Fault tolerant deterministic secure quantum communication using logical Bell states against collective noise*

Wang Chao(王 朝)[a)b)†], Liu Jian-Wei(刘建伟)[a)], Chen Xiu-Bo(陈秀波)[c)d)], Bi Ya-Gang(毕亚港)[b)], and Shang Tao(尚 涛)[a)]

[a)] *School of Electronic and Information Engineering, Beihang University, Beijing* 100191, *China*
[b)] *Air Force Command College, Beijing* 100097, *China*
[c)] *Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*
[d)] *State Key Laboratory of Information Security (Institute of Information Engineering, Chinese Academy of Sciences), Beijing* 100093, *China*

(Received 12 August 2014; revised manuscript received 1 November 2014; published online 10 February 2015)

This study proposes two novel fault tolerant deterministic secure quantum communication (DSQC) schemes resistant to collective noise using logical Bell states. Either DSQC scheme is constructed based on a new coding function, which is designed by exploiting the property of the corresponding logical Bell states immune to collective-dephasing noise and collective-rotation noise, respectively. The secret message can be encoded by two simple unitary operations and decoded by merely performing Bell measurements, which can make the proposed scheme more convenient in practical applications. Moreover, the strategy of one-step quanta transmission, together with the technique of decoy logical qubits checking not only reduces the influence of other noise existing in a quantum channel, but also guarantees the security of the communication between two legitimate users. The final analysis shows that the proposed schemes are feasible and robust against various well-known attacks over the collective noise channel.

Keywords: collective noise, deterministic secure quantum communication, logical Bell states

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.1088/1674-1056/24/4/040304

1. Introduction

Quantum communication, known as a kind of theoretically unconditionally secure communication mode, has attracted enormous attention in recent years. Since a pioneering quantum key distribution (QKD) protocol was put forward by Bennett and Brassard in 1984, called the BB84 protocol,[1] more and more works have been focused on this field and various kinds of QKD protocols[2–8] have been presented. In a QKD protocol, the random shared secret key is established first through a quantum channel and then utilized to encrypt the transmitted message between two remote authorized parties. Another remarkable research field, quantum direct communication (QDC) which includes quantum secure direct communication (QSDC)[9–19] and deterministic secure quantum communication (DSQC),[20–30] has also been developed quickly.

Different from QKD, QDC provides a new means to communicate the secret message directly without creating a random shared key to encrypt it in advance. In 2002, Long and Liu proposed an efficient QKD scheme based on quantum data blocks, which can also be recognized as the first QSDC protocol.[19] Later, another two-step QSDC protocol exploiting the quantum dense coding was proposed by Deng and Long in 2003, which is the first truly secure QSDC protocol, and a criterion for QSDC was provided in this protocol.[10] After that, the extensive QSDC protocols[11–19] are presented and the idea of QSDC has been realized in many quantum communication systems. Especially, in DSQC the legitimate receiver can instantaneously obtain the deterministic information after exchanging one round of classical communication. In 1999, Shimizu and Imoto[20] proposed the first DSQC protocol, and another DSQC protocol based on single photon two-qubit states was presented by Beige *et al.*[21] in 2002. Thereafter, many advanced DSQC protocols have been introduced utilizing the entangled quantum states.[22–30]

However, these protocols can only work well under an ideal condition that the quantum channel is noiseless. Actually, the channel noise is inevitable. In a practical transmission process, the quantum channel is always influenced by thermal and mechanical fluctuations of some medium (e.g., the optical fiber), which tends to produce channel noise. Generally speaking, the channel noise not only changes the fidelity of the quantum states carrying the information, which will decrease the successful probability of the schemes, but also gives

*Project supported by the National Natural Science Foundation of China (Grant Nos. 61272501, 61272514, 61170272, 61472048, 61402058, 61121061, and 61411146001), the Program for New Century Excellent Talents in University of China (Grant No. NCET-13-0681), the National Development Foundation for Cryptological Research (Grant No. MMJJ201401012), the Fok Ying Tong Education Foundation (Grant No. 131067), the Natural Science Foundation of Beijing (Grant Nos. 4132056 and 4152038), the Postdoctoral Science Foundation of China (Grant No. 2014M561826), and the National Key Basic Research Program, China (Grant No. 2012CB315905)

†Corresponding author. E-mail: wangchaopaper@126.com

© 2015 Chinese Physical Society and IOP Publishing Ltd

the eavesdropper a chance to disguise her disturbance with a better fiber, which will directly affect the security of the quantum communication.[31] The practical experiments show that the fluctuation is always slow in time. Therefore, if the qubits travel inside a time window shorter than the variation of the noise sources, these qubits will be affected by the identical noise, which is known as the collective noise.[32,33] Thus, at present, it is always suppose that the channel noise is a collective one in quantum cryptography communication.

In order to overcome the noise disturbance, one needs to design new fault tolerant protocols over the noisy channel or new physical channels for implementing the original protocols. Now, there are two valid solutions to deal with such a problem: one way is to design a new protocol with a higher channel error rate threshold, such as the results presented in Refs. [34] and [35]; the other way is first to construct an appropriate channel noise model and then find a resolvent accordingly to reduce or eliminate the quantum channel noise, such as a quantum error correct code (QECC),[36] single-photon error rejection,[37] and decoherence-free (DF) subspace.[38,39] Among these proposed methods, DF subspace is an important one since it can be made up of several physical qubits experiencing the identical noise and keep invariant over a collective-noise channel. Therefore, DF subspace is frequently used in quantum communication to implement a fault-tolerance communication. Varieties of quantum cryptographic protocols against collective noise have been developed quickly, including QKD,[31–33,40–44] QSDC,[45–50] and quantum secret sharing (QSS),[51–55] etc.

However, compared to those fields, so few DSQC protocols over a collective noise channel have been published.[56–59] In fact, DSQC has some advantages over QSDC in a practical channel. The major advantage is that the qubits carrying the secret message are not transmitted again after the eavesdropping check in DSQC, which will make DSQC more secure than QSDC over a noisy channel and make DSQC more convenient for quantum error correction. In 2009, Dong *et al.*[56] presented a DSQC scheme against collective-dephasing noise by using EPR pairs and auxiliary photons, without giving the corresponding scheme against collective-rotation noise. And, in the same year, Gu *et al.*[57] proposed two DSQC protocols exploiting three-photon entangled states over a collective-dephasing noise channel and a collective-rotation noise channel, respectively. Then, in 2013, by taking advantage of the GHZ state and GHZ-like state, Yang *et al.*[58] designed two DSQC protocols, each of which is robust under one kind of collective noise: collective-dephasing noise, and collective-rotation noise, respectively. Just recently, Yuan *et al.* carefully investigated four special two-qubit entangled states and presented a new DSQC protocol against collective rotating noise based on order rearrangement of photon pairs.[59]

Different from the above-mentioned DSQC protocols, in this work, two fault tolerant DSQC schemes against collective noise, i.e., the collective-dephasing noise and the collective-rotation noise, respectively, are put forward based on the logical Bell states for the first time. By merely using the property of logical Bell states immune to collective-noise, two novel coding functions are designed, each of which can be applied to construct the corresponding DSQC scheme. In the proposed DSQC schemes, the sender, Alice, only performs two simple unitary operations on the corresponding qubits of the prepared logical Bell states to encode the transmitted secret message. The receiver, Bob, can decode the secret information by performing Bell measurement after the additional classical bit is exchanged between two legitimate users. In practical application, these encoding and decoding operations can be realized easily, and the logical Bell states, as the quantum resource, are verified to be feasible in experiment. More importantly, the proposed schemes combine the one-step quanta transmission strategy and the decoy logical qubits checking technique, which can effectively reduce the influence of other noise existing in the quantum channel, and further guarantee the unconditional security against various kinds of attacks, such as the information leakage attack, the intercept-resend attack, the entangle-measure attack, the correlation–elicitation attack, and the Trojan horse attack, etc.

The structure of the rest of the paper is organized as follows. In Section 2, we first introduce the related works. Then, we construct two new coding functions and propose our DSQC schemes over the collective noise channel in Section 3 and Section 4, respectively. Then, in Section 5, we analyze the security of the proposed schemes. Finally, in Section 6, we summarize the work and give the main conclusion.

2. The related works

In this section, the elementary models of collective noise and DF subspace are first introduced. Then, the logical Bell states immune to collective-dephasing noise and collective-rotation noise are further defined, respectively.

2.1. The elementary models of collective noise and DF subspace

The transformation of collective noise can be described by a unitary operation $U(t)$, where t denotes the transmission time and means a temporal dependence. As mentioned in Ref. [32], if several photons transmit through the noisy channel and the time delay between them is small compared to τ_{fluc}, the effect of collective noise on an N-qubit quantum state can be well approximated as the following model

$$\rho_N \Rightarrow [U(t)]^{\otimes N} \rho_N [U(t)^{\dagger}]^{\otimes N}, \tag{1}$$

where $\tau_{\rm fluc}$ is the shortest time scale of thermal and mechanical fluctuations of the fiber, ρ_N is a quantum state composed of N qubits, and $[U(t)]^{\otimes N} = U(t)\otimes\cdots\otimes U(t)$ denotes the tensor product of N unitary transformation operations $U(t)$.

The collective noise is divided into two main types: the collective-dephasing noise and the collective-rotation noise. Therefore, when a polarized photon state $|0\rangle$ (horizontal polarization state) or $|1\rangle$ (vertical polarization state) passes through the noisy channel, it will experience the transformations of the collective-dephasing noise and the collective-rotation noise, which can be formulized as follows according to Eq. (1), respectively.[33]

(i) A collective-dephasing noise can be described as

$$|0\rangle \Rightarrow U_{\rm d}|0\rangle = |0\rangle, \quad |1\rangle \Rightarrow U_{\rm d}|1\rangle = {\rm e}^{{\rm i}\theta}|1\rangle.$$

(ii) A collective-rotation noise can be described as

$$|0\rangle \Rightarrow U_{\rm r}|0\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle,$$
$$|1\rangle \Rightarrow U_{\rm r}|1\rangle = -\sin\theta|0\rangle + \cos\theta|1\rangle.$$

Here,

$$U_{\rm d} = \begin{pmatrix} 1 & 0 \\ 0 & {\rm e}^{{\rm i}\theta} \end{pmatrix} \quad \text{and} \quad U_{\rm r} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

indicate the equivalent unitary operations of the collective-dephasing noise and the collective-rotation noise respectively, and θ is the parameter of the noise fluctuating with time.

The DF subspace is invariant under collective noise no matter how strong the interaction is, which can be modeled as

$$\rho_N = [U(t)]^{\otimes N}\rho_N[U(t)^{\dagger}]^{\otimes N}. \tag{2}$$

Due to the invariance property, the transmitted information is always carried by DF subspace in quantum communication. The amount of quantum information that a given DF subspace is able to protect is determined by the number of N qubits used.[60] Here, the elementary model of DF subspace for $N = 2$ is introduced as follows.

To combat the collective-dephasing noise, two basic logical qubits can be constructed as $|0_{\rm dL}\rangle = |0\rangle_1 \otimes |1\rangle_2 = |01\rangle_{12}$ and $|1_{\rm dL}\rangle = |1\rangle_1 \otimes |0\rangle_2 = |10\rangle_{12}$, respectively. Here, the subscript "1" and "2" indicate two physical qubits, and "dL" denotes the logical qubit immune to collective-dephasing noise.

Therefore, for $N = 2$, the DF subspace spanned by $|0_{\rm dL}\rangle$ and $|1_{\rm dL}\rangle$ can be generalized as

$$|\Phi_{\rm dL}\rangle = c_0|0_{\rm dL}\rangle + c_1|1_{\rm dL}\rangle.$$

Here c_0 and c_1 are both complex numbers. In addition,

$$|+_{\rm dL}\rangle = \frac{1}{\sqrt{2}}(|0_{\rm dL}\rangle + |1_{\rm dL}\rangle) = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{12} = |\Psi^+\rangle_{12},$$
$$|-_{\rm dL}\rangle = \frac{1}{\sqrt{2}}(|0_{\rm dL}\rangle - |1_{\rm dL}\rangle) = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)_{12} = |\Psi^-\rangle_{12},$$

are another two common logical qubits resistant to collective-dephasing noise, in which $|\Psi^+\rangle_{12}$ and $|\Psi^-\rangle_{12}$ are two antiparallel Bell states from $\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$.

Similarly, to counteract the collective-rotation noise two basic logical qubits can be constructed as

$$|0_{\rm rL}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{12} = |\Phi^+\rangle_{12}$$

and

$$|1_{\rm rL}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)_{12} = |\Psi^-\rangle_{12},$$

respectively. Accordingly, the generated DF subspace for $N = 2$ is that

$$|\Phi_{\rm rL}\rangle = c_0|0_{\rm rL}\rangle + c_1|1_{\rm rL}\rangle = c_0|\Phi^+\rangle_{12} + c_1|\Psi^-\rangle_{12},$$

where, the subscript "rL" denotes the logical qubit immune to collective-rotation noise. Obviously,

$$|+_{\rm rL}\rangle = \frac{1}{\sqrt{2}}(|0_{\rm rL}\rangle + |1_{\rm rL}\rangle) = \frac{1}{\sqrt{2}}(|\Phi^+\rangle_{12} + |\Psi^-\rangle_{12}),$$
$$|-_{\rm rL}\rangle = \frac{1}{\sqrt{2}}(|0_{\rm rL}\rangle - |1_{\rm rL}\rangle) = \frac{1}{\sqrt{2}}(|\Phi^+\rangle_{12} - |\Psi^-\rangle_{12})$$

are another two common logical qubits immune to collective-rotation noise.

2.2. The logical Bell states immune to collective-dephasing noise

As explained in Ref. [60], the immunity of four-qubits polarization-entangled DF states against collective noise is experimentally verified by showing their invariance when passing the four photons through a noisy environment simulated by birefringent transmission medium. The special four-qubits DF states immune to collective noise, called logical Bell states, can be generated by using the product state of the aforementioned basic logical qubits, such as $|0_{\rm dL}\rangle$, $|1_{\rm dL}\rangle$, $|+_{\rm dL}\rangle$, $|-_{\rm dL}\rangle$.

To resist collective-dephasing noise, four logical Bell states denoted with $|\Phi^+_{\rm dL}\rangle$, $|\Phi^-_{\rm dL}\rangle$, $|\Psi^+_{\rm dL}\rangle$, and $|\Psi^-_{\rm dL}\rangle$ are constructed by entangling $|0_{\rm dL}\rangle$ and $|1_{\rm dL}\rangle$ as shown in Eq. (3).

$$\begin{aligned}
|\Phi^+_{\rm dL}\rangle &= \frac{1}{\sqrt{2}}(|0_{\rm dL}\rangle|0_{\rm dL}\rangle + |1_{\rm dL}\rangle|1_{\rm dL}\rangle) \\
&= \frac{1}{\sqrt{2}}(|01\rangle_{12}|01\rangle_{34} + |10\rangle_{12}|10\rangle_{34}) \\
&= \frac{1}{\sqrt{2}}(|00\rangle_{13}|11\rangle_{24} + |11\rangle_{13}|00\rangle_{24}) \\
&= \frac{1}{\sqrt{2}}(|\Phi^+\rangle_{13}|\Phi^+\rangle_{24} - |\Phi^-\rangle_{13}|\Phi^-\rangle_{24}), \\
|\Phi^-_{\rm dL}\rangle &= \frac{1}{\sqrt{2}}(|0_{\rm dL}\rangle|0_{\rm dL}\rangle - |1_{\rm dL}\rangle|1_{\rm dL}\rangle) \\
&= \frac{1}{\sqrt{2}}(|01\rangle_{12}|01\rangle_{34} - |10\rangle_{12}|10\rangle_{34}) \\
&= \frac{1}{\sqrt{2}}(|00\rangle_{13}|11\rangle_{24} - |11\rangle_{13}|00\rangle_{24}) \\
&= \frac{1}{\sqrt{2}}(|\Phi^-\rangle_{13}|\Phi^+\rangle_{24} - |\Phi^+\rangle_{13}|\Phi^-\rangle_{24}),
\end{aligned}$$

$$
\begin{aligned}
\left|\Psi_{\mathrm{dL}}^{+}\right\rangle &= \frac{1}{\sqrt{2}}(|0_{\mathrm{dL}}\rangle|1_{\mathrm{dL}}\rangle+|1_{\mathrm{dL}}\rangle|0_{\mathrm{dL}}\rangle)\\
&= \frac{1}{\sqrt{2}}(|01\rangle_{12}|10\rangle_{34}+|10\rangle_{12}|01\rangle_{34})\\
&= \frac{1}{\sqrt{2}}(|01\rangle_{13}|10\rangle_{24}+|10\rangle_{13}|01\rangle_{24})\\
&= \frac{1}{\sqrt{2}}(\left|\Psi^{+}\right\rangle_{13}\left|\Psi^{+}\right\rangle_{24}-\left|\Psi^{-}\right\rangle_{13}\left|\Psi^{-}\right\rangle_{24}),\\
\left|\Psi_{\mathrm{dL}}^{-}\right\rangle &= \frac{1}{\sqrt{2}}(|0_{\mathrm{dL}}\rangle|1_{\mathrm{dL}}\rangle-|1_{\mathrm{dL}}\rangle|0_{\mathrm{dL}}\rangle)\\
&= \frac{1}{\sqrt{2}}(|01\rangle_{12}|10\rangle_{34}-|10\rangle_{12}|01\rangle_{34})\\
&= \frac{1}{\sqrt{2}}(|01\rangle_{13}|10\rangle_{24}-|10\rangle_{13}|01\rangle_{24})\\
&= \frac{1}{\sqrt{2}}(\left|\Psi^{-}\right\rangle_{13}\left|\Psi^{+}\right\rangle_{24}-\left|\Psi^{+}\right\rangle_{13}\left|\Psi^{-}\right\rangle_{24}), \qquad (3)
\end{aligned}
$$

Obviously, the logical Bell states $\left|\Phi_{\mathrm{dL}}^{+}\right\rangle$, $\left|\Phi_{\mathrm{dL}}^{-}\right\rangle$, $\left|\Psi_{\mathrm{dL}}^{+}\right\rangle$, and $\left|\Psi_{\mathrm{dL}}^{-}\right\rangle$ are resistant to the collective-dephasing noise. To distinguish these four logical Bell states, the corresponding Bell measurements on the 1st and the 3rd particles, and on the 2nd and the 4th particles should be performed, respectively, in which the measurement results are all different from one another according to Eq. (3). Note that, the 2nd and the 4th qubits in $\left|\Psi_{\mathrm{dL}}^{+}\right\rangle$ and $\left|\Psi_{\mathrm{dL}}^{-}\right\rangle$ are invariant over the collective-dephasing noise channel, which can be demonstrated as follows:

$$
\begin{aligned}
\left|\Psi_{\mathrm{dL}}^{+}\right\rangle &= \frac{1}{\sqrt{2}}(|01\rangle_{12}|10\rangle_{34}+|10\rangle_{12}|01\rangle_{34})\\
&= \frac{1}{\sqrt{2}}(|01\rangle_{13}|1_{\mathrm{dL}}\rangle_{24}+|10\rangle_{13}|0_{\mathrm{dL}}\rangle_{24})\\
&\Rightarrow \frac{1}{\sqrt{2}}(|01\rangle_{13}\otimes \mathrm{e}^{\mathrm{i}\theta}|1_{\mathrm{dL}}\rangle_{24}+|10\rangle_{13}\otimes \mathrm{e}^{\mathrm{i}\theta}|0_{\mathrm{dL}}\rangle_{24}),\\
\left|\Psi_{\mathrm{dL}}^{-}\right\rangle &= \frac{1}{\sqrt{2}}(|01\rangle_{12}|10\rangle_{34}-|10\rangle_{12}|01\rangle_{34})\\
&= \frac{1}{\sqrt{2}}(|01\rangle_{13}|1_{\mathrm{dL}}\rangle_{24}-|10\rangle_{13}|0_{\mathrm{dL}}\rangle_{24})\\
&\Rightarrow \frac{1}{\sqrt{2}}(|01\rangle_{13}\otimes \mathrm{e}^{\mathrm{i}\theta}|1_{\mathrm{dL}}\rangle_{24}-|10\rangle_{13}\otimes \mathrm{e}^{\mathrm{i}\theta}|0_{\mathrm{dL}}\rangle_{24}).
\end{aligned}
$$

Here, $\mathrm{e}^{\mathrm{i}\theta}$ is the global phase factor which is irrelevant to the observability of quantum states, and thus the actual fidelity of a quantum state can be regarded as 1 when it experiences the quantum collective-dephasing noise channel.

2.3. The logical Bell states immune to collective-rotation noise

With the similar means as stated in Subsection 2.2, the corresponding logical Bell states immune to collective-rotation noise, denoted with $\left|\Phi_{\mathrm{rL}}^{+}\right\rangle$, $\left|\Phi_{\mathrm{rL}}^{-}\right\rangle$, $\left|\Psi_{\mathrm{rL}}^{+}\right\rangle$, and $\left|\Psi_{\mathrm{rL}}^{-}\right\rangle$, can be formed based on the basic logical qubits $|0_{\mathrm{rL}}\rangle$ and $|1_{\mathrm{rL}}\rangle$ as the following Eq. (4).

$$
\begin{aligned}
\left|\Phi_{\mathrm{rL}}^{+}\right\rangle &= \frac{1}{\sqrt{2}}(|0_{\mathrm{rL}}\rangle|0_{\mathrm{rL}}\rangle+|1_{\mathrm{rL}}\rangle|1_{\mathrm{rL}}\rangle)\\
&= \frac{1}{\sqrt{2}}(\left|\Phi^{+}\right\rangle_{12}\left|\Phi^{+}\right\rangle_{34}+\left|\Psi^{-}\right\rangle_{12}\left|\Psi^{-}\right\rangle_{34})\\
&= \frac{1}{2\sqrt{2}}(|0000\rangle+|0011\rangle+|1100\rangle+|1111\rangle\\
&\quad +|0101\rangle-|0110\rangle-|1001\rangle+|1010\rangle)_{1234}\\
&= \frac{1}{\sqrt{2}}(\left|\Phi^{+}\right\rangle_{13}\left|\Phi^{+}\right\rangle_{24}+\left|\Psi^{-}\right\rangle_{13}\left|\Psi^{-}\right\rangle_{24}),\\
\left|\Phi_{\mathrm{rL}}^{-}\right\rangle &= \frac{1}{\sqrt{2}}(|0_{\mathrm{rL}}\rangle|0_{\mathrm{rL}}\rangle-|1_{\mathrm{rL}}\rangle|1_{\mathrm{rL}}\rangle)\\
&= \frac{1}{\sqrt{2}}(\left|\Phi^{+}\right\rangle_{12}\left|\Phi^{+}\right\rangle_{34}-\left|\Psi^{-}\right\rangle_{12}\left|\Psi^{-}\right\rangle_{34})\\
&= \frac{1}{2\sqrt{2}}(|0000\rangle+|0011\rangle+|1100\rangle+|1111\rangle\\
&\quad -|0101\rangle+|0110\rangle+|1001\rangle-|1010\rangle)_{1234}\\
&= \frac{1}{\sqrt{2}}(\left|\Phi^{-}\right\rangle_{13}\left|\Phi^{-}\right\rangle_{24}+\left|\Psi^{+}\right\rangle_{13}\left|\Psi^{+}\right\rangle_{24}),\\
\left|\Psi_{\mathrm{rL}}^{+}\right\rangle &= \frac{1}{\sqrt{2}}(|0_{\mathrm{rL}}\rangle|1_{\mathrm{rL}}\rangle+|1_{\mathrm{rL}}\rangle|0_{\mathrm{rL}}\rangle)\\
&= \frac{1}{\sqrt{2}}(\left|\Phi^{+}\right\rangle_{12}\left|\Psi^{-}\right\rangle_{34}+\left|\Psi^{-}\right\rangle_{12}\left|\Phi^{+}\right\rangle_{34})\\
&= \frac{1}{2\sqrt{2}}(|0001\rangle-|0010\rangle+|1101\rangle-|1110\rangle\\
&\quad +|0100\rangle+|0111\rangle-|1000\rangle-|1011\rangle)_{1234}\\
&= \frac{1}{\sqrt{2}}(\left|\Phi^{-}\right\rangle_{13}\left|\Psi^{+}\right\rangle_{24}-\left|\Psi^{+}\right\rangle_{13}\left|\Phi^{-}\right\rangle_{24}),\\
\left|\Psi_{\mathrm{rL}}^{-}\right\rangle &= \frac{1}{\sqrt{2}}(|0_{\mathrm{rL}}\rangle|1_{\mathrm{rL}}\rangle-|1_{\mathrm{rL}}\rangle|0_{\mathrm{rL}}\rangle)\\
&= \frac{1}{\sqrt{2}}(\left|\Phi^{+}\right\rangle_{12}\left|\Psi^{-}\right\rangle_{34}-\left|\Psi^{-}\right\rangle_{12}\left|\Phi^{+}\right\rangle_{34})\\
&= \frac{1}{2\sqrt{2}}(|0001\rangle-|0010\rangle+|1101\rangle-|1110\rangle\\
&\quad -|0100\rangle-|0111\rangle+|1000\rangle+|1011\rangle)_{1234}\\
&= \frac{1}{\sqrt{2}}(\left|\Phi^{+}\right\rangle_{13}\left|\Psi^{-}\right\rangle_{24}-\left|\Psi^{-}\right\rangle_{13}\left|\Phi^{+}\right\rangle_{24}). \qquad (4)
\end{aligned}
$$

Undoubtedly, the generated four logical Bell states $\left|\Phi_{\mathrm{rL}}^{+}\right\rangle$, $\left|\Phi_{\mathrm{rL}}^{-}\right\rangle$, $\left|\Psi_{\mathrm{rL}}^{+}\right\rangle$, and $\left|\Psi_{\mathrm{rL}}^{-}\right\rangle$ are the linear superposition of the product state of $|0_{\mathrm{rL}}\rangle$ and $|1_{\mathrm{rL}}\rangle$, so they are resistant to the collective-rotation noise. To distinguish these four logical Bell states, the corresponding Bell measurements on the 1st and 3rd particles, and on the 2nd and 4th particles in each logical Bell state should be performed, respectively. Note that, similar to Subsection 2.2, the 2nd and 4th qubits in $\left|\Phi_{\mathrm{rL}}^{+}\right\rangle$ and $\left|\Psi_{\mathrm{rL}}^{-}\right\rangle$ are invariant over the collective-rotation noise channel.

3. New coding functions

In this section, two novel coding functions are constructed in detail. The coding function for the logical Bell states immune to collective-dephasing noise is introduced in Subsection 3.1, and the other one for the logical Bell states immune to collective-rotation noise is proposed in Subsection 3.2. In either coding function, the specific unitary operations are utilized to encode the classical secret message, and the Bell mea-

surements are used to decode the corresponding secret message.

3.1. Coding function for logical Bell states immune to collective-dephasing noise

In this subsection, the coding function, including encoding function and decoding function, is constructed over the collective-dephasing noise channel as follows.

3.1.1. Encoding function

It is not difficult to find that there is a specific property among the four logical Bell states immune to collective-dephasing noise according to Eq. (3). That is, $\left|\Psi_{\mathrm{dL}}^{+}\right\rangle$ and $\left|\Psi_{\mathrm{dL}}^{-}\right\rangle$ can be transformed into each other if the corresponding unitary operation is performed on the 4th qubit in either state, which can be exploited to design the encoding function in our proposed DSQC scheme against the collective-dephasing noise.

In the encoding function, two unitary operations U_0 and U_1 are introduced to encode a one-bit classical message "0" and "1", respectively, where $U_0 = I = |0\rangle\langle 0| + |1\rangle\langle 1|$, $U_1 = \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$. Here, we take $\left|\Psi_{\mathrm{dL}}^{+}\right\rangle$ as the quantum information carrier, and then encode one bit classical message by performing the corresponding unitary operation on the 4th qubit in $\left|\Psi_{\mathrm{dL}}^{+}\right\rangle$, which can be shown in Eq. (5) and Eq. (6).

For encoding one classical bit "0",

$$\begin{aligned} U_0\left|\Psi_{\mathrm{dL}}^{+}\right\rangle &= U_0\frac{1}{\sqrt{2}}(|01\rangle_{12}|10\rangle_{34}+|10\rangle_{12}|01\rangle_{34}) \\ &= \frac{1}{\sqrt{2}}(|01\rangle_{12}|1\rangle_3\otimes I|0\rangle_4+|10\rangle_{12}|0\rangle_3\otimes I|1\rangle_4) \\ &= \frac{1}{\sqrt{2}}(|01\rangle_{12}|10\rangle_{34}+|10\rangle_{12}|01\rangle_{34}) \\ &= \left|\Psi_{\mathrm{dL}}^{+}\right\rangle. \end{aligned} \tag{5}$$

For encoding one classical bit "1",

$$\begin{aligned} U_1\left|\Psi_{\mathrm{dL}}^{+}\right\rangle &= U_1\frac{1}{\sqrt{2}}(|01\rangle_{12}|10\rangle_{34}+|10\rangle_{12}|01\rangle_{34}) \\ &= \frac{1}{\sqrt{2}}(|01\rangle_{12}|1\rangle_3\otimes\sigma_z|0\rangle_4+|10\rangle_{12}|0\rangle_3\otimes\sigma_z|1\rangle_4) \\ &= \frac{1}{\sqrt{2}}(|01\rangle_{12}|10\rangle_{34}-|10\rangle_{12}|01\rangle_{34}) \\ &= \left|\Psi_{\mathrm{dL}}^{-}\right\rangle. \end{aligned} \tag{6}$$

3.1.2. Decoding function

From Eq. (5) and Eq. (6), we can find that the final encoded states will be $\left|\Psi_{\mathrm{dL}}^{+}\right\rangle$ and $\left|\Psi_{\mathrm{dL}}^{-}\right\rangle$ after encoding the classical bit "0" and "1" on $\left|\Psi_{\mathrm{dL}}^{+}\right\rangle$, respectively. Consequently, if Alice performs the Bell measurement on the 1st and the 3rd qubits while Bob performs the corresponding Bell measurement on the 2nd and the 4th qubits in each encoded state, respectively, the encoded states will be transformed into the following decomposable forms as shown in Eq. (7) and Eq. (8).

For the encoded state carried classical bit "0",

$$\begin{aligned} U_0\left|\Psi_{\mathrm{dL}}^{+}\right\rangle &= \left|\Psi_{\mathrm{dL}}^{+}\right\rangle \\ &= \frac{1}{\sqrt{2}}(|01\rangle_{12}|10\rangle_{34}+|10\rangle_{12}|01\rangle_{34}) \\ &= \frac{1}{\sqrt{2}}(|01\rangle_{13}|10\rangle_{24}+|10\rangle_{13}|01\rangle_{24}) \\ &= \frac{1}{\sqrt{2}}(\left|\Psi^{+}\right\rangle_{13}\left|\Psi^{+}\right\rangle_{24}-\left|\Psi^{-}\right\rangle_{13}\left|\Psi^{-}\right\rangle_{24}). \end{aligned} \tag{7}$$

For the encoded state carried classical bit "1",

$$\begin{aligned} U_1\left|\Psi_{\mathrm{dL}}^{+}\right\rangle &= \left|\Psi_{\mathrm{dL}}^{-}\right\rangle \\ &= \frac{1}{\sqrt{2}}(|01\rangle_{12}|10\rangle_{34}-|10\rangle_{12}|01\rangle_{34}) \\ &= \frac{1}{\sqrt{2}}(|01\rangle_{13}|10\rangle_{24}-|10\rangle_{13}|01\rangle_{24}) \\ &= \frac{1}{\sqrt{2}}(\left|\Psi^{-}\right\rangle_{13}\left|\Psi^{+}\right\rangle_{24}-\left|\Psi^{+}\right\rangle_{13}\left|\Psi^{-}\right\rangle_{24}). \end{aligned} \tag{8}$$

Based on the joint correlations of the Bell measurement results, a decoding table can be constructed as shown in Table 1, which shows the correspondence of the unitary operation, Alice's Bell measurement result (ABMR) on the 1st and the 3rd qubits, Bob's Bell measurement result (BBMR) on the 2nd and the 4th qubits, and the transmitted secret message over the collective-dephasing noise channel in detail.

Table 1. The decoding table against collective-dephasing noise.

Unitary operation	ABMR	BBMR	Secret message
U_0	$\|\Psi^{+}\rangle_{13}$	$\|\Psi^{+}\rangle_{24}$	0
U_0	$\|\Psi^{-}\rangle_{13}$	$\|\Psi^{-}\rangle_{24}$	0
U_1	$\|\Psi^{-}\rangle_{13}$	$\|\Psi^{+}\rangle_{24}$	1
U_1	$\|\Psi^{+}\rangle_{13}$	$\|\Psi^{-}\rangle_{24}$	1

3.2. Coding function for logical Bell states immune to collective-rotation noise

This subsection introduces the coding function, i.e., encoding function and decoding function, against collective-rotation noise as follows.

3.2.1. Encoding function

Similar to Subsubsection 3.1.1, the encoding function can be constructed by performing the corresponding unitary operation on the 4th qubit in $\left|\Phi_{\mathrm{rL}}^{+}\right\rangle$ or $\left|\Psi_{\mathrm{rL}}^{-}\right\rangle$. Here, we take $\left|\Phi_{\mathrm{rL}}^{+}\right\rangle$ as the quantum information carrier, and define $U_0' = I = |0\rangle\langle 0| + |1\rangle\langle 1|$ and $U_1' = \mathrm{i}\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|$ as two unitary operations to encode a one-bit classical message "0" and "1", which is shown in Eq. (9) and Eq. (10), respectively.

$$\begin{aligned} U_0'\left|\Phi_{\mathrm{rL}}^{+}\right\rangle &= U_0'\frac{1}{2\sqrt{2}}(|0000\rangle+|0011\rangle+|1100\rangle+|1111\rangle \\ &\quad +|0101\rangle-|0110\rangle-|1001\rangle+|1010\rangle)_{1234} \\ &= \frac{1}{2\sqrt{2}}(|0000\rangle+|0011\rangle+|1100\rangle+|1111\rangle \\ &\quad +|0101\rangle-|0110\rangle-|1001\rangle+|1010\rangle)_{1234} \end{aligned}$$

$$= \left|\Phi_{\mathrm{rL}}^{+}\right\rangle, \tag{9}$$

$$\begin{aligned} U_1'\left|\Phi_{\mathrm{rL}}^{+}\right\rangle &= U_1'\frac{1}{2\sqrt{2}}(|0000\rangle+|0011\rangle+|1100\rangle+|1111\rangle \\ &\quad +|0101\rangle-|0110\rangle-|1001\rangle+|1010\rangle)_{1234} \\ &= \frac{1}{2\sqrt{2}}(|0001\rangle-|0010\rangle+|1101\rangle-|1110\rangle \\ &\quad -|0100\rangle-|0111\rangle+|1000\rangle+|1011\rangle)_{1234} \\ &= \left|\Psi_{\mathrm{rL}}^{-}\right\rangle. \end{aligned} \tag{10}$$

3.2.2. Decoding function

Similar to Subsubsection 3.1.2, if the corresponding Bell measurements are performed on the 1st and the 3rd qubits, and the 2nd and the 4th qubits in $\left|\Phi_{\mathrm{rL}}^{+}\right\rangle$ or $\left|\Psi_{\mathrm{rL}}^{-}\right\rangle$, respectively, the encoded states will be transformed into the following decomposable forms as shown in Eq. (11) and Eq. (12), respectively.

$$\begin{aligned} U_0'\left|\Phi_{\mathrm{rL}}^{+}\right\rangle &= \left|\Phi_{\mathrm{rL}}^{+}\right\rangle \\ &= \frac{1}{2\sqrt{2}}(|0000\rangle+|0011\rangle+|1100\rangle+|1111\rangle \\ &\quad +|0101\rangle-|0110\rangle-|1001\rangle+|1010\rangle)_{1234} \\ &= \frac{1}{\sqrt{2}}(\left|\Phi^{+}\right\rangle_{13}\left|\Phi^{+}\right\rangle_{24}+\left|\Psi^{-}\right\rangle_{13}\left|\Psi^{-}\right\rangle_{24}), \end{aligned} \tag{11}$$

$$\begin{aligned} U_1'\left|\Phi_{\mathrm{rL}}^{+}\right\rangle &= \left|\Psi_{\mathrm{rL}}^{-}\right\rangle \\ &= \frac{1}{2\sqrt{2}}(|0001\rangle-|0010\rangle+|1101\rangle-|1110\rangle \\ &\quad -|0100\rangle-|0111\rangle+|1000\rangle+|1011\rangle)_{1234} \\ &= \frac{1}{\sqrt{2}}(\left|\Phi^{+}\right\rangle_{13}\left|\Psi^{-}\right\rangle_{24}-\left|\Psi^{-}\right\rangle_{13}\left|\Phi^{+}\right\rangle_{24}). \end{aligned} \tag{12}$$

Correspondingly, the decoding table of the logical Bell states immune to collective-rotation noise can be constructed as the following Table 2.

Table 2. The decoding table against collective-rotation noise.

Unitary operation	AMR	BMR	Secret message
U_0'	$\|\Phi^{+}\rangle_{13}$	$\|\Phi^{+}\rangle_{24}$	0
U_0'	$\|\Psi^{-}\rangle_{13}$	$\|\Psi^{-}\rangle_{24}$	0
U_1'	$\|\Phi^{+}\rangle_{13}$	$\|\Psi^{-}\rangle_{24}$	1
U_1'	$\|\Psi^{-}\rangle_{13}$	$\|\Phi^{+}\rangle_{24}$	1

4. Proposed DSQC schemes against collective noise

In this section, two DSQC schemes are presented. The DSQC scheme against collective-dephasing noise is constructed in Subsection 4.1, and the DSQC scheme against collective-rotation noise is constructed in Subsection 4.2.

4.1. DSQC scheme against collective-dephasing noise

In the proposed DSQC scheme, the two legitimate users are supposed to be the sender Alice and the receiver Bob, and n classical bits of secret message to be communicated between them are denoted with a sequence

$$M_n = \{m_1, m_2, \ldots, m_i, \ldots, m_n\},$$

where $m_i \in \{0,1\}$ with $i = 1,2,\ldots,n$. The main process of the DSQC scheme against collective-dephasing noise is demonstrated in the following steps.

Step 1 Initializing phase

Alice prepares n ordered logical Bell states all in $\left|\Psi_{\mathrm{dL}}^{+}\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle|10\rangle+|10\rangle|01\rangle)_{1234}$. Then, she elicits all the 1st and the 3rd particles from each logical Bell state to form the sequence $S_{\mathrm{H}} = \{S_{\mathrm{H}}^{1}(i), S_{\mathrm{H}}^{3}(i)\}$. All the 2nd and the 4th particles of each logical Bell state are formed another sequence $S_{\mathrm{T}} = \{S_{\mathrm{T}}^{2}(i), S_{\mathrm{T}}^{4}(i)\}$. Here, the superscripts represent the selected qubits, the subscripts "H" and "T" represent the home qubits and the travel qubits respectively, for $i = 1,2,\ldots,n$. In addition, Alice also prepares l ($l \ll n$) logical qubits $\{|0_{\mathrm{dL}}\rangle, |1_{\mathrm{dL}}\rangle, |+_{\mathrm{dL}}\rangle, |-_{\mathrm{dL}}\rangle\}$ as decoy logical qubits.

Step 2 Encoding phase

Alice encodes the secret message M_n to be communicated with Bob. That is, if the secret message m_i is "0" (or "1"), then Alice performs the unitary operation $U_0 = I = |0\rangle\langle 0| + |1\rangle\langle 1|$ (or $U_1 = \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$) on the 4th qubit in $\left|\Psi_{\mathrm{dL}}^{+}\right\rangle$. Consequently, $\left|\Psi_{\mathrm{dL}}^{+}\right\rangle$ is transformed into $\left|\Psi_{\mathrm{dL}}^{+}\right\rangle$ (or $\left|\Psi_{\mathrm{dL}}^{-}\right\rangle$), and the sequence S_{T} is simultaneously updated into the new sequence $S_{\mathrm{T}'}$, denoted with $S_{\mathrm{T}'} = \{S_{\mathrm{T}'}^{2}(i), S_{\mathrm{T}'}^{4}(i)\}$. For instance, provided that the secret message to be delivered is $M_4 = \{0110\}$, then Alice will perform U_0, U_1, U_1, and U_0 on the corresponding particles $S_{\mathrm{T}}^{4}(1)$, $S_{\mathrm{T}}^{4}(2)$, $S_{\mathrm{T}}^{4}(3)$, and $S_{\mathrm{T}}^{4}(4)$ in order, and the initial logical Bell states will be transformed into $\left|\Psi_{\mathrm{dL}}^{+}\right\rangle$, $\left|\Psi_{\mathrm{dL}}^{-}\right\rangle$, $\left|\Psi_{\mathrm{dL}}^{-}\right\rangle$, and $\left|\Psi_{\mathrm{dL}}^{+}\right\rangle$ correspondingly.

Step 3 Eavesdropping check phase

Alice randomly inserts the prepared l decoy logical qubits into $S_{\mathrm{T}'}$ to get S_{T^*} and send it to Bob via the quantum channel. Note that the transmitted states in the sequence $S_{\mathrm{T}'} = \{S_{\mathrm{T}'}^{2}(i), S_{\mathrm{T}'}^{4}(i)\}$ are constructed from $|0_{\mathrm{dL}}\rangle$ and $|1_{\mathrm{dL}}\rangle$, so they are also resistant to the collective-dephasing noise. After confirming that Bob has received S_{T^*} successfully, Alice informs him of the positions and the measurement bases of the decoy logical qubits for the eavesdropping check. Afterwards, Bob measures the corresponding check sets and regains the sequence $S_{\mathrm{T}'}$, then tells Alice his measurement results. Alice can analyze whether there is an eavesdropper or not in the quantum channel. That is, if the detected error rate exceeds a predetermined threshold τ ($\tau \approx 2\% \sim 8.9\%$) depending on the channel situation (e.g., attenuation, etc.),[61,62] Alice aborts the communication and restarts a new one. Otherwise, the scheme continues to the next step.

Step 4 Decoding phase

According to Eq. (7) and Eq. (8), Alice performs the Bell measurement on the particles in the sequence $S_{\mathrm{H}} = \{S_{\mathrm{H}}^{1}(i), S_{\mathrm{H}}^{3}(i)\}$ and sends the measurement results to Bob. Concretely, if the measurement result is $|\Psi^{+}\rangle$ (or $|\Psi^{-}\rangle$), Alice sends the classical bit "0" (or "1") to Bob via the authorized classical channel. Meanwhile, Bob also performs

the Bell measurement on the corresponding particles in the sequence $S_{T'} = \{S^2_{T'}(i), S^4_{T'}(i)\}$. Once Bob receives the exchanged information of classical bits from Alice, he can confirm the transmitted secret message successfully according to the decoding Table 1. For example, if the received classical bits are "0101" and the Bell measurement outcomes on the corresponding particles in $S_{T'}$ are $\{|\Psi^+\rangle, |\Psi^+\rangle, |\Psi^-\rangle, |\Psi^-\rangle\}$, Bob can first infer Alice's measurement results that are $\{|\Psi^+\rangle, |\Psi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$, and then further deduce the delivered secret message is $M_4 = \{0110\}$.

4.2. DSQC scheme against collective-rotation noise

Alternatively, the process of the DSQC scheme against collective-rotation noise is similar to the DSQC scheme against collective-dephasing noise. There are a few differences listed as follows.

In the initial phase, Alice prepares the logical Bell state $|\Phi^+_{rL}\rangle$ instead of $|\Psi^+_{dL}\rangle$, and also prepares the decoy logical qubits randomly from $\{|0_{rL}\rangle, |1_{rL}\rangle, |+_{rL}\rangle, |-_{rL}\rangle\}$ instead of $\{|0_{dL}\rangle, |1_{dL}\rangle, |+_{dL}\rangle, |-_{dL}\rangle\}$ as in Step 1 of the aforementioned scheme. In the encoding phase, i.e., Step 2, Alice takes $U'_0 = I = |0\rangle\langle 0| + |1\rangle\langle 1|$ and $U'_1 = i\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|$ instead as two unitary operations to encode a one-bit classical message "0" and "1", which is introduced in Subsubsection 3.2.1. Then, in the decoding phase, Bob can decode the secret message using the decoding Table 2. Consequently, this proposed DSQC scheme can also work well over the collective-rotation noise channel.

5. Security analysis

In this section, the security of the proposed scheme is further discussed including the security against an information leakage problem, an intercept-resend attack, an entangle-measure attack, a correlation–elicitation attack, and a Trojan horse attack. It should be noted that only the security analysis of the proposed scheme over the collective-dephasing noise channel is given in detail, which is suitable for the proposed scheme over the collective-rotation noise channel.

5.1. Security against information leakage attack

Information leakage is a common problem, that is, the malicious eavesdropper, Eve, can deduce partial or entire secret messages only by analyzing the transmitted qubits or classical bits between the sender Alice and the receiver Bob. For the proposed DSQC scheme against the collective-dephasing noise, the information leakage problem may occur in two cases.

The first case is that Eve intercepts the transmitted qubits, and measures them to extract the carried useful information. This case occurs before the eavesdropping check phase, so Eve may steal the secret message successfully without being detected. If so, even though the attack action is discovered by the subsequent eavesdropping check, it will be too late. However, this case cannot work well in the proposed DSQC scheme. As we know, after the unitary operation $U_0 = I = |0\rangle\langle 0| + |1\rangle\langle 1|$ (or $U_1 = \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$) is performed, a one-bit secret message "0" (or "1") is encoded on the corresponding qubits $\{S^2_{T'}(i), S^4_{T'}(i)\}$ in $S_{T'}$. However, at this point, Eve has no knowledge of Alice's measurement outcomes which will be published only after the eavesdropping check phase, and thus she cannot obtain any secret message. Concretely, if Eve's measurement result is $|\Psi^+\rangle$, the decoding combination may be $(|\Psi^+\rangle, |\Psi^+\rangle$, "0") or $(|\Psi^-\rangle, |\Psi^+\rangle$, "1") with the same possibility. Similarly, if the measurement result is $|\Psi^-\rangle$, the decoding combination may be $(|\Psi^-\rangle, |\Psi^-\rangle$, "0") or $(|\Psi^+\rangle, |\Psi^-\rangle$, "1"). In essence, according to Shannon's information theory,[63] the uncertainty for Eve is that $H = \sum -p_i \log_2 {}^{p_i} = -2 \times \frac{1}{2} \log_2 {}^{1/2} = 1$ bit. Therefore, Eve cannot deduce any secret message in this situation.

The second case is that Eve can wiretap the exchanged classical information in the decoding phase to attempt to distill Alice's secret message. Generally, this case always takes place after the eavesdropping check phase, so Eve will not be detected as long as she obtains the transmitted secret message in this situation. However, Eve also has no chance to achieve this aim in the proposed DSQC scheme. When Eve captures the exchanged classical bit "0" (or "1"), she can easily infer Alice's measurement result on the corresponding qubits $\{S^1_H(i), S^3_H(i)\}$ in S_H is $|\Psi^+\rangle$ (or $|\Psi^-\rangle$). Obviously, only depending on this result, she cannot reveal any secret message since she cannot determine Bob's measurement results on the corresponding qubits $\{S^2_{T'}(i), S^4_{T'}(i)\}$. Hence, according to Shannon's information theory she cannot further deduce the correct decoding combination to obtain Alice's secret message.

5.2. Security against intercept-resend attack

The intercept-resend attack always works well on many quantum secure communication schemes.[64–66] Suppose the intercept-resend attack is carried out on the proposed DSQC scheme. In the eavesdropping check phase, Alice randomly inserts l decoy logical qubits from $\{|0_{dL}\rangle, |1_{dL}\rangle, |+_{dL}\rangle, |-_{dL}\rangle\}$ into $S_{T'}$ to guarantee the security of the quantum channel between Alice and Bob. Similar to the famous BB84 protocol, the probability for the eavesdropper to pass the public discussion for one decoy logical qubit is $3/4$ without knowing the corresponding information of the position and the measurement basis in advance. Accordingly, the probability of avoiding the eavesdropping check successfully for the eavesdropper for all l decoy logical qubits is $(3/4)^l$, which will converge to zero as l is large enough. Therefore, suppose a potential eaves-

dropper, Eve, intercepted the sequence S_{T^*} to measure it, and then resent a forged sequence to Bob, she would be detected inevitably in this step.

5.3. Security against entangle-measure attack

The entangle-measure attack[69,70] should be considered in the presented DSQC scheme. In this attack, the eavesdropper prepares some specific particles in advance and entangles them with the sent sequence. By measuring these particles, the eavesdropper may obtain the information about the encoding operations and further deduce the secret message. Suppose that Eve prepares $n+l$ auxiliary logical qubits, $P_{dL} = \{|P_{dL}(i)\rangle\}$ for $i = 1,2,\ldots,n+l$. According to Stinespring dilation theorem, Eve can entangle $|P_{dL}(i)\rangle$ with the corresponding qubits $|S_{T^*}(i)\rangle$ by a unitary operation $\hat{E}$ on a larger Hilbert space when Alice sends S_{T^*} to Bob in Step 3, that is, $\hat{E}|S_{T^*}(i), P_{dL}(i)\rangle = \hat{E}|S_{T^*}(i)\rangle|P_{dL}(i)\rangle$. However, since the quantum states of the decoy logical qubits are unknown to Eve, there will be four possible outcomes after performing the unitary operations on each decoy logical qubits as follows:

$$\hat{E}|0_{dL}, P_{dL}(i)\rangle = \alpha|0_{dL}\rangle|E_{00}\rangle + \beta|1_{dL}\rangle|E_{01}\rangle, \quad (13)$$

$$\hat{E}|1_{dL}, P_{dL}(i)\rangle = \alpha'|0_{dL}\rangle|E_{10}\rangle + \beta'|1_{dL}\rangle|E_{11}\rangle, \quad (14)$$

$$\begin{aligned}\hat{E}|+_{dL}, P_{dL}(i)\rangle = \frac{1}{2}[&|+_{dL}\rangle(\alpha|E_{00}\rangle + \beta|E_{01}\rangle \\ &+ \alpha'|E_{10}\rangle + \beta'|E_{11}\rangle) \\ &+ |-_{dL}\rangle(\alpha|E_{00}\rangle - \beta|E_{01}\rangle \\ &+ \alpha'|E_{10}\rangle - \beta'|E_{11}\rangle)], \end{aligned} \quad (15)$$

$$\begin{aligned}\hat{E}|-_{dL}, P_{dL}(i)\rangle = \frac{1}{2}[&|+_{dL}\rangle(\alpha|E_{00}\rangle + \beta|E_{01}\rangle \\ &- \alpha'|E_{10}\rangle - \beta'|E_{11}\rangle) \\ &+ |-_{dL}\rangle(\alpha|E_{00}\rangle - \beta|E_{01}\rangle \\ &- \alpha'|E_{10}\rangle + \beta'|E_{11}\rangle)]. \end{aligned} \quad (16)$$

Here, since $\hat{E}$ is a unitary operation, the complex number α, β and α', β' must satisfy

$$|\alpha|^2 + |\beta|^2 = 1, \quad |\alpha'|^2 + |\beta'|^2 = 1. \quad (17)$$

Hence, if Eve wants to pass the eavesdropping check and derives the useful information from the encoding operations, the following relationships should be established. Here, $|E_{00}\rangle$, $|E_{01}\rangle$, $|E_{10}\rangle$, and $|E_{11}\rangle$ are four quantum states which can be distinguished by Eve.

i) From Eq. (13), the complex number β should satisfy $\beta = 0$ when the decoy logical qubits is $|0_{dL}\rangle$.

ii) From Eq. (14), the complex number α' should satisfy $\alpha' = 0$ when the decoy logical qubits is $|1_{dL}\rangle$.

iii) From Eq. (15), the mathematical relation $\alpha|E_{00}\rangle - \beta|E_{01}\rangle + \alpha'|E_{10}\rangle - \beta'|E_{11}\rangle = 0$ should hold when the decoy logical qubits is $|+_{dL}\rangle$, where $\mathbf{0}$ is represented as a zero vector.

iv) From Eq. (16), the mathematical relation $\alpha|E_{00}\rangle + \beta|E_{01}\rangle - \alpha'|E_{10}\rangle - \beta'|E_{11}\rangle = 0$ should hold when the decoy logical qubits is $|-_{dL}\rangle$, where $\mathbf{0}$ is represented as a zero vector.

Therefore, only when the four relationships above are all satisfied synchronously, can Eve's attack not be detected during the public discussion of the eavesdropping check. Consequently, the equation that $\alpha|E_{00}\rangle - \beta'|E_{11}\rangle = 0$ is established as the equation that $\beta = \alpha' = 0$ holds, which indicates that $\alpha|E_{00}\rangle = \beta'|E_{11}\rangle$. That is, Eve cannot distinguish $|E_{00}\rangle$ from $|E_{11}\rangle$, which is contradictory to the precondition. Conversely, if Eve tries to make them distinguishable, i.e., $\alpha|E_{00}\rangle \neq \beta'|E_{11}\rangle$, to obtain some useful information, the decoy logical qubits will be inevitably disturbed, and Eve will be certainly detected. Therefore, Eve will not obtain any secret message if she launches the entangle-measure attack on the proposed DSQC scheme.

5.4. Security against correlation-elicitation attack

In the correlation–elicitation (CE) attack,[69,70] the eavesdropper can distill part or all of the secret message by utilizing the relationship between two different qubits at different times. Performing CNOT operations on the particles introduced by an eavesdropper and the particles transmitted between the legitimate users is the usual means to implement this attack. Suppose that Eve performs the CE attack on the proposed DSQC scheme. As we know, the attack will be successful if Eve can deduce Bob's Bell measurement results on $S_{T'} = \{S^2_{T'}(i), S^4_{T'}(i)\}$ by measuring his own introduced particles without being detected. For that, Eve may prepare a quantum sequence, say, S_{E^*} composed of $n+l$ quantum states $|E\rangle$.

Herein, to illustrate this attack explicitly, we take $|E\rangle = |00\rangle$ as an example. In fact, the following analysis is analogical whenever the quantum state $|E\rangle$ is a single particle polarization state or a multi-particle entangled state. Then, in Step iii), Eve intercepts the sequence S_{T^*} and perform the CNOT operations, in which the particles in S_{T^*} are the control qubits while the corresponding particles in S_{E^*} are the target qubits, to generate the six-qubits entangled states. Subsequently, she resends the sequence S_{T^*} to Bob as usual, while keeping S_{E^*} in her quantum register. Once she gets the information about the position and measurement basis of the decoy logical qubits in Step iii), Eve immediately performs the corresponding Bell measurements on the particles in S_{E^*} to deduce Bob's measurement outcomes according to the joint correlations of the Bell measurement results in the six-particle entangled states. Then, she further wiretaps Alice's Bell measurement results to attempt to reveal the secret message in Step iv). Even so, the CE attack also will be detected eventually, since the decoy logical states $|0_{dL}\rangle$, $|1_{dL}\rangle$, $|+_{dL}\rangle$, and $|-_{dL}\rangle$ will be transformed into the corresponding quantum states after the CNOT opera-

tions, respectively.

$$\begin{aligned}
&\mathrm{CNOT}_{\mathrm{D_1}\to\mathrm{E_1},\mathrm{D_2}\to\mathrm{E_2}}(|0_{\mathrm{dL}}\rangle\otimes|E\rangle)\\
&=\mathrm{CNOT}_{\mathrm{D_1}\to\mathrm{E_1},\mathrm{D_2}\to\mathrm{E_2}}(|01\rangle_{\mathrm{D_1D_2}}\otimes|00\rangle_{\mathrm{E_1E_2}})\\
&=|01\rangle_{\mathrm{D_1D_2}}|01\rangle_{\mathrm{E_1E_2}}=|0_{\mathrm{dL}}\rangle|0_{\mathrm{dL}}\rangle, \qquad (18)\\
&\mathrm{CNOT}_{\mathrm{D_1}\to\mathrm{E_1},\mathrm{D_2}\to\mathrm{E_2}}(|1_{\mathrm{dL}}\rangle\otimes|E\rangle)\\
&=\mathrm{CNOT}_{\mathrm{D_1}\to\mathrm{E_1},\mathrm{D_2}\to\mathrm{E_2}}(|10\rangle_{\mathrm{D_1D_2}}\otimes|00\rangle_{\mathrm{E_1E_2}})\\
&=|10\rangle_{\mathrm{D_1D_2}}|10\rangle_{\mathrm{E_1E_2}}=|1_{\mathrm{dL}}\rangle|1_{\mathrm{dL}}\rangle, \qquad (19)\\
&\mathrm{CNOT}_{\mathrm{D_1}\to\mathrm{E_1},\mathrm{D_2}\to\mathrm{E_2}}(|+_{\mathrm{dL}}\rangle\otimes|E\rangle)\\
&=\mathrm{CNOT}_{\mathrm{D_1}\to\mathrm{E_1},\mathrm{D_2}\to\mathrm{E_2}}\left[\frac{1}{\sqrt{2}}(|01\rangle+|10\rangle)_{\mathrm{D_1D_2}}\otimes|00\rangle_{\mathrm{E_1E_2}}\right]\\
&=\frac{1}{\sqrt{2}}(|01\rangle_{\mathrm{D_1D_2}}|01\rangle_{\mathrm{E_1E_2}}+|10\rangle_{\mathrm{D_1D_2}}|10\rangle_{\mathrm{E_1E_2}})\\
&=\frac{1}{\sqrt{2}}(|+_{\mathrm{dL}}\rangle|+_{\mathrm{dL}}\rangle+|-_{\mathrm{dL}}\rangle|-_{\mathrm{dL}}\rangle), \qquad (20)\\
&\mathrm{CNOT}_{\mathrm{D_1}\to\mathrm{E_1},\mathrm{D_2}\to\mathrm{E_2}}(|-_{\mathrm{dL}}\rangle\otimes|E\rangle)\\
&=\mathrm{CNOT}_{\mathrm{D_1}\to\mathrm{E_1},\mathrm{D_2}\to\mathrm{E_2}}\left[\frac{1}{\sqrt{2}}(|01\rangle-|10\rangle)_{\mathrm{D_1D_2}}\otimes|00\rangle_{\mathrm{E_1E_2}}\right]\\
&=\frac{1}{\sqrt{2}}(|01\rangle_{\mathrm{D_1D_2}}|01\rangle_{\mathrm{E_1E_2}}-|10\rangle_{\mathrm{D_1D_2}}|10\rangle_{\mathrm{E_1E_2}})\\
&=\frac{1}{\sqrt{2}}(|+_{\mathrm{dL}}\rangle|-_{\mathrm{dL}}\rangle+|-_{\mathrm{dL}}\rangle|+_{\mathrm{dL}}\rangle). \qquad (21)
\end{aligned}$$

Here, the qubits denoted with the subscripts "$\mathrm{D_1}$" and "$\mathrm{D_2}$", are the control qubits in decoy logical states, and the corresponding qubits denoted with the subscripts "$\mathrm{E_1}$" and "$\mathrm{E_2}$", are the target qubits in S_{E^*}. Obviously, according to Eq. (18) and Eq. (19), Eve can avoid the eavesdropping check successfully when the decoy logical is $|0_{\mathrm{dL}}\rangle$ or $|1_{\mathrm{dL}}\rangle$. However, she will be detected with the probability of $1/2$ when the decoy particle is $|+_{\mathrm{dL}}\rangle$ or $|-_{\mathrm{dL}}\rangle$ according to Eq. (20) and Eq. (21). So, the total probability of being detected by the eavesdropping check is $1-(3/4)^l$ for l decoy logical qubit, which approaches to 100% as l is large enough. Therefore, the proposed DSQC scheme is security against the CE attack.

5.5. Security against Trojan horse attack

Plenty of quantum secure communication protocols easily suffer from Trojan horse attacks, i.e., the invisible photon eavesdropping (IPE) attack and the delay-photon attack.[71,72] In an IPE attack, the eavesdropper produces an invisible spy photon sequence whose wavelength is close to the legitimate one, and adds it to the sent sequence. In a delay-photon attack, the eavesdropper inserts a spy photon sequence into a legitimate signal with a delay time, shorter than the time windows. The attacker can capture these spy photons and deduce the secret message by performing an appropriate measurement.

In the proposed DSQC scheme, Eve may try to get the secret message by carrying out the IPE attack. That is, she produces a special photon sequence $S_{\mathrm{E}*}$ composed of $n+l$ Bell states from $\{|\Phi^+\rangle,|\Phi^-\rangle,|\Psi^+\rangle,|\Psi^-\rangle\}$ with the wavelength $\lambda'\approx\lambda$, where λ is the legitimate wavelength. Then, in Step iii), she inserts $S_{\mathrm{E}*}$ into the transmitted sequence $S_{\mathrm{T}*}$ and forwards them to Bob. Generally speaking, only when the legitimate sequence is transmitted at least twice, may the eavesdropper have the opportunity to deduce the secret message by analyzing the measurement results of the spy photon sequence. However, in the proposed DSQC scheme, the sequence S_{T^*} is only transmitted one way, i.e., from Alice to Bob, so that Eve has no chance to filter out the inserted invisible photons and measure them to steal the secret message. Moreover, the unitary operations have been performed by Alice before the spy photon sequence is inserted, and Bob only performs the corresponding measurement without any unitary operations for decoding the secret message. Therefore, the eavesdropper Eve still cannot reveal the secret message even though she captures the spy photon sequence. Similarly, when the delay-photon attack is carried out, Eve also cannot obtain any useful secret information. Therefore, Trojan horse attacks can be congenitally avoided without introducing extra hardware devices, such as the wavelength filter and photon number splitter (PNS).

6. Conclusions

To summarize, our paper proposes two DSQC schemes using logical Bell states, which are resistant to one kind of collective noise: the collective-dephasing noise and the collective-rotation noise, respectively. Compared with other DSQC schemes,[56–59] our proposed scheme has two merits. The first one is that the logical Bell states (i.e., the four-particle decoherence-free states) are exploited to design the DSQC scheme for the first time. In order to implement the transmission of the secret message, two novel coding functions are constructed by advantage of the property of the logical Bell states. Based on the new coding functions, the sender, Alice, can encode her secret message by two simple unitary operations and the receiver, Bob, can read out the secret message by merely using the Bell measurements after the additional classical information is exchanged. For simplicity, we demonstrate the process of the proposed DSQC scheme over the collective-dephasing noise channel in detail against over collective noise. The second one is that the technique of decoy logical qubits checking and the strategy of one-step quanta transmission are combined together in our DSQC scheme. This combination not only ensures the security of the communication between two legitimate users, but also effectively reduces the influence of other noise existing in the quantum channel. The final security analysis shows that both the proposed DSQC schemes are feasible and robust against the information leakage attack, the intercept-resend attack, the entangle-measure attack, the correlation–elicitation attack, and the Trojan horse attack over the collective noise channel.

References

[1] Bennett C H and Brassard G 1984 *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (Bangalore, India) p. 175
[2] Wang X B 2004 *Phys. Rev. Lett.* **92** 077902
[3] Xiong Z X 2012 *Phys. Rev. A* **85** 012334
[4] Zhu C H, Pei C X, Quan D X, Gao J L, Chen N and Yi Y H 2010 *Chin. Phys. Lett.* **27** 090301
[5] Chen M J and Liu X 2011 *Chin. Phys. B* **20** 100305
[6] Hwang T, Hwang C C and Tsai C W 2011 *Eur. Phys. J. D* **61** 785
[7] Chen D, Zhao S H and Zhao W H 2014 *Acta Phys. Sin.* **63** 030302 (in Chinese)
[8] Tian P G, Zhou Y Y and Zhang H Q 2013 *Acta Phys. Sin.* **62** 200302 (in Chinese)
[9] Long G L and Liu X S 2002 *Phys. Rev. A* **65** 032302
[10] Deng F G, Long G L and Liu X S 2003 *Phys. Rev. A* **68** 042317
[11] Zhu A D, Xia Y, Fan Q B and Zhang S 2006 *Phys. Rev. A* **73** 022338
[12] Wang L Y, Chen X B, Xu G and Yang Y X 2011 *Opt. Commun.* **284** 1719
[13] Gu B, Huang Y G, Fang X and Zhang C Y 2011 *Chin. Phys. B* **20** 100309
[14] Lin S, Gao F and Liu X F 2011 *Chin. Phys. Lett.* **28** 030302
[15] Li C Y, Li X H, Deng F G and Zhou H Y 2008 *Chin. Phys. B* **17** 2352
[16] Deng F G and Long G L 2004 *Phys. Rev. A* **71** 052319
[17] Wang C, Deng F G, Li Y S, Liu X S and Long G L 2005 *Phys. Rev. A* **71** 044305
[18] Yan L L, Chang Y and Zhang S B 2013 *Chin. Phys. Lett.* **30** 090301
[19] Kao S H and Hwang T 2013 *Chin. Phys. B* **22** 060308
[20] Shimizu K and Imoto N 1999 *Phys. Rev. A* **60** 157
[21] Beige A, Englert B G and Kurtsiefer C 2002 *Acta Phys. Pol. A* **101** 357
[22] Lucamarini M and Mancini S 2005 *Phys. Rev. Lett.* **94** 140501
[23] Yuan H, Song J and Liu X Y 2011 *Int. J. Quantum Inf.* **67** 607
[24] Shukla C, Banerjee A and Pathak A 2012 *Int. J. Theor. Phys.* **67** 661
[25] Tsai C W, Hsieh C R and Hwang T 2011 *Eur. Phys. J. D* **61** 779
[26] Kao S H, Tsai C W and Hwang T 2012 *Int. J. Theor. Phys.* **51** 3868
[27] Man Z X, Zhang Z J and Li Y 2005 *Chin. Phys. Lett.* **22** 18
[28] Wang G Y, Fang X M and Tan X H 2006 *Chin. Phys. Lett.* **23** 2658
[29] Liu W J, Chen H W and Ma T H 2009 *Chin. Phys. B* **18** 4105
[30] Li D and Xiu X M 2010 *Acta Phys. Pol. B* **41** 1203
[31] Li X H, Deng F G and Zhou H Y 2008 *Phys. Rev. A* **78** 022321
[32] Boileau J C, Gottesman D, Laflamme R, Poulin D and Spekkens R W 2004 *Phys. Rev. Lett.* **92** 017901
[33] Sun Y, Wen Q Y, Gao F and Zhu F C 2009 *Phys. Rev. A* **80** 032321
[34] Li J, Jin H F and Jin B 2012 *Chin. Sci. Bull.* **57** 4434
[35] Ren B C, Wei H R, Hua M, Li T and Deng F G 2013 *Eur. Phys. J. D* **67** 30
[36] Nielsen M A and Chung I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)
[37] Li X H, Deng F G and Zhou H Y 2007 *Appl. Phys. Lett.* **91** 144101
[38] Walton Z D, Abouraddy A F, Sergienko A V, Saleh B E A and Teich M C 2003 *Phys. Rev. Lett.* **91** 087901
[39] Wang X B 2005 *Phys. Rev. A* **72** 050304
[40] Huang W, Guo F Z, Huang Z, Wen Q Y and Zhu F C 2011 *Opt. Commun.* **284** 536
[41] Yang C W and Hwang T 2013 *Quantum Inf. Process.* **12** 3207
[42] Xiu M M, Dong L, Gao Y J and Chi F 2009 *Opt. Commun.* **282** 4171
[43] Li X H, Zhao B K, Sheng Y B, Deng F G and Zhou H Y 2009 *Int. J. Quantum Inf.* **7** 1479
[44] Li C Y and Li Y S 2010 *Int. J. Quantum Inf.* **8** 1101
[45] Gu B, Zhang C Y, Cheng G S and Huang Y G 2011 *Sci. China Ser. G* **54** 942
[46] Yang C W, Tsai C W and Hwang T 2011 *Sci. China Ser. G* **54** 496
[47] Yang C W and Hwang T 2013 *Quantum Inf. Process.* **12** 3495
[48] Yang C W and Hwang T 2012 *Int. J. Theor. Phys.* **51** 3941
[49] Huang W, Wen Q Y, Jia H Y, Qin S J and Gao F 2012 *Chin. Phys. B* **21** 100308
[50] Yang J, Wang C and Zhang R 2010 *Chin. Phys. B* **19** 110306
[51] Yang Y G, Chai H P, Wang Y, Teng Y W and Wen Q Y 2011 *Sci. China Ser. G* **54** 1619
[52] Yang Y G, Teng Y W, Chai H P and Wen Q Y 2011 *Phys. Scr.* **83** 025003
[53] Li C Y and Li Y S 2011 *Chin. Phys. Lett.* **28** 020304
[54] Sun Y, Wen Q Y and Zhu F C 2010 *Opt. Commun.* **283** 181
[55] Gu B, Mu L L, Ding L G, Zhang C Y and Li C Q 2010 *Opt. Commun.* **283** 3099
[56] Dong L, Xiu X M, Gao Y J and Chi F 2009 *Opt. Commun.* **282** 1688
[57] Gu B, Pei S X, Song B and Zhong K 2009 *Sci. China Ser. G* **52** 1913
[58] Yang C W, Tsai C W and Hwang T 2013 *Quantum Inf. Process.* **12** 3043
[59] Yuan H, Zhang Q, Hong L, Yin W J and Xu D 2014 *Int. J. Theor. Phys.*
[60] Bourennane M, Eibl M, Gaertner S, Kurtsiefer C, Cabello A and Weinfurter H 2004 *Phys. Rev. Lett.* **92** 107901
[61] Beveratos A, Brouri R, Gacoin T, Villing A, Poizat J P and Grangier P 2002 *Phys. Rev. Lett.* **89** 187901
[62] Gobby C, Yuan Z L and Shields A J 2004 *Appl. Phys. Lett.* **84** 3762
[63] Shannon C E 1949 *Bell Syst. Tech. J.* **28** 656
[64] Yang C W, Tsai C W and Hwang T 2012 *Quantum Inf. Process.* **11** 113
[65] Yang S, Chen X B and Yang Y X 2012 *Commun. Theor. Phys.* **58** 51
[66] Wang T Y and Wen Q Y 2011 *Opt. Commun.* **284** 3664
[67] Chen X B, Yang S, Su Y and Yang Y X 2012 *Phys. Scr.* **86** 055002
[68] Wang M M, Chen X B and Yang Y X 2013 *Quantum Inf. Process.* **12** 785
[69] Gao F, Wen Q Y and Zhu F C 2007 *Phys. Lett. A* **360** 748
[70] Wang T Y, Wen Q Y and Chen X B 2010 *Opt. Commun.* **283** 5261
[71] Cai Q Y 2006 *Phys. Lett. A* **351** 23
[72] Li X H, Deng F G and Zhou H Y 2006 *Phys. Rev. A* **74** 054302