit through the noisy channel simultaneously or they are close to each other, the changes caused by noise on each qubit is identical. For overcoming this kind of noise, some good methods have been proposed for quantum communication, such as entanglement purification,[52] single-photon error rejection,[53] decoherence-free subspace (DFS),[54] and so on. "Entanglement purification is a method to distill maximally entangled states from some less-entanglement states by sacrificing several samples affected by the noise. The influence of noise can only be reduced in entanglement purification, and infinite steps are needed to get a perfect maximally entangled state."[55] Single-photon error rejection protocols require less quantum resources, but it can succeed probabilistically. DFS is a subspace of a system's Hilbert space, which does not experience decoherence and the state in DFS (decoherence-free state) is composed of several qubits. As the qubits of a decoherence-free state suffering from the same noise in a quantum channel will compensate the effect of noise, the decoherence-free state can keep the invariability under the noise. This good feature can be used in quantum communication over a collective-noise channel.[9,55−57]

In this paper, we present two robust channel-encrypting QSDC protocols against collective noise with decoy states, which can withstand the attack[58,59] on many other channel-encrypting protocols.[17−19] Different from previous QSDC schemes over collective-noise channels, which are all source-encrypting protocols, our two protocols are based on channel-encryption. In both QSDC schemes, two authorized users first share a sequence of EPR pairs $|\Phi^+\rangle$ as their reusable quantum key. Then they use their quantum key to encrypt and decrypt the secret message carried by the decoherence-free states. In theory, the intrinsic efficiencies of both the protocols are high since there is no need to consume any entangled states including both the quantum key and the information carriers except the ones used for eavesdropping checking. To check for eavesdropping, the two parties need only perform two-particle measurements on the decoy states during each round. Finally, we make a security analysis of our two protocols and show that they are secure in principle.

The rest of this paper is arranged as follows. In Section 2, the two robust fault-tolerant channel-encrypting quantum secure direct communication protocols are presented in detail, especially the distribution processes of the quantum key over the two kinds of collective-noise channels. In Section 3, we analyze the security of our two protocols and show that they are secure, and finally a conclusion is made in Section 4.

2. The fault tolerant channel-encryption quantum secure direct communication protocols against collective noise

In both of our two channel-encrypting quantum secure direct communication protocols, two authorized users should first share a sequence of EPR pairs $|\phi^+\rangle$ which will act as the quantum key to encode and decode the secret message carried by the decohenrence-free states. In this section, the two robust fault-tolerant channel-encrypting quantum secure direct communication protocols are presented in detail respectively, especially the distribution processes of the quantum key over the two collective-noise channels. Here,

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \tag{1}$$

2.1. Fault tolerant channel-encryption quantum secure direct communication protocol against collective-dephasing noise

A collective-dephasing noise can be described as

$$U_{\rm dp}|0\rangle = |0\rangle, \quad U_{\rm dp}|1\rangle = {\rm e}^{{\rm i}\phi}|1\rangle, \tag{2}$$

where ϕ is the noise parameter and it fluctuates with time. $|0\rangle$ and $|1\rangle$ represent the horizontal and vertical polarizations of photons, respectively. In general, a logical qubit encoded into two antiparallel qubits can be secure against this kind of noise as these two logical qubits acquire the same phase factor ${\rm i}\phi$

$$|0\rangle_L \equiv |0\rangle|1\rangle, \quad |1\rangle_L \equiv |1\rangle|0\rangle. \tag{3}$$

To communicate securely, at least two nonorthogonal measuring bases (MBs) are required. Another MB is chosen as

$$\begin{aligned} |+\rangle_L &= \frac{1}{\sqrt{2}}(|0\rangle_L + |1\rangle_L), \\ |-\rangle_L &= \frac{1}{\sqrt{2}}(|0\rangle_L - |1\rangle_L). \end{aligned} \tag{4}$$

It is straightforward to verify that $|\langle +|0\rangle_L|^2 = |\langle +|1\rangle_L|^2 = |\langle -|0\rangle_L|^2 = |\langle -|1\rangle_L|^2$, which means $\{|0\rangle_L, |1\rangle_L\}$ and $\{|+\rangle_L, |-\rangle_L\}$ form two nonorthogonal unbiased bases. Before we describe the principle of our robust channel-encrypting QSDC against collective-dephasing noise, we first introduce the distribution process of the quantum key over the collective-dephasing noise channel.

2.1.1. Distribution process of the quantum key over the collective-dephasing noise channel

Inspired by the ideas in Ref. [55], we find an interesting method for sharing the EPR pairs $|\Phi^+\rangle$ between two authorized users over a collective-dephasing noise channel. In this method, Alice prepares a sequence of entangled states $|\Phi^+_{\rm dp}\rangle_{AB} = (1/\sqrt{2})(|0\rangle|1\rangle_L + |1\rangle|0\rangle_L)_{AB} = (1/\sqrt{2})(|0\rangle_A|01\rangle_{B_1B_2} + |1\rangle_A|10\rangle_{B_1B_2})$ and share them securely with Bob, same as the first three steps in Ref. [55]. That is, Alice divides the quantum entangled states into two photon sequences, S_A and S_B. S_A is composed of all the qubits A in these states and S_B is made up of the logical qubits B, each of which is composed of two physical qubits B_1 and B_2. Then Alice sends the logical qubit sequence S_B to Bob and preserves the sequence S_A. After receiving the sequence S_B, Bob randomly chooses a subset of logical qubits as the samples for security analysis and the rest of the logical qubits can make up the private quantum key shared between Alice and Bob. Bob measures each qubit in the samples by randomly choosing one of the two bases $\sigma_z^B = \sigma_z^{B_1} \otimes \sigma_z^{B_2}$ and $\sigma_x^B = \sigma_x^{B_1} \otimes \sigma_x^{B_2}$. After that he tells Alice which logical qubits are chosen as samples. Here, $\sigma_x^{B_1}$ means measuring the particle B_1 with the basis $\sigma_x = \{|+\rangle, |-\rangle\}$. After that, Alice measures each logical qubit in S_A of the samples by randomly choosing one of the two bases σ_z^A and σ_x^A. Under these two bases, the original entangled state can be written as

$$\begin{aligned} |\Phi^+_{\rm dp}\rangle_{AB} &= \frac{1}{\sqrt{2}}(|0\rangle_A|01\rangle_{B_1B_2} + |1\rangle_A|10\rangle_{B_1B_2}) \\ &= \frac{1}{2}[|+\rangle_A(|++\rangle - |--\rangle)_{B_1B_2} \\ &\quad + |-\rangle_A(|-+\rangle - |+-\rangle)_{B_1B_2}]. \end{aligned} \tag{5}$$

Here

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{6}$$

That is, the measurement outcomes obtained by Alice and Bob are correlated if they choose the same bases to measure their logical qubits. However, whatever a vicious action done by Eve will destroy this correlation and be detected, same as those in Refs. [3] and [55]. So Alice and Bob can exploit the correlation to guarantee the security of the transmission of the logical qubits between Alice and Bob. After they make sure that the transmission is secure, they have successfully

shared a sequence of entangle states $|\Phi_{\rm dp}^{+}\rangle_{AB}$. For each of the remaining states $|\Phi_{\rm dp}^{+}\rangle_{AB}$, Bob performs a controlled-NOT operation on particles B_1 and B_2 ($\rm CNOT_{B_1B_2}$, particle B_1 is the controller and B_2 is the target). Then the state of the quantum system will be converted from $|\Phi_{\rm dp}^{+}\rangle_{AB}$ into

$$\begin{aligned}|\Theta_{\rm dp}\rangle_{AB} &= \frac{1}{\sqrt{2}}(|0\rangle_A|01\rangle_{B_1B_2}+|1\rangle_A|11\rangle_{B_1B_2})\\ &= \frac{1}{2}(|0\rangle_A|0\rangle_{B_1}+|1\rangle_A|1\rangle_{B_1})|1\rangle_{B_2}. \qquad (7)\end{aligned}$$

So far, Alice and Bob have successfully shared a sequence of Bell sates $|\Phi^{+}\rangle_{AB_1}=(1/\sqrt{2})(|0\rangle_A|0\rangle_{B_1}+|1\rangle_A|1\rangle_{B_1})$ securely, which will be used as their private quantum key in the following QSDC protocol.

2.1.2. The principle of the robust channel-encrypting QSDC against collective-dephasing noise

The principle of our robust channel-encryption QSDC protocol against collective-dephasing noise can be described as follows.

(i) The two authorized users (Alice and Bob) first share a sequence of N EPR pairs $|\Phi^{+}\rangle_{AB}=(1/\sqrt{2})(|0|0\rangle+|1|1\rangle)_{AB}$ securely as their private quantum key by the method described in Subsubsection 2.1.1.

(ii) Alice prepares a sequence of N traveling states $|\gamma_i\rangle$ $(i=1,2,\ldots,N)$ which are in one of the two states $\{|0\rangle_L,|1\rangle_L\}$ according to her secret meassage. Here, the travelling states sequence is denoted as $S_{\rm T}$. For checking eavesdropping, similar to Refs. [22] and [50], Alice utilizes a small trick in the sequence $S_{\rm T}$ before she sends it to Bob. That is, she inserts some decoy states,[60] which are randomly in the four states $\{|0\rangle_L,|1\rangle_L,|+\rangle_L,|-\rangle_L\}$ and inserted randomly in the sequence $S_{\rm T}$. Alice uses the quantum key, the Bell states $|\Phi^{+}\rangle_{AB}$ shared with Bob to encrypt the travelling states in the sequence $S_{\rm T}$ except for the decoy states. That is, Alice performs a controlled-U_1 operation (CU_1) on the particles A_i and $|\gamma_i\rangle$ $(i=1,2,\ldots,N)$ by using the particle A_i as the control qubit and $|\gamma_i\rangle$ as target qubit. After that, Alice sends all the travelling states to Bob. Here

$$\begin{aligned}&CU_1=|0\rangle\langle 0|\otimes I+|1\rangle\langle 1|\otimes U_1,\\ &U_1=U_{y1}\otimes U_{x2},\quad I=I_1\otimes I_2,\\ &U_x=|1\rangle\langle 0|+|0\rangle\langle 1|,\quad U_y=|1\rangle\langle 0|-|0\rangle\langle 1|. \qquad (8)\end{aligned}$$

The subscripts 1 and 2 in the unitary operations I and U represent the first and the second physical qubits in each logical state, respectively. The effect of the unitary operation U_1 on each logical state can be written as

$$\begin{aligned}&U_1|0\rangle_L=|1\rangle_L,\quad U_1|1\rangle_L=-|0\rangle_L,\\ &U_1|+\rangle_L=-|-\rangle_L,\quad U_1|-\rangle_L=|+\rangle_L. \qquad (9)\end{aligned}$$

(iii) After receiving all the states that Alice has sent to him, Bob asks Alice to tell him the positions and the states of the decoy states in sequence $S_{\rm T}$, and then measures them with their initial bases. Then Bob performs a CU_1 operation on particle B_i and $|\gamma_i\rangle$ $(i=1,2,\ldots,N)$ by using the particle B_i as the control qubit and $|\gamma_i\rangle$ as target qubit to decrypt the encrypted states in the sequence $S_{\rm T}$, similar to Alice. After that, he measures the states $|\gamma_i\rangle$ with the basis $\sigma_z\otimes\sigma_z$ and records the outcomes of the measurements.

(iv) With all the measurement outcomes, Alice and Bob check the security of their transmission. They analyze the error rate of the decoy states. If the error rate is unacceptable, they abort the results and repeat the procedures from the beginning. If the error rate is very low, Bob can trust this transmission and read out the message directly.

(v) If the protocol succeeds, for each of their shared EPR pairs $|\Phi^{+}\rangle_{AB}$, the two parties (Alice and Bob) rotate their respective particle by angle θ, respectively. The rotation can be described as

$$R(\theta)=\begin{pmatrix}\cos\theta & \sin\theta\\ -\sin\theta & \cos\theta\end{pmatrix}. \qquad (10)$$

The state $|\Phi^{+}\rangle_{AB}$ does not change under bilateral operation of $R(\theta)$. The purpose of this operation is to prevent the other parties from eavesdropping (The interpretation and the selection of θ will be given later in the security analysis section). After the rotation for all the EPR pairs, Alice and Bob can repeat their procedures from step (ii). That is, they use repeatedly the EPR $|\Phi^{+}\rangle_{AB}$ pairs as their private quantum key to transmit the secret message again in the next round.

2.2. Fault tolerant channel-encryption quantum secure communication protocol against collective-rotation noise

A collective-rotation noise can be described as

$$\begin{aligned}&U_r|0\rangle=\cos\theta|0\rangle+\sin\theta|1\rangle,\\ &U_r|1\rangle=-\sin\theta|0\rangle+\cos\theta|1\rangle. \qquad (11)\end{aligned}$$

The parameter θ depends on the noise and fluctuates with time. The two Bell states $|\Phi^+\rangle = (1/\sqrt{2})(|00\rangle + |11\rangle)$ and $|\Psi^-\rangle = (1/\sqrt{2})(|01\rangle - |10\rangle)$ are invariant under this collective-rotation noise. Hence, logical qubits under this noise can be chosen as

$$|0_r\rangle_L = |\Phi^+\rangle, \quad |1_r\rangle_L = |\Psi^-\rangle. \tag{12}$$

To communicate securely, at least two nonorthogonal measuring bases (MBs) are required. One of the bases is in Eq. (9), the other is

$$\begin{aligned} |+_r\rangle_L &= \frac{1}{\sqrt{2}}(|0\rangle_L + |1\rangle_L), \\ |-_r\rangle_L &= \frac{1}{\sqrt{2}}(|0\rangle_L - |1\rangle_L). \end{aligned} \tag{13}$$

It can be easily proved that $|\langle_r+|0_r\rangle_L|^2 = |\langle_r+|1_r\rangle_L|^2 = |\langle-_r|0_r\rangle_L|^2 = |\langle_r-|1_r\rangle_L|^2 = 1/2$, which means $\{|0_r\rangle_L, |1_r\rangle_L\}$ and $\{|+_r\rangle_L, |-_r\rangle_L\}$ form two nonorthogonal unbiased bases. Before we describe the principle of our robust channel-encrypting QSDC against collective-rotation noise, we first introduce the distribution process of the quantum key over collective-rotation noise channel.

2.2.1. Distribution process of the quantum key over collective-ratation noise channel

Inspired by the ideas in Ref. [55], we find an interesting method for sharing the EPR pairs $|\Phi^+\rangle$ between two authorized users over collective-rotation noise channel. In this method, Alice prepares a sequence of entangled states $|\Phi_r^+\rangle_{AB} = (1/2)(|0\rangle|0_r\rangle_L + |1\rangle|1_r\rangle_L)_{AB} = (1/2)(|0\rangle_A(|00\rangle+|11\rangle)_{B_1B_2}+|1\rangle_A(|01\rangle-|10\rangle)_{B_1B_2})$ and share them securely with Bob, same as the first three steps in Ref. [55]. That is, Alice divides the quantum entangled states into two photon sequences, S_A and S_B. S_A is composed of all the qubits A in these states and S_B is made up of the logical qubits B, which is composed of two physical qubits B_1 and B_2. Then Alice sends the logical qubit sequence S_B to Bob and keeps the sequence S_A. After receiving the sequence S_B, Bob randomly chooses a subset of logical qubits as the samples for security analysis and the rest of the logical qubits can be used to establish the private quantum key shared between Alice and Bob. Bob measures each qubit in the samples by randomly choosing one of the two bases $\sigma_z^B = \sigma_z^{B_1} \otimes \sigma_z^{B_2}$ and $\sigma_y^B = \sigma_y^{B_1} \otimes \sigma_y^{B_2}$. After that he tells Alice which logical qubits are chosen as samples. Here, $\sigma_z^{B_1}$ means measuring the particle B_1 with the basis $\sigma_z = \{|0\rangle, |1\rangle\}$. After that Alice measures each logical qubit in S_A of the samples by randomly choosing one of the two bases σ_z^A and σ_y^A. Under these two bases, the original entangled state can be written as

$$\begin{aligned} |\Phi_r^+\rangle_{AB} &= \frac{1}{2}(|0\rangle_A(|00\rangle + |11\rangle)_{B_1B_2} \\ &\quad + |1\rangle_A(|01\rangle - |10\rangle)_{B_1B_2}) \\ &= \frac{1}{\sqrt{2}}(|+y\rangle_A|+y\rangle_{B_1}|-y\rangle_{B_2} \\ &\quad + |-y\rangle_A|-y\rangle_{B_1}|+y\rangle_{B_2}). \end{aligned} \tag{14}$$

Here

$$\begin{aligned} |+y\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + \mathrm{i}|1\rangle), \\ |-y\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - \mathrm{i}|1\rangle). \end{aligned} \tag{15}$$

That is, the measurement outcomes obtained by Alice and Bob are correlated if they choose the same bases for their logical qubits. However, whatever a vicious action done by Eve will destroy this correlation and be detected, same as those in Refs. [3] and [55]. So Alice and Bob can exploit the correlation to guarantee the security of the transmission of the logical qubits between Alice and Bob. After they make sure that the transmission is secure, they successfully share a sequence of entangled states $|\Phi_r^+\rangle_{AB}$. Then Alice and Bob perform operations $S \otimes S \otimes S$ and $H \otimes H \otimes H$ on each of their entangled state $|\Phi_r^+\rangle_{AB}$. Here S is phase gate and H is Hadamard gate

$$S = \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{i} \end{pmatrix}, \quad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{16}$$

After these operations, the state of the quantum system will be converted from $|\Phi_r^+\rangle_{AB}$ into

$$|\Xi_r\rangle_{AB} = \frac{1}{\sqrt{2}}(|1\rangle_A|1\rangle_{B_1}|0\rangle_{B_2} + |0\rangle_A|0\rangle_{B_1}|1\rangle_{B_2}). \tag{17}$$

For each of the remaining state $|\Xi_r\rangle_{AB}$, Bob performs a controlled-NOT operation on particles B_1 and B_2 ($\mathrm{CNOT}_{B_1B_2}$, particle B_1 is the controller and B_2 is the target). Now the state is in the form

$$\begin{aligned} |\Pi_r\rangle_{AB} &= \frac{1}{\sqrt{2}}(|1\rangle_A|1\rangle_{B_1}|1\rangle_{B_2} + |0\rangle_A|0\rangle_{B_1}|1\rangle_{B_2}) \\ &= \frac{1}{\sqrt{2}}(|1\rangle_A|1\rangle_{B_1} + |0\rangle_A|0\rangle_{B_1})|1\rangle_{B_2}. \end{aligned} \tag{18}$$

So far, Alice and Bob have successfully shared a sequence of Bell sates $|\Phi^+\rangle_{AB_1} = (1/\sqrt{2})(|0\rangle_A|0\rangle_{B_1} + |1\rangle_A|1\rangle_{B_1})$ securely, which will be used as their private quantum key in the following QKD protocol.

2.2.2. The principle of the robust channel-encrypting QSDC against collective-rotation noise

The principle of our robust channel-encryption QSDC protocol against collective-rotation noise can be described as follows.

(I) The two authorized users (Alice and Bob) share a sequence of N EPR pairs $|\Phi^+\rangle_{AB} = (1/\sqrt{2})(|0\rangle|0\rangle + |1\rangle|1\rangle)_{AB}$ securely as their private quantum key by the method described in Subsubsection 2.2.1.

(II) Alice prepares a sequence of N traveling states $|\gamma_i\rangle$ $(i = 1, 2, \ldots, N)$ which are in one of the two states $\{|0_r\rangle_L, |1_r\rangle_L\}$ according to her secret message. Here, the travelling states sequence is denoted as $S_{\rm T}$. For checking eavesdropping, similar to Refs. [22] and [50], Alice utilizes a small trick in the sequence $S_{\rm T}$ before she sends it to Bob. That is, she inserts some decoy states,[60] which are randomly in the four states $\{|0_r\rangle_L, |1_r\rangle_L, |+_r\rangle_L, |-_r\rangle_L\}$ and inserted randomly in the sequence $S_{\rm T}$. Alice uses the quantum key, the Bell states $|\Phi^+\rangle_{AB}$ shared with Bob to encrypt the travelling states in the sequence $S_{\rm T}$ except for the decoy states. That is, Alice performs a controlled-U_2 operation (CU_2) on the particle A_i and $|\gamma_i\rangle$ $(i = 1, 2, \ldots, N)$ by using the particles A_i as the control qubit and $|\gamma_i\rangle$ as target qubit. After that, Alice sends all the travelling states to Bob. Here

$$\begin{aligned} &CU_2 = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U_2, \quad U_2 = I_1 \otimes U_{y2}, \\ &U_y = |1\rangle\langle 0| - |0\rangle\langle 1|, \quad I = I_1 \otimes I_2. \end{aligned} \tag{19}$$

The subscripts 1 and 2 in the unitary operations I and U represent the first and the second physical qubits in each logical state, respectively. The effect of the unitary operation U_1 on each logical state can be written as

$$\begin{aligned} &U_2|0_r\rangle_L = |1_r\rangle_L, \quad U_2|1_r\rangle_L = -|0_r\rangle_L, \\ &U_2|+_r\rangle_L = -|-_r\rangle_L, \quad U_2|-_r\rangle_L = |+_r\rangle_L. \end{aligned} \tag{20}$$

(III) After receiving all the states Alice sent to him, Bob asks Alice to tell him the positions and the states of the decoy states in sequence $S_{\rm T}$, and then measures them with their initial bases. Then Bob performs a CU_2 operation on particles B_i and $|\gamma_i\rangle$ $(i = 1, 2, \ldots, N)$ by using the particle B_i as the control qubit and $|\gamma_i\rangle$ as target qubit to decrypt the encrypted states in the sequence $S_{\rm T}$, similar to Alice. After that, he measures the states $|\gamma_i\rangle$ with Bell basis and records the outcomes of the measurements.

(IV) With all the measurement outcomes, Alice and Bob check the security of their transmission. They analyze the error rate of the decoy states. If the error rate is unacceptable, they abort the results and repeat the procedures from the beginning. If the error rate is very low, Bob can trust this transmission and read out the message directly.

(V) If the protocol succeeds, for each of their shared EPR pairs $|\Phi^+\rangle_{AB}$, the two parties (Alice and Bob) rotate their respective particle by angle θ, respectively. The rotation can be described as

$$R(\theta) = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}. \tag{21}$$

The state $|\Phi^+\rangle_{AB}$ does not change under bilateral operation of $R(\theta)$. The purpose of this operation is to prevent the other parties from eavesdropping (the interpretation and the selection of θ will be given later in the security analysis section). After the rotation for all the EPR pairs. Alice and Bob can repeat their procedures from step (II). That is, they use the EPR $|\Phi^+\rangle_{AB}$ pairs repeatedly as their private quantum key to transmit the secret message again in the next round.

3. Security analysis

Suppose Eve is an evil attacker who wants to eavesdrop the transmitted secret message without being detected. Now let us discuss the security of our two proposed schemes. We analyze the security of the quantum-encrypting QSDC against collective-rotation noise in detail. As for the security of the quantum-encrypting QSDC against collective-dephsing noise, it can be made the same as the case with a collective-rotation noise.

First, we analyze the security of the distribution process of the quantum key over collective-rotation noise channel. As the logical states in S_B are always in the maximal mixture of $|0_r\rangle_L$ and $|1_r\rangle_L$ $((1/2)|0_r\rangle_{LL}\langle 0_r| + (1/2)|1_r\rangle_{LL}\langle 1_r|)$ during the transmission, the intercept-resending attack strategy by Eve will not work. The transmission of the sequence S_B from Alice to Bob is completely the same as that in the Bennett–Brassard–Mermin 1992 (BBM92) QKD protocol,[3] which has been proven unconditional secure.[61,62] Therefore, there is security problem of the transmission of the sequence S_B from Alice to Bob in principle. That is to say, our distribution process of

the quantum key over collective-rotation noise channel is secure in principle.

Based on the security analysis of the distribution process of the quantum key, now we analyze the security of the process of transmitting the secret message directly between Alice and Bob with their shared quantum key. In theory, this channel-encrypting QSDC protocol is secure for any intercepting-resending attack strategies if the quantum key is private. Because the proposed scheme is equivalent to a quantum one-time-pad cryptosystem[22,63] under the condition that the quantum key is private. The encryption on a travelling state $|\gamma_i\rangle$ with a CU_2 operation makes it entangle with a quantum system in the quantum key $|\Phi^+\rangle_{AB}$. After the CU_2 operation done by Alice, the three particles A_i, B_i, and $|\gamma_i\rangle$ are in the state $|\Phi\rangle_{AB\gamma_i} = (1/\sqrt{2})(|0\rangle 0\rangle|0_r\rangle_L + |1\rangle 1\rangle|1_r\rangle_L)_{AB\gamma_i}$ or $|\Psi\rangle_{AB\gamma_i} = (1/\sqrt{2})(|0\rangle 0\rangle|1_r\rangle_L + |1\rangle 1\rangle|0_r\rangle_L)_{AB\gamma_i}$ randomly. It is obvious that the logical qubits $|\gamma_i\rangle$ in $S_{\rm T}$ are always in the maximal mixture of $|0_r\rangle_L$ and $|1_r\rangle_L$ ($|\gamma_i\rangle$=$(1/2)|0_r\rangle_{LL}\langle 0_r| + (1/2)|1_r\rangle_{LL}\langle 1_r|$) during the transmission. Therefore, the eavesdropper cannot elicit any information even if she intercepts the cipher text. If Eve wants to steal the message carried by the travelling states $|\gamma_i\rangle$, she should eavesdrop the quantum key by capturing the states sent in the distribution process of the quantum key, and then steal the information of the travelling states $|\gamma_i\rangle$ transmitted in the following rounds. However, her action will inevitably leave a track in the eavesdropping check, because the distribution process is the same as the famous BBM92 protocol,[3] which has been proved secure.

Then we consider the individual attack[17,58] on many other channel-encrypting protocols, in which the eavesdropper first entangles his own state with Alice and Bob's quantum key $|\Phi^+\rangle_{AB}$ and utilizes this entangled relation to elicit some information of the secret message without being detected. The procedure of checking eavesdropping done by the two authorized users (Alice and Bob) in this scheme, in essence, is the same as that in the BB84 QKD protocol.[1] That is, the decoy states are produced by choosing randomly one of the two bases $\{|0_r\rangle_L, |1_r\rangle_L\}$ and $\{|+_r\rangle_L, |-_r\rangle_L\}$, and are randomly inserted into the travelling states sequence $S_{\rm T}$. Also, Bob measures them with their initial bases after he receives the travelling sequence and obtains the information about their bases of the decoy states. For any eavesdropper, the bases chosen by Bob are random, even though they are announced in public finally. Same as that in the BB84 protocol,[1] any eavesdropping will inevitably disturb part of the states of the decoy states and be detected by the two authorized users if an eavesdropper eavesdrops in the quantum channel. However, different from the random classical bits in QKD, the ones transmitted in QSDC protocols are the secret message which can neither be leaked out nor be discarded. In order to make the eavesdropper using the individual attack strategy[17,58] obtain no information of the transmitted secret message before our eavesdropping check. Alice and Bob need to add a small trick before each new round. That is, they rotate their respective particle by angle θ respectively, for each of their shared EPR pairs $|\Phi^+\rangle_{AB}$. Here the rotation can be described as

$$R(\theta) = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}. \tag{22}$$

It has been proved in Ref. [59] that the individual attacks[18,58] on many other channel-encrypting protocols are invalid when $\theta \neq k\pi + \pi/4$ ($k = 0, \pm 1, \pm 2, \ldots$). Therefore, the eavesdropper cannot elicit any information with these individual attacks when we choose a proper θ and will inevitably be detected in the eavesdropping check.

So far, we have demonstrated that the proposed protocols can resist all the intercept-resending attack strategies and the individual attacks that are fatal to many other channel-encrypting schemes. Moreover, as the noises in a practical channel may affect the entanglement of the private quantum key, the users in our protocols should exploit entanglement purification[52] to keep the entanglement in the quantum key, and do quantum privacy amplification[63,64] on them to insure the security of their private quantum key as well.

4. Conclusion

In summary, two robust channel-encrypting quantum secure communication protocols over different collective-noise channels are proposed. One is against collective-dephasing noise, the other is against collective-rotation noise. Different from other channel-encrypting schemes, the procedures of sharing the EPR pairs which will act as the quantum key in the proposed fault-tolerant protocols between two authorized users are described in detail. In our protocols,

the classical information is encoded into two-particle logical states, which is invariant when it is transmitted in the collective-noise channel. For checking eavesdropping, the two parties only need to perform the two-particle measurements on the decoy states. Furthermore, the quantum key is reusable and the eavesdropper cannot elicit any information from the states that Alice sends to Bob.

Compared with other quantum secure direct communication protocols, there are several remarkable advantages in our protocols. First, different from the previous channel-encrypting QSDC scheme designed in ideal conditions, our two protocols can resist collective noise. Second, our proposed protocols can resist individual attacks[58] which are fatal to many other channel-encrypting protocols.[17–19] Third, only passive detection is enough to gain the message, except for the requirement of two nonorthogonal bases measurement for the eavesdropping check, Bob need not switch his two conjugate bases to obtain the secret message. Moreover, it is unnecessary for the two parties to discard states. In theory, the intrinsic efficiencies of both the protocols are high since there is no need to consume any entangled states including both the quantum key and the information carriers except the ones used for eavesdropping check.

References

[1] Bennett C H and Brassard G 1984 *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processings,* Bangalore, India, p. 175

[2] Ekert A E 1991 *Phys. Rev. Lett.* **67** 661

[3] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557

[4] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121

[5] Gao F, Guo F Z, Wen Q Y and Zhu F C 2006 *Phys. Lett.* A **349** 53

[6] Cabello A 2000 *Phys. Rev.* A **61** 052312

[7] Zhang Y S, Li C F and Guo G C 2001 *Phys. Rev.* A **63** 036301

[8] Song D 2004 *Phys. Rev.* A **69** 034301

[9] Huang W, Guo F Z, Huang Z, Wen Q Y and Zhu F C 2011 *Opt. Commun.* **284** 536

[10] Guo F Z, Liu T L, Wen Q Y and Zhu F C 2006 *Int. J. Quantum Inform.* **4** 769

[11] Goldenberg L and Vaidman L 1995 *Phys. Rev. Lett.* **75** 1239

[12] Koashi M and Imoto N 1997 *Phys. Rev. Lett.* **79** 2383

[13] Guo G P, Li C F, Shi B S, Li J and Guo G C 2001 *Phys. Rev.* A **64** 042301

[14] Deng F G and Long G L 2003 *Phys. Rev.* A **68** 042315

[15] Deng F G, Long G L and Liu X S 2003 *Phys. Rev.* A **68** 042317

[16] Tan Y G and Cai Q Y 2010 *Eur. Phys. J.* D **56** 449

[17] Zhang Y S, Li C F and Guo G C 2001 *Phys. Rev.* A **64** 024302

[18] Karimipour V, Bahraminasab A and Bagherinezhad S 2002 *Phys. Rev.* A **65** 052331

[19] Bagherinezhad S and Karimipour V 2003 *Phys. Rev.* A **67** 044302

[20] Guo F Z, Gao F, Wen Q Y and Zhu F C 2010 *Int. J. Quantum Inform.* **8** 1013

[21] Long G L and Liu X S 2002 *Phys. Rev.* A **65** 032302

[22] Deng F G and Long G L 2004 *Phys. Rev.* A **69** 052319 (2004)

[23] Boström K and Felbinger T 2002 *Phys. Rev. Lett.* **89** 187902

[24] Long G L, Deng F G, Wang C, Li X H, Wen K and Wang W Y 2007 *Front. Phys. Chin.* **2** 251

[25] Gao T, Yan F L and Wang Z X 2004 *Nuovo Cimento Della Societa Italiana Di Fisica* B **119** 313

[26] Wójcik A and Felbinger T 2003 *Phys. Rev. Lett.* **90** 157901

[27] Cai Q Y 2003 *Phys. Rev. Lett.* **91** 109801

[28] Cai Q Y and Li B W 2004 *Phys. Rev.* A 69 054301

[29] Wang C, Deng F G and Long G L 2005 *Opt. Commun.* **253** 15

[30] Wang C, Deng F G and Long G L 2005 *Phys. Rev.* A **71** 044305

[31] Li X H, Zhou P, Liang Y J, Li C Y, Zhou H Y and Deng F G 2006 *Chin. Phys. Lett.* **23** 1080

[32] Deng F G, Li X H, Chun Y L, Zhou P and Zhou H Y 2006 *Phys. Lett.* A **359** 359

[33] Zhang Z J, Man Z X and Li Y 2004 *Phys. Lett.* A **333** 46

[34] Lin S, Wen Q Y, Gao F and Zhu F C 2008 *Phys. Rev.* A **78** 064304

[35] Gao F, Qin S J, Wen Q Y and Zhu F C 2010 *Opt. Commun.* **283** 192

[36] Yang Y G and Wen Q Y 2008 *Sci. Chin.* G: *Phys. Mech. Astron.* **51** 176

[37] Gu B, Huang Z Y, Xia F and Chen Y L 2011 *Commun. Theor. Phys.* **56** 659

[38] Gu B, Huang Y G, Fang X and Zhang C Y 2011 *Chin. Phys.* B **20** 100309

[39] Wang J, Zhang Q and Tang C J 2006 *Phys. Lett.* A **358** 256

[40] Dong L, Xiu X M, Gao Y and Chi F 2008 *Commun. Theor. Phys.* **50** 359

[41] Zhang Z J, Liu J, Wang D and Shi S H 2007 *Phys. Rev.* A **75** 02630

[42] Yan F L and Zhang X Q 2004 *Eur. Phys. J.* B **41** 75

[43] Zhu A D, Xia Y, Fan Q B and Zhang S 2006 *Phys. Rev.* A **73** 022338

[44] Yuan H, Song J and He Q 2008 *Commun. Theor. Phys.* **50** 627

[45] Qin S J, Gao F, Wen Q Y and Zhu F C 2010 *Commun. Theor. Phys.* **53** 645

[46] Qin S J, Wen Q Y and Wen L M 2009 *Sci. Chin.* G: *Phys. Mech. Astron.* **52** 1208

[47] Yang C, Tsai C and Hwang T 2011 *Sci. Chin.* G: *Phys. Mech. Astron.* **54** 496

[48] Yang J, Wang C and Zhang R 2010 *Chin. Phys.* B **19** 110311

[49] Zhang X L, Zhang Y X and Wei H 2009 *Chin. Phys.* B **18** 435

[50] Li X H, Li C Y, Deng F G, Zhou P, Liang Y J and Zhou H Y 2007 *Chin. Phys.* **16** 2149

[51] Zanardi P and Rasetti M 1997 *Phys. Rev. Lett.* **79** 3306

[52] Bennett C H, Brassard G, Popescu S, Schumacher B, Smolin J A and Wootters W K 1996 *Phys. Rev. Lett.* **76** 722

[53] Li X H, Deng F G and Zhou H Y 2007 *Appl. Phys. Lett.* **91** 144101

[54] Walton Z D, Abouraddy A F, Sergienko A V, Saleh B E A and Teich M C 2003 *Phys. Rev. Lett.* **91** 087901

[55] Li X H, Zhao B K, Sheng Y B, Deng F G and Zhou H Y 2009 *Int. J. Quantum Inform.* **7** 1479

[56] Boileau J C, Gottesman D, Laflamme R, Poulin D and Spekkens R W 2004 *Phys. Rev. Lett.* **92** 017901

[57] Li X H, Deng F G and Zhou H Y 2008 *Phys. Rev.* A **78** 022321

[58] Gao F, Guo F Z, Wen Q Y and Zhu F C 2005 *Phys. Rev.* A **72** 066301

[59] Gao F, Qin S J, Wen Q Y and Zhu F C 2005 *Lecture Notes in Computer Science*, Vol. 3822 December 15–17, 2005, Beijing, China, pp. 302–312

[60] Lo H K and Chau H F 1999 *Science* **283** 2050

[61] Inamori H, Rallan L and Vedral V 2001 *J. Phys.* A: *Math. Gen.* **34** 6913

[62] Waks E, Zeevi A and Yamamoto Y 2002 *Phys. Rev.* A **65** 052310

[63] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145

[64] Deutsch D, Ekert A, Jozsa R, Macchiavello C, Popescu S and Sanpera A 1996 *Phys. Rev. Lett.* **77** 2818