ISSN 1674-1056
http://cpb.iphy.ac.cn
http://iopscience.iop.org/cpb
中国物理 B
Chinese Physics
中国物理 Chinese Physics B

Fault tolerant controlled quantum dialogue against collective noise

Li-Wei Chang(常利伟)[1,2], Yu-Qing Zhang(张宇青)[1], Xiao-Xiong Tian(田晓雄)[1], Yu-Hua Qian(钱宇华)[2], Shi-Hui Zheng(郑世慧)[3]

Citation: Chin. Phys. B . 2020, 29(1): 010304 . **doi:** 10.1088/1674-1056/ab5786
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Quantum discord of two-qutrit system under quantum-jump-based feedback control

Chang Wang(王畅), Mao-Fa Fang(方卯发)
Chin. Phys. B . 2019, 28(12): 120302 . **doi:** 10.1088/1674-1056/ab4e83

Faithful deterministic secure quantum communication and authentication protocol based on hyperentanglement against collective noise

Chang Yan, Zhang Shi-Bin, Yan Li-Li, Han Gui-Hua
Chin. Phys. B . 2015, 24(8): 080306 . **doi:** 10.1088/1674-1056/24/8/080306

Multi-user quantum key distribution with collective eavesdropping detection over collective-noise channels

Huang Wei, Wen Qiao-Yan, Liu Bin, Gao Fei
Chin. Phys. B . 2015, 24(7): 070308 . **doi:** 10.1088/1674-1056/24/7/070308

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

Wang Chao, Liu Jian-Wei, Chen Xiu-Bo, Bi Ya-Gang, Shang Tao
Chin. Phys. B . 2015, 24(4): 040304 . **doi:** 10.1088/1674-1056/24/4/040304

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

Huang Wei, Wen Qiao-Yan, Jia Heng-Yue, Qin Su-Juan, Gao Fei
Chin. Phys. B . 2012, 21(10): 100308 . **doi:** 10.1088/1674-1056/21/10/100308

Fault tolerant controlled quantum dialogue against collective noise*

Li-Wei Chang(常利伟)[1,2,†], Yu-Qing Zhang(张宇青)[1], Xiao-Xiong Tian(田晓雄)[1], Yu-Hua Qian(钱宇华)[2], and Shi-Hui Zheng(郑世慧)[3]

[1] College of Information, Shanxi University of Finance and Economics, Taiyuan 030006, China
[2] Institute of Big Data Science and Industry, Shanxi University, Taiyuan 030006, China
[3] School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100876, China

(Received 5 September 2019; revised manuscript received 21 October 2019; accepted manuscript online 14 November 2019)

Quantum system is inevitably affected by the external environment in the real world. Two controlled quantum dialogue protocols are put forward based on logical χ-type states under collective noise environment. One is against collective-dephasing noise, while the other is against collective-rotation noise. Compared with existing protocols, there exist several outstanding advantages in our proposed protocols: Firstly, the χ-type state is utilized as quantum channels, it possesses better entanglement properties than GHZ state, W state as well as cluster state, which make it difficult to be destroyed by local operations. Secondly, two kinds of logical χ-type states are constructed by us in theory, which can be perfectly immune to the effects of collective noise. Thirdly, the controller can be offline after quantum distribution and permission announcement, without waiting for all the participants to complete the information coding. Fourthly, the security analysis illuminates that our protocols can not only be free from the information leakage, but also resist against the intercept-and-resend attack, the entanglement-and-measure attack, the modification attack, the conspiring attack, and especially the dishonest controller's attacks.

Keywords: controlled quantum dialogue, collective noise, logical χ-type state, dishonest controller's attacks

PACS: 03.67.–a, 03.67.Dd, 03.67.Hk **DOI:** 10.1088/1674-1056/ab5786

1. Introduction

With the advent of the era of big data and cloud computing, the problem of personal information leakage will be increasingly prominent although the data can bring much convenience to human life. This problem will make every one become a transparent person in this era. Hence, how to effectively ensure the security of information is of great importance.

Classical cryptography is always a common choice, but it will face the threat of being broken through in polynomial time with the advent of quantum algorithms.[1,2] Quantum cryptography has been proven to be unconditionally secure over an insecure channel, whose security is guaranteed by quantum mechanics such as Heisenberg uncertainty principle and non-cloning theorem. Therefore, quantum cryptography is attracting more and more attention from both industry and academia. Up to date, various quantum communication protocols have been presented by scholars and engineers, such as quantum key distribution (QKD),[3–5] quantum secure direct communication (QSDC),[6–8] quantum secret sharing (QSS),[9–11] quantum teleportation (QT),[12,13] remote state preparation (RSP),[14,15] and quantum signature (QS).[16,17]

As a significant branch of quantum cryptography, quantum dialogue (QD) allows two participants to exchange their secret message simultaneously, which is also known as bidirectional quantum secure direct communication (BQSDC). In 2004, Nguyen *et al.* invented the first QD protocol by extending the quantum secure direct communication (QSDC).[18] To date, the fruitful research results have been achieved.[19–25] In 2006, Man *et al.*[26] introduced the novel notion of controlled quantum dialogue (CQD) and proposed a CQD protocol based on GHZ entangled states. In fact CQD adds a new role to the whole dialogue process, called controller, who is responsible for supervising the secret communication between two legitimate participants. In 2013, Yang *et al.*[27] devised a novel scheme of CQD based on Brown states, unfortunately, there exists a risk of information leakage in it. In the same year, Ye *et al.*[28] found out that the information leakage problem exists in the protocol proposed by Man *et al.*[26] and then put forward two approaches to be free from it. However, it was proven that these two improved approaches still suffer from the information leakage problem[29,30] as well as the intercept-and-resend attack.[31] In 2016, Kao *et al.*[32] indicated that the conspiring attack exists in all the previous CQD protocols, and designed an improvement scheme. In 2017, Kao *et al.*[33] put forward a new CQD protocol based on cluster states again and suggested that some security requirements must be satisfied in the CQD protocols:

(1) The users' secrets will not be leaked to the outsiders or even to the controller.

(2) A user can obtain the other user's secret message con-

*Project supported by the National Natural Science Foundation of China (Grant No. 61502048), the Natural Science Foundation of Shanxi Province of China (Grant No. 201801D221159), the Scientific and Technological Innovation Programs of Higher Education Institutions in Shanxi Province of China (Grant No. 2019L0470), and Youth Research Foundation of Shanxi University of Finance and Economics in Shanxi Province of China (Grant No. QN-2016009).

†Corresponding author. E-mail: changliwei002@163.com

© 2020 Chinese Physical Society and IOP Publishing Ltd

tent only if the controller provides a permission.

(3) The users in a CQD protocol cannot conspire to communicate without the controller's permission.

Recently, Liu *et al.* pointed out that the protocol presented in Ref. [33] will inevitably suffer from the dishonest controller's attacks, namely, so-called different-initial-state (DIS) attack and denial-of-service (DoS) attack, and designed an improved scheme for mending these security loopholes.[34] Owing to these loopholes, this paper introduced a new requirement for CQD protocols.

(4) The users in a CQD protocol must be capable of preventing the dishonest controller's attacks. In brief, how to design an efficient and secure CQD protocol meeting the above four requirements is a hot issue for the researchers.

So far, a majority of existing CQD protocols are designed in an ideal environment. In fact, the qubits will inevitably be affected by channel noise during the transmission over the quantum channel. As a result, a malicious attacker can launch the baleful attack under the cover of all the noises. Hence, it is necessary to consider the noise factor when some new CQD protocols are put forward. The simple and practical method for realizing the reliable transmission of qubits over collective noise channel is to construct decoherence-free states (DFS). Because they can eliminate the effects of collective noise better, the decoherence-free states have been widely applied to design QD protocols against collective noise.[35–42] However, to our knowledge, the specific CQD protocols against collective noise have been rarely studied so far. In consequence, we take into account how to design the CQD protocols against collective noise.

Quantum entanglement, one of the most striking features of quantum mechanics, is exploited as an important resource for quantum communication and quantum information processing (QIP). In 2006, a new type of four-qubit genuine entangled states was proposed by Yeo *et al.* in Ref. [43], called the χ-type state. It can be expressed as

$$\begin{aligned}|\chi\rangle &= \frac{1}{2\sqrt{2}}[|00\rangle(|00\rangle-|11\rangle)-|01\rangle(|01\rangle-|10\rangle)\\ &\quad+|10\rangle(|01\rangle+|10\rangle)+|11\rangle(|00\rangle+|11\rangle)]_{1234}\\ &= \frac{1}{2}(|00\rangle|\phi^-\rangle-|01\rangle|\psi^-\rangle\\ &\quad+|10\rangle|\psi^+\rangle+|11\rangle|\phi^+\rangle)_{1234}, \end{aligned} \tag{1}$$

where

$$|\phi^\pm\rangle=\frac{1}{\sqrt{2}}(|00\rangle\pm|11\rangle),\quad |\psi^\pm\rangle=\frac{1}{\sqrt{2}}(|01\rangle\pm|10\rangle). \tag{2}$$

It does not belong to the well-known three types of multipartite entangled states, i.e., GHZ, cluster and W states. It owns two valuable features: On the one hand, it has been shown that the χ-type state optimally violates a new Bell inequality. On the other hand, the χ-type state has the maximum entanglement between qubits (1,2) and (3,4), and between qubits (1,3) and (2,4), that is, it is difficult to be destroyed by local operations. Over the past few years, the schemes of generating χ-type states have been explored in various physical systems.[44–47] By utilizing the χ-type states, Liu *et al.*[48] presented a new quantum protocol for comparing the equal information with the help of a semi-honest third party (TP). Kang *et al.*[49] proposed a novel scheme for multi-party quantum state sharing (MQSTS) of an arbitrary multi-qubit state by means of the χ-type states. Dong *et al.*[50] came up with a protocol teleporting a general two-photon polarization state by employing a polarization-entangled χ-type state. Xu *et al.*[51] put forward an improved quantum information hiding protocol based on entanglement swapping among χ-type states. Tan *et al.*[52] designed a delegated quantum computation protocol with the χ-type states. Yang *et al.*[53] devised a simultaneous dense coding protocol with the χ-type states, in which two participants can simultaneously obtain the classical information from the other.

For satisfying the demands of practical applications, we put forward two controlled quantum dialogue (CQD) protocols based on logical χ-type states under collective noise environment. One is against collective-dephasing noise, while the other is against collective-rotation noise. These two protocols own four outstanding features:

(1) The χ-type states are used as information carriers, which are in possession of excellent entanglement properties.

(2) By drawing on the advantages of DFS, we construct two kinds of logical χ-type states, which can be immune to the effects of collective-dephasing noise and collective-rotation noise, respectively.

(3) The controller can be offline after quantum distribution and permission announcement, without waiting for all the participants to complete the information coding, that is to say, the waiting time of the controller will be effectively reduced.

(4) They can not only perfectly avoid the information leakage problem, but also withstand several well-known attacks, such as the intercept-and-resend attack, the entanglement-and-measure attack, the modification attack, the conspiring attack, and especially the dishonest controller's attacks.

The rest of this paper is organized as follows: Section 2 introduces the basic knowledge of two types of collective noise and makes a detailed explanation on how to construct two kinds of logical χ-type states in theory. Section 3 comes up with a fault tolerant controlled quantum dialogue protocol by exploiting the logical χ-type states, which can be against collective-dephasing noise. In Section 4, a fault tolerant controlled quantum dialogue protocol against collective-rotation noise is put forward by means of logical χ-type states. Section 5 analyzes why our protocols are secure against various

well-known attacks in detail. In Section 6, we make a comparison between previous CQD protocols and our proposed CQD protocols. Lastly, a conclusion is drawn in Section 7.

2. Preliminaries

In this section, we firstly together give a review of both collective-dephasing noise and collective-rotation noise; secondly study the characters of logical qubit and its corresponding logical unitary operations; and finally construct two kinds of logical χ-type states in theory to be against collective noise.

2.1. Collective-dephasing noise

A collective-dephasing noise can be expressed as

$$U_{\rm dp}|0\rangle = |0\rangle,\ \ U_{\rm dp}|1\rangle = {\rm e}^{{\rm i}\varphi}|1\rangle, \tag{3}$$

where φ is the noise parameter which fluctuates along with time; $|0\rangle$ and $|1\rangle$ are the horizontal and vertical polarizations of photons, respectively. The two logical qubits can be written as

$$|0_{\rm dp}\rangle = |01\rangle,\ \ |1_{\rm dp}\rangle = |10\rangle. \tag{4}$$

Each of them is encoded into two antiparallel qubits and can be perfectly immune to the collective-dephasing noise since the same phase factor ${\rm e}^{{\rm i}\varphi}$ is acquired. The superpositions of these two logical qubits

$$|\pm_{\rm dp}\rangle = \frac{1}{\sqrt{2}}(|0_{\rm dp}\rangle \pm |1_{\rm dp}\rangle) = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle) \tag{5}$$

are also invariant over this kind of noise. Moreover, we define three logical unitary operations as

$$\begin{aligned} &U_0^{\rm dp} = I_1 \otimes I_2,\quad U_1^{\rm dp} = ({\rm i}\sigma_y)_1 \otimes (\sigma_x)_2,\\ &U_2^{\rm dp} = (\sigma_z)_1 \otimes I_2, \end{aligned} \tag{6}$$

where $I = |0\rangle\langle 0| + |1\rangle\langle 1|$, ${\rm i}\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|$, $\sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|$ and $\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$ are four unitary operations and the subscripts 1 and 2 represent the first and the second physical qubits in each logical qubit, respectively. The effects of the unitary operations $U_1^{\rm dp}$ and $U_2^{\rm dp}$ on each logical qubit can be described as

$$\begin{aligned} &U_1^{\rm dp}|0_{\rm dp}\rangle = -|1_{\rm dp}\rangle,\quad U_1^{\rm dp}|1_{\rm dp}\rangle = |0_{\rm dp}\rangle,\\ &U_1^{\rm dp}|+_{\rm dp}\rangle = |-_{\rm dp}\rangle,\quad U_1^{\rm dp}|-_{\rm dp}\rangle = -|+_{\rm dp}\rangle,\\ &U_2^{\rm dp}|0_{\rm dp}\rangle = |0_{\rm dp}\rangle,\quad U_2^{\rm dp}|1_{\rm dp}\rangle = -|1_{\rm dp}\rangle,\\ &U_2^{\rm dp}|+_{\rm dp}\rangle = |-_{\rm dp}\rangle,\quad U_2^{\rm dp}|-_{\rm dp}\rangle = |+_{\rm dp}\rangle. \end{aligned} \tag{7}$$

2.2. Collective-rotation noise

A collective-rotation noise can be expressed as

$$U_{\rm r}|0\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle,\quad U_{\rm r}|1\rangle = -\sin\theta|0\rangle + \cos\theta|1\rangle, \tag{8}$$

where the parameter θ depends on the noise and fluctuates with time. Under this noise environment, $|\phi^+\rangle$ and $|\psi^-\rangle$ are invariant, hence they can be chosen as two logical qubits

$$\begin{aligned} |0_{\rm r}\rangle &= |\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle),\\ |1_{\rm r}\rangle &= |\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \end{aligned} \tag{9}$$

The superpositions of these two logical qubits are also invariant over this kind of noise, which can be depicted as

$$|\pm_{\rm r}\rangle = \frac{1}{\sqrt{2}}(|0_{\rm r}\rangle \pm |1_{\rm r}\rangle) = \frac{1}{\sqrt{2}}(|\phi^+\rangle \pm |\psi^-\rangle). \tag{10}$$

In addition, we define three logical unitary operations as

$$U_0^{\rm r} = I_1 \otimes I_2,\quad U_1^{\rm r} = I_1 \otimes ({\rm i}\sigma_y)_2,\quad U_2^{\rm r} = (\sigma_x)_1 \otimes (\sigma_x)_2, \tag{11}$$

where $I = |0\rangle\langle 0| + |1\rangle\langle 1|$, ${\rm i}\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|$ and $\sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|$ are three unitary operations and the subscripts 1 and 2 represent the first and the second physical qubits in each logical qubit, respectively. The effects of the unitary operations $U_1^{\rm r}$ and $U_2^{\rm r}$ on each logical qubit can be described as

$$\begin{aligned} &U_1^{\rm r}|0_{\rm r}\rangle = -|1_{\rm r}\rangle,\quad U_1^{\rm r}|1_{\rm r}\rangle = |0_{\rm r}\rangle,\\ &U_1^{\rm r}|+_{\rm r}\rangle = |-_{\rm r}\rangle,\quad U_1^{\rm r}|-_{\rm r}\rangle = -|+_{\rm r}\rangle,\\ &U_2^{\rm r}|0_{\rm r}\rangle = |0_{\rm r}\rangle,\quad U_2^{\rm r}|1_{\rm r}\rangle = -|1_{\rm r}\rangle,\\ &U_2^{\rm r}|+_{\rm r}\rangle = |-_{\rm r}\rangle,\quad U_2^{\rm r}|-_{\rm r}\rangle = |+_{\rm r}\rangle. \end{aligned} \tag{12}$$

2.3. The logical χ-type state against collective noise

Generating some logical states with good properties is a good choice for being against collective noise. Hence we are considering how to prepare two kinds of logical χ-type states against both collective-dephasing noise and collective-rotation noise. Fortunately, the dilemma is entirely solved by us. Subsequently, we offer a detailed explanation on how these two kinds of logical χ-type states are prepared.

2.3.1. The logical χ-type state against collective-dephasing noise

As shown in Fig. 1, we plot the illustration of how to prepare the logical χ-type states against collective-dephasing noise from three superposition states and one product state. The specific generation scheme can be described as follows:

Step 1 One performs a controlled-$U_1^{\rm dp}$ ($CU_1^{\rm dp}$) operation on the first physical qubit c_1 of logical qubit c and the logical qubit d (c_1 is the controller and d is the target), where $CU_1^{\rm dp} = |0\rangle\langle 0| \otimes U_0^{\rm dp} + |1\rangle\langle 1| \otimes U_1^{\rm dp}$, and performs a controlled-$U_2^{\rm dp}$ ($CU_2^{\rm dp}$) on the qubit c_1 and the logical qubit d (c_1 is the controller and d is the target), where $CU_2^{\rm dp} = |0\rangle\langle 0| \otimes U_0^{\rm dp} + |1\rangle\langle 1| \otimes U_2^{\rm dp}$.

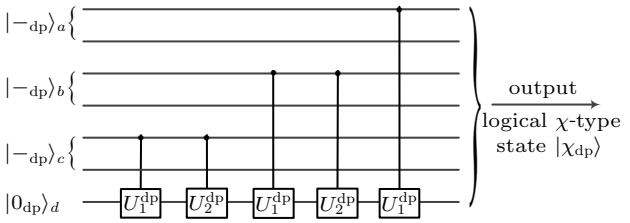


Fig. 1. The quantum circuit for the preparation of the logical χ-type state against collective-dephasing noise. The horizontal lines denote the qubits a_1, a_2, b_1, b_2, c_1, c_2 and the logical qubit d from top to bottom, where the subscripts 1 and 2 represent the first and the second physical qubits of logical qubit, respectively. In addition, $|-_{\rm dp}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ and $|0_{\rm dp}\rangle = |01\rangle$.

Step 2 In the similar way, one implements a $CU_1^{\rm dp}$ operation on the first physical qubit b_1 of logical qubit b and the logical qubit d (b_1 is the controller and d is the target). Afterward, he performs a $CU_2^{\rm dp}$ operation on the qubit b_1 and the logical qubit d (b_1 is the controller and d is the target).

Step 3 One carries out a $CU_1^{\rm dp}$ operation on the first physical qubit a_1 of logical qubit a and the logical qubit d using the qubit a_1 as the control qubit and the logical qubit d as the target qubit.

The whole process of preparing the logical χ-type state against collective-dephasing noise can be shown as

$$
\begin{aligned}
& \frac{1}{\sqrt{2}}(|0_{\rm dp}\rangle - |1_{\rm dp}\rangle)_a \otimes \frac{1}{\sqrt{2}}(|0_{\rm dp}\rangle - |1_{\rm dp}\rangle)_b \otimes \frac{1}{\sqrt{2}}(|0_{\rm dp}\rangle - |1_{\rm dp}\rangle)_c \otimes |0_{\rm dp}\rangle_d \\
\xrightarrow{CU_1^{\rm dp}{}_{(c_1,d)}} & \frac{1}{2\sqrt{2}}(|0_{\rm dp}\rangle - |1_{\rm dp}\rangle)_a \otimes (|0_{\rm dp}\rangle - |1_{\rm dp}\rangle)_b \otimes (|0_{\rm dp}0_{\rm dp}\rangle + |1_{\rm dp}1_{\rm dp}\rangle)_{cd} \\
\xrightarrow{CU_2^{\rm dp}{}_{(c_1,d)}} & \frac{1}{2\sqrt{2}}(|0_{\rm dp}\rangle - |1_{\rm dp}\rangle)_a \otimes (|0_{\rm dp}\rangle - |1_{\rm dp}\rangle)_b \otimes (|0_{\rm dp}0_{\rm dp}\rangle - |1_{\rm dp}1_{\rm dp}\rangle)_{cd} \\
\xrightarrow{CU_1^{\rm dp}{}_{(b_1,d)}} & \frac{1}{2\sqrt{2}}(|0_{\rm dp}\rangle - |1_{\rm dp}\rangle)_a \otimes (|0_{\rm dp}0_{\rm dp}0_{\rm dp}\rangle - |0_{\rm dp}1_{\rm dp}1_{\rm dp}\rangle + |1_{\rm dp}0_{\rm dp}1_{\rm dp}\rangle + |1_{\rm dp}1_{\rm dp}0_{\rm dp}\rangle)_{bcd} \\
\xrightarrow{CU_2^{\rm dp}{}_{(b_1,d)}} & \frac{1}{2\sqrt{2}}(|0_{\rm dp}\rangle - |1_{\rm dp}\rangle)_a \otimes (|0_{\rm dp}0_{\rm dp}0_{\rm dp}\rangle - |0_{\rm dp}1_{\rm dp}1_{\rm dp}\rangle - |1_{\rm dp}0_{\rm dp}1_{\rm dp}\rangle + |1_{\rm dp}1_{\rm dp}0_{\rm dp}\rangle)_{bcd} \\
\xrightarrow{CU_1^{\rm dp}{}_{(a_1,d)}} & \frac{1}{2\sqrt{2}}(|0_{\rm dp}0_{\rm dp}0_{\rm dp}0_{\rm dp}\rangle - |0_{\rm dp}0_{\rm dp}1_{\rm dp}1_{\rm dp}\rangle - |0_{\rm dp}1_{\rm dp}0_{\rm dp}1_{\rm dp}\rangle + |0_{\rm dp}1_{\rm dp}1_{\rm dp}0_{\rm dp}\rangle \\
& + |1_{\rm dp}0_{\rm dp}0_{\rm dp}1_{\rm dp}\rangle + |1_{\rm dp}0_{\rm dp}1_{\rm dp}0_{\rm dp}\rangle + |1_{\rm dp}1_{\rm dp}0_{\rm dp}0_{\rm dp}\rangle + |1_{\rm dp}1_{\rm dp}1_{\rm dp}1_{\rm dp}\rangle)_{abcd} \\
= & \frac{1}{2}(|0_{\rm dp}0_{\rm dp}\rangle|\phi_{\rm dp}^-\rangle - |0_{\rm dp}1_{\rm dp}\rangle|\psi_{\rm dp}^-\rangle + |1_{\rm dp}0_{\rm dp}\rangle|\psi_{\rm dp}^+\rangle + |1_{\rm dp}1_{\rm dp}\rangle|\phi_{\rm dp}^+\rangle)_{abcd}, \qquad (13)
\end{aligned}
$$

where the subscripts a_1, b_1 and c_1 stand for the first physical qubit of logical qubits a, b, and c in each pair, respectively.

2.3.2. The logical χ-type state against collective-rotation noise

As demonstrated in Fig. 2, we plot the illustration of how to prepare the logical χ-type states against collective-rotation noise from four superposition states. The detailed generation scheme can be depicted as follows:

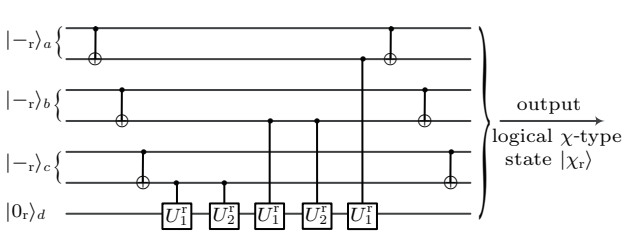


Fig. 2. The quantum circuit for the preparation of the logical χ-type state against collective-rotation noise. The horizontal lines denote the qubits a_1, a_2, b_1, b_2, c_1, c_2 and the logical qubit d from top to bottom, where the subscripts 1 and 2 represent the first and the second physical qubits of logical qubit, respectively. In addition, $|-_{\rm r}\rangle = \frac{1}{\sqrt{2}}(|\phi^+\rangle - |\psi^-\rangle)$ and $|0_{\rm r}\rangle = |\phi^+\rangle$.

Step 1 For each of logical qubits $|-_r\rangle$, one performs a controlled-NOT (CNOT) operation on the first and the second physical qubits of each logical qubit (the first is the controller and the second is the target), while the logical qubit $|-_r\rangle$ is changed into $|\xi\rangle = \frac{1}{2}(|00\rangle + |10\rangle - |01\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|+\rangle|0\rangle - |-\rangle|1\rangle)$.

Step 2 One performs a controlled-$U_1^{\rm r}$ ($CU_1^{\rm r}$) operation on the second physical qubit c_2 of logical qubit c and the logical qubit d (c_2 is the controller and d is the target), where $CU_1^{\rm r} = |0\rangle\langle 0| \otimes U_0^{\rm r} + |1\rangle\langle 1| \otimes U_1^{\rm r}$, and performs a controlled-$U_2^{\rm r}$ ($CU_2^{\rm r}$) on the qubit c_2 and the logical qubit d (c_2 is the controller and d is the target), where $CU_2^{\rm r} = |0\rangle\langle 0| \otimes U_0^{\rm r} + |1\rangle\langle 1| \otimes U_2^{\rm r}$.

Step 3 Similarly, one implements a $CU_1^{\rm r}$ operation on the second physical qubit b_2 of logical qubit b and the logical qubit d (b_2 is the controller and d is the target). Afterward, he performs a $CU_2^{\rm r}$ operation on the qubit b_2 and the logical qubit d (b_2 is the controller and d is the target).

Step 4 One carries out a $CU_1^{\rm r}$ operation on the second physical qubit a_2 of logical qubit a and the logical qubit d using the qubit a_2 as the control qubit and the logical qubit d as

the target qubit.

Step 5 For logical qubits a, b, and c, one performs CNOT operations on the first and the second physical qubits of each logical qubit using the first as the control qubit and the second as the target qubit, while the state $|\xi\rangle = \frac{1}{\sqrt{2}}(|+\rangle|0\rangle - |-\rangle|1\rangle)$ is changed into $|-_{\rm r}\rangle = \frac{1}{\sqrt{2}}(|\phi^+\rangle - |\psi^-\rangle)$.

The whole process of preparing the logical χ-type state against collective-rotation noise can be shown as follows:

$$
\begin{aligned}
& \frac{1}{\sqrt{2}}(|0_{\rm r}\rangle - |1_{\rm r}\rangle)_a \otimes \frac{1}{\sqrt{2}}(|0_{\rm r}\rangle - |1_{\rm r}\rangle)_b \otimes \frac{1}{\sqrt{2}}(|0_{\rm r}\rangle - |1_{\rm r}\rangle)_c \otimes |0_{\rm r}\rangle_d \\
\xrightarrow{\text{CNOT}} \quad & \frac{1}{2\sqrt{2}}(|+\rangle|0\rangle - |-\rangle|1\rangle)_{a_1a_2} \otimes (|+\rangle|0\rangle - |-\rangle|1\rangle)_{b_1b_2} \otimes (|+\rangle|0\rangle - |-\rangle|1\rangle)_{c_1c_2} \otimes |0_{\rm r}\rangle_d \\
\xrightarrow{CU^{\rm r}_{1(c_2,d)}} \quad & \frac{1}{2\sqrt{2}}(|+\rangle|0\rangle - |-\rangle|1\rangle)_{a_1a_2} \otimes (|+\rangle|0\rangle - |-\rangle|1\rangle)_{b_1b_2} \otimes (|+\rangle|0\rangle|0_{\rm r}\rangle + |-\rangle|1\rangle|1_{\rm r}\rangle)_{c_1c_2d} \\
\xrightarrow{CU^{\rm r}_{2(c_2,d)}} \quad & \frac{1}{2\sqrt{2}}(|+\rangle|0\rangle - |-\rangle|1\rangle)_{a_1a_2} \otimes (|+\rangle|0\rangle - |-\rangle|1\rangle)_{b_1b_2} \otimes (|+\rangle|0\rangle|0_{\rm r}\rangle - |-\rangle|1\rangle|1_{\rm r}\rangle)_{c_1c_2d} \\
\xrightarrow{CU^{\rm r}_{1(b_2,d)}} \quad & \frac{1}{2\sqrt{2}}(|+\rangle|0\rangle - |-\rangle|1\rangle)_{a_1a_2} \otimes (|+\rangle|0\rangle|+\rangle|0\rangle|0_{\rm r}\rangle - |+\rangle|0\rangle|-\rangle|1\rangle|1_{\rm r}\rangle + |-\rangle|1\rangle|+\rangle|0\rangle|1_{\rm r}\rangle + |-\rangle|1\rangle|-\rangle|1\rangle|0_{\rm r}\rangle)_{b_1b_2c_1c_2d} \\
\xrightarrow{CU^{\rm r}_{2(b_2,d)}} \quad & \frac{1}{2\sqrt{2}}(|+\rangle|0\rangle - |-\rangle|1\rangle)_{a_1a_2} \otimes (|+\rangle|0\rangle|+\rangle|0\rangle|0_{\rm r}\rangle - |+\rangle|0\rangle|-\rangle|1\rangle|1_{\rm r}\rangle \\
& -|-\rangle|1\rangle|+\rangle|0\rangle|1_{\rm r}\rangle + |-\rangle|1\rangle|-\rangle|1\rangle|0_{\rm r}\rangle)_{b_1b_2c_1c_2d} \\
\xrightarrow{CU^{\rm r}_{1(a_2,d)}} \quad & \frac{1}{2\sqrt{2}}(|+\rangle|0\rangle|+\rangle|0\rangle|+\rangle|0\rangle|0_{\rm r}\rangle - |+\rangle|0\rangle|+\rangle|0\rangle|-\rangle|1\rangle|1_{\rm r}\rangle - |+\rangle|0\rangle|-\rangle|1\rangle|+\rangle|0\rangle|1_{\rm r}\rangle \\
& +|+\rangle|0\rangle|-\rangle|1\rangle|-\rangle|1\rangle|0_{\rm r}\rangle + |-\rangle|1\rangle|+\rangle|0\rangle|+\rangle|0\rangle|1_{\rm r}\rangle + |-\rangle|1\rangle|+\rangle|0\rangle|-\rangle|1\rangle|0_{\rm r}\rangle \\
& +|-\rangle|1\rangle|-\rangle|1\rangle|+\rangle|0\rangle|0_{\rm r}\rangle + |-\rangle|1\rangle|-\rangle|1\rangle|-\rangle|1\rangle|1_{\rm r}\rangle)_{a_1a_2b_1b_2c_1c_2d} \\
\xrightarrow{\text{CNOT}} \quad & \frac{1}{8}[(|00\rangle + |11\rangle)(|00\rangle + |11\rangle)(|00\rangle + |11\rangle)|0_{\rm r}\rangle - (|00\rangle + |11\rangle)(|00\rangle + |11\rangle)(|01\rangle - |10\rangle)|1_{\rm r}\rangle \\
& -(|00\rangle + |11\rangle)(|01\rangle - |10\rangle)(|00\rangle + |11\rangle)|1_{\rm r}\rangle + (|00\rangle + |11\rangle)(|01\rangle - |10\rangle)(|01\rangle - |10\rangle)|0_{\rm r}\rangle \\
& +(|01\rangle - |10\rangle)(|00\rangle + |11\rangle)(|00\rangle + |11\rangle)|1_{\rm r}\rangle + (|01\rangle - |10\rangle)(|00\rangle + |11\rangle)(|01\rangle - |10\rangle)|0_{\rm r}\rangle \\
& +(|01\rangle - |10\rangle)(|01\rangle - |10\rangle)(|00\rangle + |11\rangle)|0_{\rm r}\rangle + (|01\rangle - |10\rangle)(|01\rangle - |10\rangle)(|01\rangle - |10\rangle)|1_{\rm r}\rangle]_{a_1a_2b_1b_2c_1c_2d} \\
= \quad & \frac{1}{2\sqrt{2}}(|0_{\rm r}0_{\rm r}0_{\rm r}0_{\rm r}\rangle - |0_{\rm r}0_{\rm r}1_{\rm r}1_{\rm r}\rangle - |0_{\rm r}1_{\rm r}0_{\rm r}1_{\rm r}\rangle + |0_{\rm r}1_{\rm r}1_{\rm r}0_{\rm r}\rangle + |1_{\rm r}0_{\rm r}0_{\rm r}1_{\rm r}\rangle + |1_{\rm r}0_{\rm r}1_{\rm r}0_{\rm r}\rangle + |1_{\rm r}1_{\rm r}0_{\rm r}0_{\rm r}\rangle + |1_{\rm r}1_{\rm r}1_{\rm r}1_{\rm r}\rangle)_{abcd} \\
= \quad & \frac{1}{2}(|0_{\rm r}0_{\rm r}\rangle|\phi^-_{\rm r}\rangle - |0_{\rm r}1_{\rm r}\rangle|\psi^-_{\rm r}\rangle + |1_{\rm r}0_{\rm r}\rangle|\psi^+_{\rm r}\rangle + |1_{\rm r}1_{\rm r}\rangle|\phi^+_{\rm r}\rangle)_{abcd}, \qquad (14)
\end{aligned}
$$

where the subscripts a_2, b_2, and c_2 signify the second physical qubit of logical states a, b, and c in each pair, respectively.

3. CQD protocol against collective-dephasing noise

In this section, a fault tolerant CQD protocol against collective-dephasing noise is put forward, which includes one controller, Charlie, and two communicants, Alice and Bob. As shown in Fig. 3, the whole workflow is described as follows:

Step 1 Alice sends a communication request to Charlie. Charlie generates a sequence of $2N$ logical χ-type states, each of which is in the state

$$
\begin{aligned}
|\chi_{\rm dp}\rangle = & \frac{1}{2}(|0_{\rm dp}0_{\rm dp}\rangle|\phi^-_{\rm dp}\rangle - |0_{\rm dp}1_{\rm dp}\rangle|\psi^-_{\rm dp}\rangle \\
& + |1_{\rm dp}0_{\rm dp}\rangle|\psi^+_{\rm dp}\rangle + |1_{\rm dp}1_{\rm dp}\rangle|\phi^+_{\rm dp}\rangle)_{A_1B_1A_2B_2} \\
= & \frac{1}{2\sqrt{2}}[|01\rangle|01\rangle(|01\rangle|01\rangle - |10\rangle|10\rangle) \\
& - |01\rangle|10\rangle(|01\rangle|10\rangle - |10\rangle|01\rangle) \\
& + |10\rangle|01\rangle(|01\rangle|10\rangle + |10\rangle|01\rangle) + |10\rangle|10\rangle(|01\rangle|01\rangle \\
& + |10\rangle|10\rangle)]_{A_1^1A_1^2B_1^1B_1^2A_2^1A_2^2B_2^1B_2^2}. \qquad (15)
\end{aligned}
$$

Afterwards, Charlie firstly divides these logical χ-type states into two qubit sequences S_A and S_B, where S_A is composed of all the logical qubits A_1 and A_2, and all the logical qubits B_1 and B_2 constitute S_B; secondly performs the operations $U_0^{\rm dp}$ or $U_1^{\rm dp}$ on the logical qubits A_2 in S_A to form S'_A in random and records these operations as her permission; and thirdly generates $4N$ logical qubits as checking qubits, where every checking qubit is arbitrarily chosen from $\{|0_{\rm dp}\rangle, |1_{\rm dp}\rangle, |+_{\rm dp}\rangle, |-_{\rm dp}\rangle\}$, mixes them with S'_A (S_B) to form a new sequence Q_A (Q_B), and sends it to Alice (Bob) in the method of data block transmission[54] through a collective-dephasing noise channel.

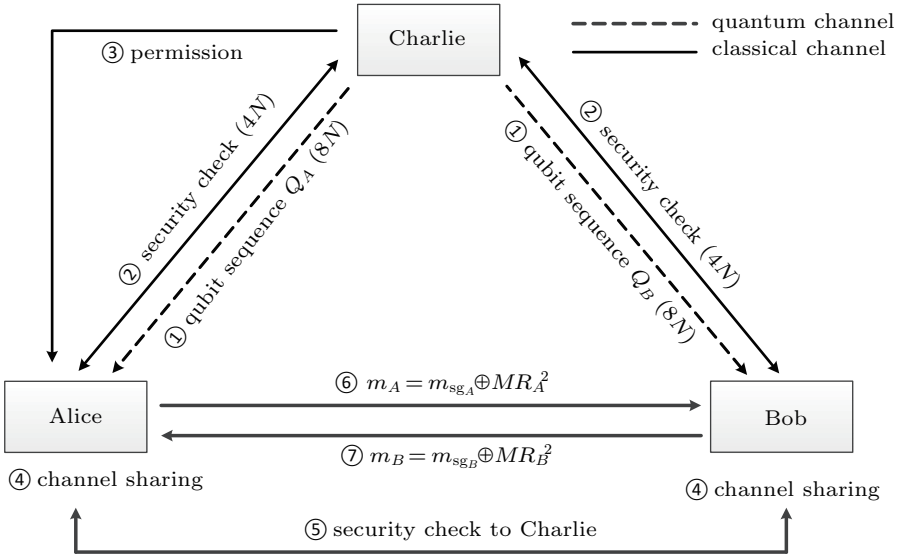


Fig. 3. The CQD protocol using the logical χ-type states against collective-dephasing noise.

Step 2 Upon receiving Q_A (Q_B), Alice (Bob) publicly discusses the measurement results of checking qubits with Charlie. If the error rate is low enough, they believe that the quantum transmission is secure, and remove the checking qubits from Q_A (Q_B). Otherwise, the communication will be halted.

Step 3 If Charlie allows Alice and Bob to communicate, she will announce the permission to Alice. In the light of Charlie's permission, Alice performs the same operations as what Charlie did on the logical qubits A_2 in S'_A. Because both $U_0^{\rm dp}$ and $U_1^{\rm dp}$ are unitary operations, Alice is able to cancel Charlie's operations, and then the entangled states shared for Alice and Bob can be recovered to the initial states, except for a global phase factor (i.e., -1), when $U_1^{\rm dp}$ is carried out.

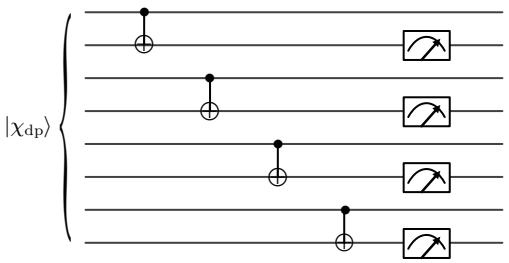


Fig. 4. The process of transforming the logical χ-type states against collective-dephasing noise into the χ-type states. The horizontal lines represent the qubits A_1^1, A_1^2, B_1^1, B_1^2, A_2^1, A_2^2, B_2^1, and B_2^2 from top to bottom, respectively.

Step 4 As depicted in Fig. 4, for each remaining χ-type state, Alice performs a CNOT operation on her qubits A_1^1 (A_2^1) and A_1^2 (A_2^2) using A_1^1 (A_2^1) as the control qubit and A_1^2 (A_2^2) as the target qubit. In a similar manner, Bob implements a CNOT operation on his qubits B_1^1 (B_2^1) and B_1^2 (B_2^2) using B_1^1 (B_2^1) as the control qubit and B_1^2 (B_2^2) as the target qubit

$$\begin{aligned}|\Theta_{\rm dp}\rangle \;=\; & \frac{1}{2\sqrt{2}}[|01\rangle|01\rangle(|01\rangle|01\rangle-|11\rangle|11\rangle)\\ & -|01\rangle|11\rangle(|01\rangle|11\rangle-|11\rangle|01\rangle)\\ & +|11\rangle|01\rangle(|01\rangle|11\rangle+|11\rangle|01\rangle)+|11\rangle|11\rangle(|01\rangle|01\rangle\\ & +|11\rangle|11\rangle)]_{A_1^1A_1^2B_1^1B_1^2A_2^1A_2^2B_2^1B_2^2}. \end{aligned} \tag{16}$$

Then, Alice (Bob) carries out Z-basis measurements on her (his) qubits A_1^2 (B_1^2) and A_2^2 (B_2^2), respectively, and then $|\Theta_{\rm dp}\rangle$ will collapse into

$$\begin{aligned} & {}_{A_1^2}\langle 1|_{B_1^2}\langle 1|_{A_2^2}\langle 1|_{B_2^2}\langle 1|\Theta_{\rm dp}\rangle\\ = \; & \frac{1}{2\sqrt{2}}[|00\rangle(|00\rangle-|11\rangle)-|01\rangle(|01\rangle-|10\rangle)\\ & +|10\rangle(|01\rangle+|10\rangle)+|11\rangle(|00\rangle+|11\rangle)]_{A_1^1B_1^1A_2^1B_2^1}. \end{aligned} \tag{17}$$

To be obvious, three legitimate participants have succeeded in sharing $2N$ χ-type states. For convenience, we replace the original subscript $A_1^1B_1^1A_2^1B_2^1$ with $A_1B_1A_2B_2$.

Step 5 For checking whether Charlie is honest, Bob randomly selects N sample qubits from S_B and tells Alice to choose the corresponding sample qubits from S_A. Whereafter Bob informs Alice of the chosen measurement bases through a classical channel. To be specific, the qubits A_1, B_1, A_2 and B_2 of a sample χ-type state are measured by two sets of measurement bases with the same probability respectively. One is that these qubits are measured by the X-basis, the X-basis, the X-basis and the Z-basis; the other is that the qubits A_1 and A_2 are respectively measured by the Z-basis and the Z-basis, and the qubits B_1 and B_2 are measured by the Bell basis. After that, Alice and Bob compare their measurement results to evaluate whether Charlie is honest or not in accordance with

the following two equations:

$$|\chi\rangle = \frac{1}{2}(|+++0\rangle+|---0\rangle +|+--1\rangle-|-++1\rangle)_{A_1B_1A_2B_2}, \quad (18)$$

$$|\chi\rangle = \frac{1}{2}(|00\rangle|\phi^-\rangle-|01\rangle|\psi^-\rangle +|10\rangle|\psi^+\rangle+|11\rangle|\phi^+\rangle)_{A_1A_2B_1B_2}. \quad (19)$$

Step 6 For each of the remaining N χ-type states, Alice performs X-basis measurements on the qubits A_1 and A_2, respectively. All the measurement results are denoted as two bit strings MR_A^1 and MR_A^2, where $|0\rangle$ and $|+\rangle$ are denoted as 0; $|1\rangle$ and $|-\rangle$ are denoted as 1. Then, Alice transmits the value $m_A = M_{\mathrm{sg}_A} \oplus MR_A^2$ to Bob through a classical channel, where M_{sg_A} is defined as Alice's secret information and $\oplus$ denotes the exclusive-or (XOR) operation.

Step 7 Analogously, for each of the remaining N χ-type states, Bob performs an X-basis measurement on the qubit B_1 and a Z-basis measurement on the qubit B_2, respectively. The measurement results are denoted as two bit strings MR_B^1 and MR_B^2. Later, he transmits the value $m_B = M_{\mathrm{sg}_B} \oplus MR_B^2$ to Alice, where M_{sg_B} is defined as Bob's secret information.

Step 8 In line with her measurement results MR_A^1 and MR_A^2, and the deterministic entanglement correlation of χ-type states, as shown in Eq. (18), Alice can deduce the value of MR_B^2 (see Table 1). As a result, Alice can decode Bob's secret information $M_{\mathrm{sg}_B} = m_B \oplus MR_B^2$. Similarly, Bob can decode Alice's secret information $M_{\mathrm{sg}_A} = m_A \oplus MR_A^2$.

Table 1. Corresponding relationship between measurement outcomes and decoding rules.

MR_A^1	MR_B^1	MR_A^2	MR_B^2
0 ($\|+\rangle$)	0 ($\|+\rangle$)	0 ($\|+\rangle$)	0 ($\|0\rangle$)
0 ($\|+\rangle$)	1 ($\|-\rangle$)	1 ($\|-\rangle$)	1 ($\|1\rangle$)
1 ($\|-\rangle$)	0 ($\|+\rangle$)	0 ($\|+\rangle$)	1 ($\|1\rangle$)
1 ($\|-\rangle$)	1 ($\|-\rangle$)	1 ($\|-\rangle$)	0 ($\|0\rangle$)

4. CQD protocol against collective-rotation noise

In this section, a fault tolerant CQD protocol against collective-rotation noise is elaborated by us, including one controller, Charlie, and two communicants, Alice and Bob. The schematic demonstration of this protocol is the same as Fig. 3. The whole workflow is described as follows:

Step 1 Alice sends a communication request to Charlie. Charlie generates a sequence of $2N$ logical χ-type states, each of which is in the state

$$\begin{aligned}|\chi_{\mathrm{r}}\rangle &= \frac{1}{2}(|0_{\mathrm{r}}0_{\mathrm{r}}\rangle|\phi_{\mathrm{r}}^-\rangle-|0_{\mathrm{r}}1_{\mathrm{r}}\rangle|\psi_{\mathrm{r}}^-\rangle+|1_{\mathrm{r}}0_{\mathrm{r}}\rangle|\psi_{\mathrm{r}}^+\rangle+|1_{\mathrm{r}}1_{\mathrm{r}}\rangle|\phi_{\mathrm{r}}^+\rangle)_{A_1B_1A_2B_2}\\ &= \frac{1}{8\sqrt{2}}\{(|00\rangle+|11\rangle)(|00\rangle+|11\rangle)[(|00\rangle+|11\rangle)(|00\rangle+|11\rangle)-(|01\rangle-|10\rangle)(|01\rangle-|10\rangle)]\\ &\quad-(|00\rangle+|11\rangle)(|01\rangle-|10\rangle)[(|00\rangle+|11\rangle)(|01\rangle-|10\rangle)-(|01\rangle-|10\rangle)(|00\rangle+|11\rangle)]\\ &\quad+(|01\rangle-|10\rangle)(|00\rangle+|11\rangle)[(|00\rangle+|11\rangle)(|01\rangle-|10\rangle)+(|01\rangle-|10\rangle)(|00\rangle+|11\rangle)]\\ &\quad+(|01\rangle-|10\rangle)(|01\rangle-|10\rangle)[(|00\rangle+|11\rangle)(|00\rangle+|11\rangle)+(|01\rangle-|10\rangle)(|01\rangle-|10\rangle)]\}_{A_1^1A_1^2B_1^1B_1^2A_2^1A_2^2B_2^1B_2^2}. \quad (20)\end{aligned}$$

Therewith, Charlie firstly divides these χ-type states into two qubit sequences S_A and S_B, where S_A is composed of all the logical qubits A_1 and A_2, and all the logical qubits B_1 and B_2 constitute S_B; secondly performs the operations U_0^{r} or U_1^{r} on the logical qubits A_2 in S_A to form S_A' randomly and records these operations as her permission; and thirdly generates $4N$ logical qubits as the checking qubits, where every checking qubit is arbitrarily chosen from $\{|0_{\mathrm{r}}\rangle, |1_{\mathrm{r}}\rangle, |+_{\mathrm{r}}\rangle, |-_{\mathrm{r}}\rangle\}$, mixes them with S_A' (S_B) to form a new sequence Q_A (Q_B), and sends it to Alice (Bob) in the method of data block transmission[54] through a collective-rotation noise channel.

Steps 2–3 These two steps are the same as steps 2 and 3 in Section 3.

Step 4 As described in Fig. 5, for each remaining χ-type state, Alice performs a CNOT operation on her qubits A_1^1 (A_2^1) and A_1^2 (A_2^2) using A_1^2 (A_2^2) as the control qubit and A_1^1 (A_2^1) as the target qubit. In a similar manner, Bob performs a CNOT operation on his qubits B_1^1 (B_2^1) and B_1^2 (B_2^2) using B_1^2 (B_2^2) as the control qubit and B_1^1 (B_2^1) as the target qubit.

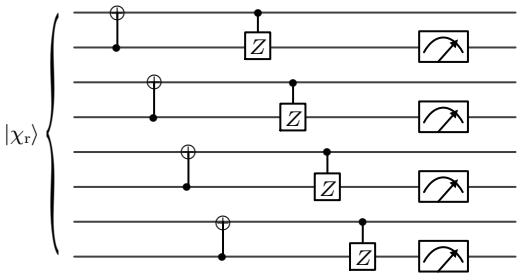


Fig. 5. The process of transforming the logical χ-type states against collective-rotation noise into the χ-type states. The horizontal lines represent the qubits A_1^1, A_1^2, B_1^1, B_1^2, A_2^1, A_2^2, B_2^1, and B_2^2 from top to bottom respectively.

$$
\begin{aligned}
|\Theta_{\rm r}\rangle \;=\; & \frac{1}{8\sqrt{2}}\{(|00\rangle+|01\rangle)(|00\rangle+|01\rangle)[(|00\rangle+|01\rangle)(|00\rangle+|01\rangle)-(|11\rangle-|10\rangle)(|11\rangle-|10\rangle)]\\
& -(|00\rangle+|01\rangle)(|11\rangle-|10\rangle)[(|00\rangle+|01\rangle)(|11\rangle-|10\rangle)-(|11\rangle-|10\rangle)(|00\rangle+|01\rangle)]\\
& +(|11\rangle-|10\rangle)(|00\rangle+|01\rangle)[(|00\rangle+|01\rangle)(|11\rangle-|10\rangle)+(|11\rangle-|10\rangle)(|00\rangle+|01\rangle)]\\
& +(|11\rangle-|10\rangle)(|11\rangle-|10\rangle)[(|00\rangle+|01\rangle)(|00\rangle+|01\rangle)+(|11\rangle-|10\rangle(|11\rangle-|10\rangle)]\}_{A_1^1A_1^2B_1^1B_1^2A_2^1A_2^2B_2^1B_2^2}\\
=\; & \frac{1}{8\sqrt{2}}\{|0\rangle(|0\rangle+|1\rangle)|0\rangle(|0\rangle+|1\rangle)[|0\rangle(|0\rangle+|1\rangle)|0\rangle(|0\rangle+|1\rangle)-|1\rangle(|1\rangle-|0\rangle)|1\rangle(|1\rangle-|0\rangle)]\\
& -|0\rangle(|0\rangle+|1\rangle)|1\rangle(|1\rangle-|0\rangle)[|0\rangle(|0\rangle+|1\rangle)|1\rangle(|1\rangle-|0\rangle)-|1\rangle(|1\rangle-|0\rangle)|0\rangle(|0\rangle+|1\rangle)]\\
& +|1\rangle(|1\rangle-|0\rangle)|0\rangle(|0\rangle+|1\rangle)[|0\rangle(|0\rangle+|1\rangle)|1\rangle(|1\rangle-|0\rangle)+|1\rangle(|1\rangle-|0\rangle)|0\rangle(|0\rangle+|1\rangle)]\\
& +|1\rangle(|1\rangle-|0\rangle)|1\rangle(|1\rangle-|0\rangle)[|0\rangle(|0\rangle+|1\rangle)|0\rangle(|0\rangle+|1\rangle)+|1\rangle(|1\rangle-|0\rangle)|1\rangle(|1\rangle-|0\rangle)]\}_{A_1^1A_1^2B_1^1B_1^2A_2^1A_2^2B_2^1B_2^2}. \qquad (21)
\end{aligned}
$$

Different from the scheme in Section 3, Alice needs to perform a controlled-U_z (CU_z) operation on her qubits A_1^1 (A_2^1) and A_1^2 (A_2^2) using A_1^1 (A_2^1) as the control qubit and A_1^2 (A_2^2) as the target qubit, where the controlled-$U_z = |0\rangle\langle 0|\otimes I + |1\rangle\langle 1|\otimes\sigma_z$. Similarly, Bob also performs a CU_z operation on his qubits B_1^1 (B_2^1) and B_1^2 (B_2^2) using B_1^1 (B_2^1) as the control qubit and B_1^2 (B_2^2) as the target qubit. As a result, $|\Theta_r\rangle$ is transformed into

$$
\begin{aligned}
|\Lambda_{\rm r}\rangle \;=\; & \frac{1}{8\sqrt{2}}\{|0\rangle(|0\rangle+|1\rangle)|0\rangle(|0\rangle+|1\rangle)[|0\rangle(|0\rangle+|1\rangle)|0\rangle(|0\rangle+|1\rangle)-|1\rangle(|1\rangle+|0\rangle)|1\rangle(|1\rangle+|0\rangle)]\\
& -|0\rangle(|0\rangle+|1\rangle)|1\rangle(|1\rangle+|0\rangle)[|0\rangle(|0\rangle+|1\rangle)|1\rangle(|1\rangle+|0\rangle)-|1\rangle(|1\rangle+|0\rangle)|0\rangle(|0\rangle+|1\rangle)]\\
& +|1\rangle(|1\rangle+|0\rangle)|0\rangle(|0\rangle+|1\rangle)[|0\rangle(|0\rangle+|1\rangle)|1\rangle(|1\rangle+|0\rangle)+|1\rangle(|1\rangle+|0\rangle)|0\rangle(|0\rangle+|1\rangle)]\\
& +|1\rangle(|1\rangle+|0\rangle)|1\rangle(|1\rangle+|0\rangle)[|0\rangle(|0\rangle+|1\rangle)|0\rangle(|0\rangle+|1\rangle)+|1\rangle(|1\rangle+|0\rangle)|1\rangle(|1\rangle+|0\rangle)]\}_{A_1^1A_1^2B_1^1B_1^2A_2^1A_2^2B_2^1B_2^2}. \qquad (22)
\end{aligned}
$$

Lastly, Alice (Bob) performs X-basis measurements on her (his) qubits A_1^2 (B_1^2) and A_2^2 (B_2^2) respectively, and then $|\Lambda_{\rm r}\rangle$ will collapse into

$$
\begin{aligned}
& {}_{A_1^2}\langle +|_{B_1^2}\langle +|_{A_2^2}\langle +|_{B_2^2}\langle +|\Lambda_{\rm r}\rangle\\
=\; & \frac{1}{2\sqrt{2}}[|00\rangle(|00\rangle-|11\rangle)-|01\rangle(|01\rangle-|10\rangle)\\
& +|10\rangle(|01\rangle+|10\rangle)+|11\rangle(|00\rangle+|11\rangle)]_{A_1^1B_1^1A_2^1B_2^1}. \qquad (23)
\end{aligned}
$$

Apparently, three legitimate participants have succeeded in sharing $2N$ χ-type states. For convenience, we replace the original subscript $A_1^1B_1^1A_2^1B_2^1$ with $A_1B_1A_2B_2$.

Steps 5–8 These steps are the same as steps 5–8 in Section 3.

5. Security analysis

This section mainly analyzes why these two protocols designed by us can not only successfully eliminate the information leakage, but also resist against the intercept-and-resend attack, the entanglement-and-measure attack, the modification attack, the conspiring attack, and especially the dishonest controller's attacks.

5.1. Information leakage

The information leakage is that an eavesdropper Eve is able to obtain a part of classical information only from the public announcement without taking any active attacks. In these two protocols presented by us, the public information includes Charlie's permission as well as the transmitted classical bits m_A and m_B. For Charlie's permission, look back at the whole process, Charlie randomly performs the unitary operation $U_0^{\rm dp}$ or $U_1^{\rm dp}$ ($U_0^{\rm r}$ or $U_1^{\rm r}$) on each logical qubit A_2 in S_A to generate her permission. Because two unitary operations are chosen at random, it is obvious that Charlie's 1-bit ($-2\times\frac{1}{2}\log\frac{1}{2}$) permission information is secret before the permission is published in step 3. For $M_{{\rm sg}_A}$, if Alice announces $m_A=0$, there are always two possible cases: (1) $M_{{\rm sg}_A}$=0 and MR_A^2=0; (2) $M_{{\rm sg}_A}$=1 and MR_A^2=1. Because the probability of these two cases happening is equal, the information entropy of $M_{{\rm sg}_A}$ is $-2\times\frac{1}{2}\log\frac{1}{2}=1$, which is equal to the length of the secret message transmitted by Alice. Meanwhile, the similar thing happens to $M_{{\rm sg}_B}$ as well. This means that Eve and Charlie cannot obtain any information about the secret message without knowing MR_A^2 and MR_B^2. Therefore, our proposed protocols are immune to the information leakage.

5.2. Intercept-and-resend attack

The intercept-and-resend attack is that an eavesdropper Eve attempts to intercept all the transmitted qubits, replace them with new qubits, and send these new qubits to the receivers. Suppose that Eve intercepts all the qubits in Q_A and

sends a sequence of fake qubits to Alice in step 1. However, it is apparent that Eve is unaware of the positions and bases of checking qubits, which are generated by Charlie, thus she cannot always prepare the same checking qubits as the ones prepared by Charlie. Eve's fake qubits will introduce errors in the security check of step 2 with the probability $1-(\frac{3}{4})^n$, where n is the number of checking qubits. When n is large enough, the probability will be infinitely close to 1.

5.3. Entanglement-and-measure attack

The entanglement-and-measure attack is that an eavesdropper Eve seeks to employ her auxiliary qubits to entangle with the transmitted qubits, and implement corresponding measurements on the auxiliary qubits to obtain secret information. In the whole protocol, most likely Eve launches the entanglement-and-measure attack in the process of sending Q_A to Alice (Q_B to Bob) by Charlie in step 1. After performing an entanglement operation, the transmitted qubit and ancilla $|e\rangle$ will be entangled together. In the whole process, the checking qubits will be changed into

$$U_e|0_{\rm dp}\rangle|e\rangle = a|0_{\rm dp}\rangle|e_{00}\rangle+b|1_{\rm dp}\rangle|e_{01}\rangle, \tag{24}$$

$$U_e|1_{\rm dp}\rangle|e\rangle = c|0_{\rm dp}\rangle|e_{10}\rangle+d|1_{\rm dp}\rangle|e_{11}\rangle, \tag{25}$$

$$\begin{aligned}U_e|+_{\rm dp}\rangle|e\rangle =& \frac{1}{2\sqrt{2}}[|+_{\rm dp}\rangle(a|e_{00}\rangle+b|e_{01}\rangle+c|e_{10}\rangle+d|e_{11}\rangle)\\&+|-_{\rm dp}\rangle(a|e_{00}\rangle-b|e_{01}\rangle+c|e_{10}\rangle-d|e_{11}\rangle)],\end{aligned} \tag{26}$$

$$\begin{aligned}U_e|-_{\rm dp}\rangle|e\rangle =& \frac{1}{2\sqrt{2}}[|+_{\rm dp}\rangle(a|e_{00}\rangle+b|e_{01}\rangle-c|e_{10}\rangle-d|e_{11}\rangle)\\&+|-_{\rm dp}\rangle(a|e_{00}\rangle-b|e_{01}\rangle-c|e_{10}\rangle+d|e_{11}\rangle)],\end{aligned} \tag{27}$$

where $|e_{00}\rangle$, $|e_{01}\rangle$, $|e_{10}\rangle$ and $|e_{11}\rangle$ are four states Eve can distinguish, and $|a|^2+|b|^2=|c|^2+|d|^2=1$. For avoiding detection, Eve has to set $a=d=1$, $b=c=0$ and $(a|e_{00}\rangle-b|e_{01}\rangle+c|e_{10}\rangle-d|e_{11}\rangle)=(a|e_{00}\rangle+b|e_{01}\rangle-c|e_{10}\rangle-d|e_{11}\rangle)=\overrightarrow{0}$. Hence, it is easy to prove that $|e_{00}\rangle=|e_{11}\rangle$. In this case, Eve cannot distinguish $|e_{00}\rangle$ from $|e_{11}\rangle$, that is to say, she cannot obtain any useful information. Instead, if she wants to steal secret message, her operation will change the states of checking qubits so that her action will be detected in the public discussion between Charlie and Alice, or between Charlie and Bob. As a consequence, our proposed protocols are free from the entanglement-and-measure attack.

5.4. Modification attack

Eve intends to carry out a great deal of random unitary operations on the transmitted qubits sent to both Alice and Bob in step 1. If Eve can successfully change MR_A^1 from $|+\rangle$ to $|-\rangle$ or change MR_A^2 from $|+\rangle$ to $|-\rangle$, then Alice and Bob will not correctly extract the other's secret message. However, because the checking qubits are inserted in the qubit sequences in random, Eve has no knowledge of the positions of checking qubits. As a result, Eve's random operations will inevitably disturb the states of checking qubits so that she will be detected in the public discussion between Alice and Charlie.

5.5. Conspiring attack

Based on the deterministic entanglement correlation of χ-type states, Alice and Bob may conspire to communicate without Charlie's permission. However, in step 1, after Charlie performs a random unitary operation on A_2 in S_A, the logical χ-type states will be unexpectedly changed. To be specific, if Charlie performs $U_1^{\rm dp}$ on A_2 in S_A, the logical χ-type state will be converted into $|\chi_{\rm dp}\rangle=-\frac{1}{2}(|0_{\rm dp}0_{\rm dp}\rangle|\psi_{\rm dp}^+\rangle-|0_{\rm dp}1_{\rm dp}\rangle|\phi_{\rm dp}^+\rangle-|1_{\rm dp}0_{\rm dp}\rangle|\phi_{\rm dp}^-\rangle-|1_{\rm dp}1_{\rm dp}\rangle|\psi_{\rm dp}^-\rangle)_{A_1B_1A_2B_2}$. Further, in step 4, the logical χ-type state will collapse into

$$\begin{aligned}|v\rangle =& -\frac{1}{2}(|00\rangle|\psi^+\rangle-|01\rangle|\phi^+\rangle-|10\rangle|\phi^-\rangle\\&-|11\rangle|\psi^-\rangle)_{A_1B_1A_2B_2}\\=& -\frac{1}{2\sqrt{2}}[|00\rangle(|01\rangle+|10\rangle)-|01\rangle(|00\rangle+|11\rangle)\\&-|10\rangle(|00\rangle-|11\rangle)-|11\rangle(|01\rangle-|10\rangle)]_{A_1B_1A_2B_2}\\=& -\frac{1}{2}(|+-+1\rangle-|++-0\rangle+|-++-1\rangle\\&+|---+0\rangle)_{A_1B_1A_2B_2}.\end{aligned} \tag{28}$$

According to steps 6–8 in Section 3, Alice and Bob can deduce the other's measurement results, as shown in Table 2, and then decode some secret messages. Unfortunately, these secrets are exactly contrary to the other's real secret message. Take Bob as an example, we assume that his measurement results are $MR_B^1=0$ and $MR_B^2=0$. If Alice announces $m_A=0$, Bob can deduce $MR_A^2=0$ from his measurement results, and obtain $M_{{\rm sg}_A}=0$. But, if Charlie has performed the operation $U_1^{\rm dp}$ on A_2 in S_A, in fact Bob obtains the wrong message 1 rather than real message 0. In short, because of random unitary operations, Bob only obtains Alice's secret message with the probability $1/2$. In the same way, Alice also only obtains Bob's secret message with the probability $1/2$.

Table 2. Corresponding relationship between measurement outcomes of the χ-type state changed and decoding rules.

MR_A^1	MR_B^1	MR_A^2	MR_B^2
0 ($\|+\rangle$)	0 ($\|+\rangle$)	1 ($\|-\rangle$)	0 ($\|0\rangle$)
0 ($\|+\rangle$)	1 ($\|-\rangle$)	0 ($\|+\rangle$)	1 ($\|1\rangle$)
1 ($\|-\rangle$)	0 ($\|+\rangle$)	1 ($\|-\rangle$)	1 ($\|1\rangle$)
1 ($\|-\rangle$)	1 ($\|-\rangle$)	0 ($\|+\rangle$)	0 ($\|0\rangle$)

5.6. The dishonest controller's attacks

As described in Ref. [34], the controller has more initiative than the sender together with the receiver when checking

security. If the controller is dishonest, he/she will be more dangerous than external attackers. Hence, the CQD protocols are more vulnerable to attack initiated by the controller, such as the different-initial-state (DIS) attack and the denial-of-service (DoS) attack. The DIS attack means that the controller can steal participants' secret message by preparing the different initial states, while the DoS attack means that the controller can deliberately announce the wrong classical information so that one legitimate user will get the wrong message from the other. We intend to take the CQD protocol against collective-dephasing noise as an example to explain why our protocols can be against these two attacks effectively.

We explain why our protocols can resist against the DIS attack first. It is easy to verify that the set $\{Z_{A_1}^k X_{A_1}^l Z_{A_2}^m X_{A_2}^n |\chi\rangle_{A_1B_1A_2B_2} | k,l,m,n \in \{0,1\}\}$ makes up a standard orthogonal basis for the four-qubit Hilbert space, where $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$ and $X = |0\rangle\langle 1| + |1\rangle\langle 0|$. This means that every state in four-qubit Hilbert space can be expressed by the linear combination of these sixteen states. Without loss of generality, we assume that every initial logical state prepared by the dishonest controller in step 1 is $|\Omega_{\rm dp}\rangle$. $|\Omega_{\rm dp}\rangle$ is made up of a logical χ-type state and a probe, which are prepared by the dishonest controller. In particular, if $U_1^{\rm dp}$ is carried out in step 1, the state will collapse into $|\zeta\rangle_{A_1B_1A_2B_2C}$ ignoring the global phase factor (i.e., -1) in step 4. Therefore, $|\zeta\rangle_{A_1B_1A_2B_2C}$ can be expressed as

$$\begin{aligned} &|\zeta\rangle_{A_1B_1A_2B_2C} \\ &= \sum_{k,l,m,n=0}^{1} a_{klmn} (Z_{A_1}^k X_{A_1}^l Z_{A_2}^m X_{A_2}^n |\chi\rangle_{A_1B_1A_2B_2}) \otimes |e_{klmn}\rangle_C, \end{aligned} \tag{29}$$

where the probe in $\{|e_{klmn}\rangle_C\}$ stays in an ancillary Hilbert space controlled by controller, and $\sum_{klmn}^{1} |a_{klmn}|^2 = 1$. Note that the probe in $\{|e_{klmn}\rangle_C\}$ may be not orthogonal with each other.

Case 1 We take into account the situation that Bob decides that the four particles A_1, B_1, A_2 and B_2 from the same sample χ-type state are respectively measured by the X-basis, the X-basis, the X-basis and the Z-basis in the security check to the controller. Through the analysis of the deterministic entanglement correlation of these sixteen χ-type states, we find that there will be no error introduced by the dishonest controller if and only if $|\zeta\rangle_{A_1B_1A_2B_2C}$ can be expressed as

$$\begin{aligned} &|\zeta\rangle_{A_1B_1A_2B_2C} \\ &= a_{0000} Z_{A_1}^0 X_{A_1}^0 Z_{A_2}^0 X_{A_2}^0 |\chi\rangle_{A_1B_1A_2B_2} |e_{0000}\rangle_C \\ &\quad + a_{0001} Z_{A_1}^0 X_{A_1}^0 Z_{A_2}^0 X_{A_2}^1 |\chi\rangle_{A_1B_1A_2B_2} |e_{0001}\rangle_C \\ &\quad + a_{0100} Z_{A_1}^0 X_{A_1}^1 Z_{A_2}^0 X_{A_2}^0 |\chi\rangle_{A_1B_1A_2B_2} |e_{0100}\rangle_C \\ &\quad + a_{0101} Z_{A_1}^0 X_{A_1}^1 Z_{A_2}^0 X_{A_2}^1 |\chi\rangle_{A_1B_1A_2B_2} |e_{0101}\rangle_C \\ &= \frac{a_{0000}}{2} (|+++0\rangle + |---0\rangle + |+--1\rangle \\ &\quad - |-++1\rangle)_{A_1B_1A_2B_2} |e_{0000}\rangle_C \\ &\quad + \frac{a_{0001}}{2} (|+++0\rangle - |---0\rangle \\ &\quad - |+--1\rangle - |-++1\rangle)_{A_1B_1A_2B_2} |e_{0001}\rangle_C \\ &\quad + \frac{a_{0100}}{2} (|+++0\rangle - |---0\rangle \\ &\quad + |+--1\rangle + |-++1\rangle)_{A_1B_1A_2B_2} |e_{0100}\rangle_C \\ &\quad + \frac{a_{0101}}{2} (|+++0\rangle + |---0\rangle \\ &\quad - |+--1\rangle + |-++1\rangle)_{A_1B_1A_2B_2} |e_{0101}\rangle_C. \end{aligned} \tag{30}$$

Case 2 For the same sample χ-type state, we take into consideration another situation that Bob decides that the particles A_1 and A_2 are respectively measured by the Z-basis and the Z-basis, and the particles B_1 and B_2 are measured by the Bell basis in the security check to the controller. After analyzing the deterministic entanglement correlation of these sixteen χ-type states, we find out that there will be no error introduced by the dishonest controller if and only if $|\zeta\rangle_{A_1B_1A_2B_2C}$ can be expressed as

$$\begin{aligned} &|\zeta\rangle_{A_1B_1A_2B_2C} \\ &= a_{0000} Z_{A_1}^0 X_{A_1}^0 Z_{A_2}^0 X_{A_2}^0 |\chi\rangle_{A_1B_1A_2B_2} |e_{0000}\rangle_C \\ &\quad + a_{0010} Z_{A_1}^0 X_{A_1}^0 Z_{A_2}^1 X_{A_2}^0 |\chi\rangle_{A_1B_1A_2B_2} |e_{0010}\rangle_C \\ &\quad + a_{1000} Z_{A_1}^1 X_{A_1}^0 Z_{A_2}^0 X_{A_2}^0 |\chi\rangle_{A_1B_1A_2B_2} |e_{1000}\rangle_C \\ &\quad + a_{1010} Z_{A_1}^1 X_{A_1}^0 Z_{A_2}^1 X_{A_2}^0 |\chi\rangle_{A_1B_1A_2B_2} |e_{1010}\rangle_C \\ &= \frac{a_{0000}}{2} (|00\rangle|\phi^-\rangle - |01\rangle|\psi^-\rangle + |10\rangle|\psi^+\rangle \\ &\quad + |11\rangle|\phi^+\rangle)_{A_1A_2B_1B_2} |e_{0000}\rangle_C \\ &\quad + \frac{a_{0010}}{2} (|00\rangle|\phi^-\rangle + |01\rangle|\psi^-\rangle \\ &\quad + |10\rangle|\psi^+\rangle - |11\rangle|\phi^+\rangle)_{A_1A_2B_1B_2} |e_{0010}\rangle_C \\ &\quad + \frac{a_{1000}}{2} (|00\rangle|\phi^-\rangle - |01\rangle|\psi^-\rangle - |10\rangle|\psi^+\rangle \\ &\quad - |11\rangle|\phi^+\rangle)_{A_1A_2B_1B_2} |e_{1000}\rangle_C \\ &\quad + \frac{a_{1010}}{2} (|00\rangle|\phi^-\rangle + |01\rangle|\psi^-\rangle - |10\rangle|\psi^+\rangle \\ &\quad + |11\rangle|\phi^+\rangle)_{A_1A_2B_1B_2} |e_{1010}\rangle_C. \end{aligned} \tag{31}$$

Compared Eq. (30) with Eq. (31), it is easy to find that there is only one choice

$$|\zeta\rangle_{A_1B_1A_2B_2C} = a_{0000} Z_{A_1}^0 X_{A_1}^0 Z_{A_2}^0 X_{A_2}^0 |\chi\rangle_{A_1B_1A_2B_2} |e_{0000}\rangle_C, \tag{32}$$

if no error occurs in both cases 1 and 2. Notice that, in step 4, the initial state prepared by the controller will collapse into a product state of a true four-particle χ-type state $|\chi\rangle_{A_1B_1A_2B_2}$ and an ancilla $|e_{0000}\rangle_C$. This means that the dishonest controller cannot pass through the security check in step 5. Consequently, our protocols can be perfectly immune to the DIS attack from the dishonest controller.

Secondly, for the DoS attack, we can find that it can be viewed as a special case of the DIS attack in our protocols. In step 1, Charlie prepares the logical χ-type states $|\chi_{\rm dp}\rangle$, randomly performs the unitary operations $U_0^{\rm dp}$ or $U_1^{\rm dp}$ on the logical qubits A_2 in S_A and records these operations as her permission. Suppose that Charlie publishes the wrong permission contrary to the real permission, Alice will perform the unitary operations corresponding to the wrong permission in step 3. As a result, the logical χ-type state $|\chi_{\rm dp}\rangle$ will collapse into $Z_{A_1}^0 X_{A_1}^0 Z_{A_2}^1 X_{A_2}^1 |\chi\rangle_{A_1B_1A_2B_2}$ in step 4. Apparently, this case is equivalent to the one that Charlie prepares the different initial states but abides by the following steps honestly. From this point of view, the DoS attack can indeed be regarded as a special case of the DIS attack in our proposed protocols. As described above, the security check to the controller can effectively prevent the dishonest controller from taking the DIS attack. Therefore, our protocols are safe against the DoS attack as well.

6. Comparisons

In order to evaluate the performance of our protocols synthetically, this section objectively compares them with previous CQD protocols in terms of some important indicators, such as quantum resource, the conspiring attack, the dishonest controller's attacks, the information leakage, controller's online waiting, collective noise environment, and qubit efficiency. The concrete parameters are summarized in Table 3.

Table 3. Comparison between ours and previous CQD protocols.

	[27]	[28]	[32]	[33]	[34]	Our protocols
Quantum resource	Brown states	GHZ states	GHZ states Bell states	Cluster states	Cluster states	Logical χ-type states
Resist collective noise	No	No	No	No	No	Yes
Resist conspiring attack	No	No	Yes	Yes	Yes	Yes
Resist dishonest controller's attacks	No	No	No	No	Yes	Yes
Resist information leakage	No	No	Yes	Yes	Yes	Yes
Controller's online waiting	Yes	Yes	Yes	No	No	No
Qubit efficiency	61.5%	28%	10.5%	25%	12.5%	6.25%

As shown in Table 3, it is obvious that our protocols own better performance than previous protocols:

(i) For quantum resources, the χ-type state is used as quantum channels in our protocols. It possesses better entanglement properties than others employed in previous protocols, which is illustrated in Ref. [43].

(ii) For resisting collective noise, to be obvious, our protocols can be perfectly immune to both collective-dephasing noise and collective-rotation noise, while the others can not.

(iii) For two new attacks which are given special attention, the conspiring attack and the dishonest controller's attacks, our protocols and the protocol in Ref. [34] are capable of resisting both attacks, while the ones in Refs. [27,28,32,33] cannot resist these two attacks at the same time.

(iv) For the information leakage, compared with the protocols of Refs. [27,28], our protocols can be free from the information leakage, which is the same as the ones in Refs. [32–34].

(v) For controller's online waiting problem, similar to the protocols in Refs. [33,34], in our protocols the controller can be offline after quantum distribution and permission announcement, without waiting for all the participants to complete the information coding. As a result the waiting time of the controller will be effectively reduced.

(vi) For qubit efficiency, intuitively the qubit efficiency of our protocols is lower than that of others. In fact, the richer functionality than others leads to the lower efficiency. It is noteworthy that the qubit efficiency of the protocol in Ref. [34], which is the most similar to our protocols, will be the same as our protocols when it is improved to be against collective noise. The qubit efficiency is defined as $\eta = m/q$, where m denotes the number of secret bits and q denotes the total number of required qubits.

7. Conclusion

In summary, in order to eliminate the disturbance from the external environment, we put forward two controlled quantum dialogue protocols against collective noise, which are against collective-dephasing noise and collective-rotation noise, respectively. Based on the comprehensive and objective evaluation on the performance, it is easy to find out that our protocols are superior to most existing protocols. Especially, it needs to emphasize that not only two kinds of logical χ-type states are constructed by us in theory to be against collective noise, but also our protocols can effectively resist against both the conspiring attack and the dishonest controller's attacks, which are attracting special attention of researchers recently.

Finally, we should keep trying to seek an answer for how

to design the controlled quantum dialogue protocols satisfying the demands of society better.

References

[1] Grover L K 1997 *Phys. Rev. Lett.* **79** 325
[2] Shor P W 1999 *SIAM Rev.* **41** 303
[3] Zhang H, Guo X X and Xiang S Y 2018 *Acta Phys. Sin.* **67** 204202 (in Chinese)
[4] Zhu K N, Zhou N R, Wang Y Q and Wen X J 2018 *Int. J. Theor. Phys.* **57** 3621
[5] Zhou N R, Zhu K N and Zou X F 2019 *Ann. Phys.* **531** 1800520
[6] Deng F G, Long G L and Liu X S 2003 *Phys. Rev. A* **68** 042317
[7] Zhao X L, Li J L, Niu P H, Ma H Y and Ruan D 2017 *Chin. Phys. B* **26** 030302
[8] Zheng X Y and Long Y X 2019 *Quantum Inf. Process.* **18** 129
[9] Du Y T and Bao W S 2018 *Chin. Phys. B* **27** 080304
[10] Yang Y G, Gao S, Li D, Zhou Y H and Shi W M 2019 *Quantum Inf. Process.* **18** 215
[11] Luo G F, Zhou R G and Hu W W 2019 *Chin. Phys. B* **28** 040302
[12] Sisodia M, Verma V, Thapliyal K and Pathak A 2017 *Quantum Inf. Process.* **16** 76
[13] Yang G, Lian B W, Nie M and Jin J 2017 *Chin. Phys. B* **26** 040305
[14] Chang L W, Zheng S H, Gu L Z, Xiao D and Yang Y X 2014 *Chin. Phys. B* **23** 090307
[15] Chang L W, Zheng S H, Gu L Z, Jin L and Yang Y X 2015 *Int. J. Theor. Phys.* **54** 2864
[16] Feng Y Y, Shi R H and Guo Y 2018 *Chin. Phys. B* **27** 020302
[17] Zhang W and Han Z F 2019 *Acta Phys. Sin.* **68** 070301 (in Chinese)
[18] Nguyen B A 2004 *Phys. Lett. A* **328** 6
[19] Xiao M, Cao Y R and Song X L 2017 *Chin. Phys. Lett.* **34** 030302
[20] Gong L H, Li J F and Zhou N R 2018 *Laser. Phys. Lett.* **15** 105204
[21] Ye T Y and Ye C Q 2018 *Int. J. Theor. Phys.* **57** 1440
[22] Qi J M, Xu G, Chen X B, Wang T Y, Cai X Q and Yang Y X 2018 *Quantum Inf. Process.* **17** 247
[23] Cao G and Jiang M 2019 *Int. J. Syst. Control Inf. Process.* **3** 26
[24] Zhang M H, Cao Z W, Peng J Y and Chai G 2019 *Eur. Phys. J. D* **73** 57
[25] Zhang M H, Peng J Y and Cao Z W 2019 *Mod. Phys. Lett. B* **33** 1950033
[26] Man Z X and Xia Y J 2006 *Chin. Phys. Lett.* **23** 1680
[27] Yang Y F, Ye Z Q and Tu C L 2013 *Acta Photon. Sin.* **42** 1305
[28] Ye T Y and Jiang L Z 2013 *Chin. Phys. Lett.* **30** 040305
[29] Liu Z H and Chen H W 2013 *Chin. Phys. Lett.* **30** 079901
[30] Ye T Y and Jiang L Z 2013 *Chin. Phys. Lett.* **30** 079902
[31] Chang C H, Luo Y P, Yang C W and Hwang T 2015 *Quantum Inf. Process.* **14** 3515
[32] Kao S H and Hwang T 2016 *Quantum Inf. Process.* **15** 4313
[33] Kao S H and Hwang T 2017 *Quantum Inf. Process.* **16** 139
[34] Liu Z H and Chen H W 2019 *Quantum Inf. Process.* **18** 98
[35] Yang C W and Hwang T 2013 *Quantum Inf. Process.* **12** 2131
[36] Ye T Y 2015 *Sci. Sin. Phys. Mech. Astron.* **45** 030301
[37] Ye T Y 2015 *Quantum Inf. Process.* **14** 3499
[38] Ye T Y 2015 *Sci. Chin.-Phys. Mech. Astron.* **58** 1
[39] Chang C H, Yang C W, Hzu G R, Hwang T and Kao S H 2016 *Quantum Inf. Process.* **15** 2971
[40] Xiao M and Liu G 2018 *Chin. J. Electron.* **27** 263
[41] Lang Y F 2019 *Int. J. Theor. Phys.* **58** 531
[42] Yang Y G, Gao S, Zhou Y H and Shi W M 2019 *Int. J. Theor. Phys.* **58** 2810
[43] Yeo Y and Chua W K 2006 *Phys. Rev. Lett.* **96** 060502
[44] Shi Y L, Mei F, Yu Y F, Feng X L and Zhang Z M 2012 *Quantum Inf. Process.* **11** 229
[45] Dong L, Xiu X M, Gao Y J and Yi X X 2013 *Quantum Inf. Process.* **12** 1787
[46] Guo Y B, Wang G Z and Jiang N Q 2014 *Int. J. Theor. Phys.* **53** 3135
[47] Leng C L, Zhang Y Q and Ji X 2015 *Acta Phys. Sin.* **64** 184207 (in Chinese)
[48] Liu W, Wang Y B, Jiang Z T and Cao Y Z 2012 *Int. J. Theor. Phys.* **51** 69
[49] Kang S Y, Chen X B and Yang Y X 2014 *Quantum Inf. Process.* **13** 2081
[50] Dong L, Wang J X, Li Q Y, Dong H K, Xiu X M and Gao Y J 2016 *Quantum Inf. Process.* **15** 2955
[51] Xu S J, Chen X B, Wang L H, Ding Q Y and Zhang S H 2016 *Commun. Theor. Phys.* **65** 705
[52] Tan X Q, Zhang X Q and Song T T 2017 *Comput. Stand. Interfaces* **54** 36
[53] Yang X, Bai M Q, Zuo Z C and Mo Z W 2018 *Quantum Inf. Process.* **17** 261
[54] Long G L and Liu X S 2002 *Phys. Rev. A* **65** 032302