

## Applying a class of general maximally entangled states in measurement-device-independent quantum secure direct communication

Jianfeng Liu,<sup>1</sup> Xiangfu Zou<sup>1,\*</sup>, Xin Wang,<sup>2,3,†</sup> Ying Chen,<sup>1</sup> Zhenbang Rong,<sup>4</sup> Zhiming Huang,<sup>5</sup> Shenggen Zheng,<sup>6</sup> Xueying Liang,<sup>1</sup> and Jianxiong Wu<sup>1</sup>

<sup>1</sup>*School of Mathematics and Computational Science, Wuyi University, Jiangmen 529020, China*


<sup>2</sup>*Department of Physics, City University of Hong Kong, Tat Chee Avenue, Kowloon, Hong Kong SAR, China*

<sup>3</sup>*City University of Hong Kong Shenzhen Research Institute, Shenzhen 518057, China*

<sup>4</sup>*School of Electronics and Information Engineering, Wuyi University, Jiangmen 529020, China*

<sup>5</sup>*School of Economics and Management, Wuyi University, Jiangmen 529020, China*

<sup>6</sup>*Quantum Science Center of Guangdong-Hong Kong-Macao Greater Bay Area (Guangdong), Shenzhen 518045, China*

 (Received 16 June 2023; revised 7 January 2024; accepted 14 March 2024; published 4 April 2024)

Quantum entanglement is a fundamental physical resource that enables a range of information-processing tasks with no efficient solution on classical computers. In this paper, we construct a class of general maximum entangled states by parameterizing the coefficients of Bell states. By calculating, we obtain the local unitary operations required to realize the mutual transformation of the constructed states, analogous to Pauli operators acting on one particle of a Bell state. Interestingly, the local unitary operations on the two particles of Bell states are identical, whereas for the constructed states, they must differ in certain cases. To explore the potential applications of these maximum entangled states and the obtained local unitary operations, we design a class of measurement-device-independent quantum secure direct communication protocols based on entanglement swapping. In the class of designed protocols, entanglement swapping is realized between a constructed maximum entangled state and a Bell state. We demonstrate that the class of designed protocols have no information leakage and can resist intercept-and-resend attacks, measure-resend attacks, and collective attacks. In addition, the unconditional security of the class of designed protocols is proved. We believe that the constructed maximum entangled states and the obtained local unitary operations may find applications in other quantum information-processing fields.

DOI: [10.1103/PhysRevApplied.21.044010](https://doi.org/10.1103/PhysRevApplied.21.044010)

### I. INTRODUCTION

Quantum information processing has more advantages in security and efficiency than classical information processing, because it can use quantum entanglement. Entanglement is a unique quantum mechanical resource that plays a key role in many of the most interesting applications of quantum computation and quantum information. In 1935, Einstein, Podolsky, and Rosen [1] put forward the definition of *entanglement*. They questioned the completeness of quantum mechanics. Subsequently, Schrödinger [2] introduced the term *quantum entanglement*, and also proposed the famous thought experiment we call it *Schrödinger's cat*. In 1964, Bell [3] transformed the discussion of whether quantum mechanics is complete into an experimentally testable proposition and proposed

a famous inequality that we call *Bell inequality*. Since then, many physicists designed experiments to test the Bell inequality, and obtained experimental data to show that the Bell inequality is violated [4–6]. In 1972, Clauser and Freedman [4] observed the Bell inequality being violated by performing experiment with exciting calcium atoms. To conquer the weakness that the setting of Alice's polarizer could influence Bob's polarizer in the experiment above, Aspect *et al.* [5] completed their Bell test by randomly changing the direction of the polarizer. In 2015, using random number generators, Zeilinger *et al.* [6] separated the setting choices, measurements, and emission events to close the locality loophole [4] and the freedom-of-choice loophole [5], simultaneously. In addition, Zeilinger *et al.* [7,8] realized a quantum teleportation experiment and a quantum entanglement swapping experiment. Nowadays, the quantum entanglement has been used as a key resource in quantum key distribution (QKD) [9], quantum secure direct communication (QSDC) [10–13], quantum

\*Corresponding authors. [xf.zou@hotmail.com](mailto:xf.zou@hotmail.com)

†[x.wang@cityu.edu.hk](mailto:x.wang@cityu.edu.hk)

dense coding [14], quantum teleportation [7,15], quantum algorithm [16,17], and quantum computer systems [18]. To enrich the knowledge of quantum entanglement, in this paper, we will construct four maximum entangled states by parameterizing the coefficients of Bell states, and explore their properties and applications.

With the rapid development of quantum entanglement research, quantum information has been widely studied. QKD is a key branch of quantum information. It allows two parties to share a secret key by quantum technology. In 1984, Bennett and Brassard [19] proposed a QKD protocol, which is known as BB84 protocol. In 1992, Bennett [20] proposed a QKD protocol based on two nonorthogonal states. In principle, QKD has unconditional security under ideal equipment conditions [21–23]. There would be significant differences if we assess the security level of QKD based on the actual implementation or the idealized, theoretical description [24]. For instance, both Alice's error in signal coding and the features of detectors not taken into account in the theoretical analysis affect the security of real-life QKD protocols. Device-independent QKD (DIQKD) [24] aims at closing the gap between theoretical analyses and practical realizations of QKD by designing protocols whose security does not require a detailed characterization of the devices. Lo *et al.* [25] proposed the idea of measurement-device-independent QKD (MDIQKD) and constructed an MDIQKD protocol, which has excellent security and performance. The MDIQKD is a solution to remove all detector side-channel attacks, which may be the most critical part in the implementation process [25]. In the MDIQKD protocol, though the quantum source is prepared by authentic communicating parties, all the measurements of quantum states are performed by a third party. The third party can be untrusted, or even an eavesdropper. Thus, all loopholes in the measurement devices will be eliminated. In 2014, Curty *et al.* [26] proved the security of MDIQKD in the finite-key regime against general attacks and demonstrated that, even with practical signals and a finite size of data, it is possible to perform secure MDIQKD over long distances.

Another branch of quantum information is QSDC, which was proposed by Long *et al.* [10–13]. Long and Liu [10] used the QSDC technology to transfer secret keys. Refs. [11,12] constructed two useful QSDC protocols, where the protocol [11] is based on EPR pairs while the protocol [12] is based on single photons. In addition, Long *et al.* [13] summarized the early work and clarified the concept of QSDC. The QSDC transmits confidential messages directly in the quantum channel without the need for a secret classical key. It cannot only sense eavesdropping, but also make eavesdroppers unable to obtain any useful information. Now, many researchers have studied it, and developed a variety of theoretical protocols and their applications. In the two-step QSDC protocol [11], secret

information is encoded by the dense coding operation. In 2005, QSDC with high-dimensional quantum dense coding was proposed [27], which realizes the characteristics of high security and high capacity. Note that, the two-step QSDC protocol [11] is easier to generalize than the above protocol and has been developed into a bidirectional quantum secure direct communication (BQSDC) protocol [28]. In 2022, Sheng *et al.* [29] proposed a one-step QSDC protocol, which requires only distribution of polarization-spatial-mode hyperentanglement states. In recent years, QSDC has developed rapidly in theories [30–32] and experiments [33–37].

In 2018, Niu *et al.* [38] proposed a measurement-device-independent quantum secure direct communication (MDIQSDC) protocol. In an MDIQSDC protocol, all the measurements of quantum states during a communication are performed by an untrusted, or even an eavesdropper, third party. Thus, all loopholes in the measurement devices will be eliminated. In addition, the MDI technique can almost double the communication distance cover by those conventional QSDC protocols. In 2019, Gao *et al.* [39] proposed a long-distance MDIQSDC protocol. The secure distance is increased by using ancillary entangled photon-pair sources and relay nodes. In 2020, Zhou *et al.* [40] proposed a device-independent quantum secure direct communication (DIQSDC) protocol. They showed that the DIQSDC protocol can be implemented in noisy environments. They also used entanglement purification and noise-free linear amplification to extend the safe communication distance of DIQSDC. After that, scholars carried out further research on DIQSDC [41–43]. In the same year, Zhou *et al.* [44] proposed an MDIQSDC protocol with sequences of entangled photon pairs and single photons. Wu *et al.* [45] proposed a high-capacity MDIQSDC protocol by encoding secure information in the polarization and spatial-mode degrees of freedom of photons. With this encoding, they can double the channel capacity of the photons and effectively improve the communication efficiency of the MDIQSDC. In 2022, Das [46] put forward an MDIQSDC protocol with user identity authentication, where both the sender and the receiver first check the authenticity of the other party and then exchange the secret message. In the same year, Ying *et al.* [47] proposed two MDI one-step QSDC protocols, which can resist all possible attacks from imperfect measurement devices.

From the above analysis, it is found that entanglement states play a key role in the field of quantum information. In particular, the Bell states play a crucial role in the fields of QKD and QSDC. The Bell states are very special entangled states of two particles. Their preparation and measurement have strict requirements. How to reduce these requirements has scientific value, such as helping us to understand entangled states and their roles in the field of quantum information. More specifically, whether it is

possible to design more general entangled states that are less demanding than Bell states, but can replace Bell states in many fields of quantum information, is an interesting question. In this paper, we will construct four maximum entangled states, by parameterizing the coefficients of Bell states. We eliminate the requirement that the coefficients in the Bell state be real numbers. Compared to the Bell states, the constructed states are more general. To realize the mutual transformation of the constructed four states, as that Pauli operators acting on one particle of a Bell state, we will explore local unitary operations for the constructed four states, also. By calculation, we obtain two types of generalized Pauli operators. In fact, the Bell states are the special cases of the constructed states meanwhile Pauli operators are the special cases of the two types of generalized Pauli operators.

The QSDC can transmit confidential messages directly in the quantum channel without the need for a secret classical key. In practice, measurement devices are not always completely reliable. MDIQSDC can eliminate all loopholes in the measurement devices. Therefore, MDIQSDC has attracted the interest of many scholars. Note that, all existing MDIQSDC protocols [38,39,44–47] are using some special entangled states. It is a very interesting issue to design a class of MDIQSDC protocols that can obtain different protocols when its parameters take different values. To explore the applications of the constructed maximum entangled states and the obtained local unitary operations, we will design a class of MDIQSDC protocols, with the entanglement swapping between a constructed maximum entangled state and a Bell state. Note that, the MDIQSDC protocol in Ref. [38] is a special instance of the class of designed MDIQSDC protocols. Furthermore, we will show that the class of designed MDIQSDC protocols have no information leakage problem, and can resist intercept-and-resend attacks, measure-resend attacks and collective attacks. In addition, the unconditional security of the class of designed protocols is proved. Therefore, the unconditional security of the MDIQSDC protocol in Ref. [38] can be obtained naturally.

The rest of this paper is organized as follows. We will introduce some preparatory knowledge about Bell states and Pauli operations in Sec. II. In Sec. III, we will construct a class of general maximum entangled states and obtain local unitary operations to realize the mutual transformation of the four states as that of Pauli operators acting on one particle of Bell states. In Sec. IV, a class of MDIQSDC protocols, using the constructed maximum entangled states, the obtained local operations, and the constructed entanglement swapping, will be designed. Section V will analysis the security of the class of designed MDIQSDC protocols under some known attacks. Section VI will prove the unconditional security of the class of designed MDIQSDC protocols. We will summarize our works in Sec. VII.

## II. PRELIMINARIES

In order to better understand the constructed maximum entangled states in the following section, we review some knowledge about Bell states and Pauli operations.

The class of maximum entangled two-particle states,

$$|\beta_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad (1)$$

$$|\beta_1\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \quad (2)$$

$$|\beta_2\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \quad (3)$$

$$|\beta_3\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle), \quad (4)$$

are called EPR states, in honor of Einstein, Podolsky, and Rosen who pointed out the magical properties about the states [1]. After the proposition of the Bell inequality [3], EPR states are also called Bell states.

On the other hand, for two single-particle states  $|x\rangle$  and  $|y\rangle$ , where  $|x\rangle, |y\rangle \in \{|0\rangle, |1\rangle\}$  or  $\{|+\rangle, |-\rangle\}$ , and  $|+\rangle = 1/\sqrt{2}(|0\rangle + |1\rangle)$ ,  $|-\rangle = 1/\sqrt{2}(|0\rangle - |1\rangle)$ . The state  $|x\rangle \otimes |y\rangle$  can be presented by a linear combination of two Bell states as

$$|00\rangle = \frac{1}{\sqrt{2}}(|\beta_0\rangle + |\beta_1\rangle), \quad (5)$$

$$|11\rangle = \frac{1}{\sqrt{2}}(|\beta_0\rangle - |\beta_1\rangle), \quad (6)$$

$$|01\rangle = \frac{1}{\sqrt{2}}(|\beta_2\rangle + |\beta_3\rangle), \quad (7)$$

$$|10\rangle = \frac{1}{\sqrt{2}}(|\beta_2\rangle - |\beta_3\rangle), \quad (8)$$

$$|++\rangle = \frac{1}{\sqrt{2}}(|\beta_0\rangle + |\beta_2\rangle), \quad (9)$$

$$|--\rangle = \frac{1}{\sqrt{2}}(|\beta_0\rangle - |\beta_2\rangle), \quad (10)$$

$$|-\rangle = \frac{1}{\sqrt{2}}(|\beta_1\rangle + |\beta_3\rangle), \quad (11)$$

$$|+-\rangle = \frac{1}{\sqrt{2}}(|\beta_1\rangle - |\beta_3\rangle). \quad (12)$$

The matrices,  $\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ ,  $\sigma_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ ,  $\sigma_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ , and  $\sigma_3 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ , are called Pauli matrices [48], which were named after the physicist Pauli. Pauli matrices can be considered as operators with respect to the orthogonal basis  $\{|0\rangle, |1\rangle\}$  for a two-dimensional Hilbert space, i.e., Pauli operators.

The Pauli operators can realize the mutual transformation of Bell states by acting on one particle of a Bell state

as

$$\sigma_0:|\beta_0\rangle \mapsto |\beta_0\rangle,|\beta_1\rangle \mapsto |\beta_1\rangle,|\beta_2\rangle \mapsto |\beta_2\rangle,|\beta_3\rangle \mapsto |\beta_3\rangle; \quad (13)$$

$$\sigma_1:|\beta_0\rangle \mapsto |\beta_1\rangle,|\beta_1\rangle \mapsto |\beta_0\rangle,|\beta_2\rangle \mapsto |\beta_3\rangle,|\beta_3\rangle \mapsto |\beta_2\rangle; \quad (14)$$

$$\sigma_2:|\beta_0\rangle \mapsto |\beta_2\rangle,|\beta_1\rangle \mapsto |\beta_3\rangle,|\beta_2\rangle \mapsto |\beta_0\rangle,|\beta_3\rangle \mapsto |\beta_1\rangle; \quad (15)$$

$$\mathbf{i}\sigma_3:|\beta_0\rangle \mapsto |\beta_3\rangle,|\beta_1\rangle \mapsto |\beta_2\rangle,|\beta_2\rangle \mapsto |\beta_1\rangle,|\beta_3\rangle \mapsto |\beta_0\rangle. \quad (16)$$

### III. A CLASS OF GENERAL MAXIMUM ENTANGLED STATES

In this section, we construct four maximum entangled states by parameterizing the coefficients of Bell states and explore local unitary operations to realize the mutual transformation of the four states as that of Pauli operators acting on one particle of a Bell state.

First, we parameterize the coefficients of Bell states to construct four maximum entangled states as follows:

$$\begin{aligned} |\alpha_0\rangle &= a|00\rangle_{AB} + b|11\rangle_{AB}, |\alpha_1\rangle = \bar{b}|00\rangle_{AB} - \bar{a}|11\rangle_{AB}, \\ |\alpha_2\rangle &= a|01\rangle_{AB} + b|10\rangle_{AB}, |\alpha_3\rangle = \bar{b}|01\rangle_{AB} - \bar{a}|10\rangle_{AB}, \end{aligned} \quad (17)$$

where  $a$  and  $b$  are two complex numbers with  $|a| = |b| = 1/\sqrt{2}$ ,  $\bar{a}$  and  $\bar{b}$  the conjugate complex numbers of  $a$  and  $b$ , respectively. Obviously, the four constructed general maximum entangled states are maximum entangled states. When both  $a$  and  $b$  are real numbers, the four constructed general maximum entangled states are the Bell states. Note that, there are constructed general maximum entangled states being not Bell states. For example,  $\mathbf{i}/\sqrt{2}|00\rangle_{AB} + (1 + \mathbf{i})/2|11\rangle_{AB}$  is a constructed general maximum entangled state but not a Bell state. Easy to verify, the four states are mutually orthogonal and maximally entangled. Since for any  $i, j \in \{0, 1, 2, 3\}$  with  $i \neq j$ ,  $\langle \alpha_i | \alpha_j \rangle = 0$  and  $\|\alpha_i\| = \|\alpha_j\| = 1$ , the four entangled states are mutually orthogonal unit vectors. Therefore, the four states constitute a basis of the Hilbert space of two particles. Quantitatively, the entanglement measure of pure state  $|\Upsilon\rangle$  in the Hilbert space  $\mathcal{H}_A \otimes \mathcal{H}_B$  is conveniently by its entropy of entanglement [49] as

$$E(|\Upsilon\rangle) = S(\rho_A) = S(\rho_B), \quad (18)$$

i.e., the apparent entropy of either subsystem considered alone, where  $\rho_A = \text{Tr}_B|\Upsilon\rangle\langle\Upsilon|$ ,  $\rho_B = \text{Tr}_A|\Upsilon\rangle\langle\Upsilon|$ , and the von Neumann entropy  $S(\rho) = -\text{Tr}\rho \log \rho$ . The quantity  $E(|\Upsilon\rangle)$  ranges from zero to  $\log N$  for an entangled state of  $N$  particles. When  $E(|\Upsilon\rangle) = \log N$ ,  $|\Upsilon\rangle$  is a maximum entangled state. In particular, a two-particle state  $|\Upsilon\rangle$  is

TABLE I. The local unitary operations on the first particle and the second particle.

Unitary operations on the first particle	Unitary operations on the second particle
$U_0^A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$U_0^B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
$U_1^A = 2\bar{a}\bar{b}e^{i\theta_0} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$U_1^B = 2\bar{a}\bar{b}e^{i\theta'_0} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
$U_2^A = e^{i\theta_4} \begin{pmatrix} 0 & 2\bar{a}\bar{b} \\ 2\bar{a}\bar{b} & 0 \end{pmatrix}$	$U_2^B = e^{i\theta'_4} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
$U_3^A = e^{i\theta_8} \begin{pmatrix} 0 & 2\bar{b}^2 \\ -2\bar{a}^2 & 0 \end{pmatrix}$	$U_3^B = 2\bar{a}\bar{b}e^{i\theta'_8} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

a maximum entangled state if and only if  $E(|\Upsilon\rangle) = 1$ . Taking  $|\alpha_0\rangle$  as an example, we have

$$\begin{aligned} \rho_A &= \text{Tr}_B(|\alpha_0\rangle\langle\alpha_0|) \\ &= |a|^2|0\rangle\langle 0| + |b|^2|1\rangle\langle 1| = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|, \end{aligned} \quad (19)$$

and

$$E(|\alpha_0\rangle) = S(\rho_A) = -|a|^2 \log|a|^2 - |b|^2 \log|b|^2 = 1. \quad (20)$$

Similarly,  $E(|\alpha_1\rangle) = E(|\alpha_2\rangle) = E(|\alpha_3\rangle) = 1$ . As a result,  $|\alpha_0\rangle$ ,  $|\alpha_1\rangle$ ,  $|\alpha_2\rangle$ , and  $|\alpha_3\rangle$  are maximum entangled states.

In order to realize the mutual transformation of the four constructed general maximum entangled states, the local unit operations of the first and second particles are constructed (see Appendix A for details). For convenience, we list all local unitary operations we obtained in Table I, and refer to the constructed general maximum entangled states,  $|\alpha_0\rangle$ ,  $|\alpha_1\rangle$ ,  $|\alpha_2\rangle$ , and  $|\alpha_3\rangle$ , as the generalized Bell states (GBell states),  $\{U_0^A, U_1^A, U_2^A, U_3^A\}$  and  $\{U_0^B, U_1^B, U_2^B, U_3^B\}$  as two types of generalized Pauli operations.

From Table I, it can be found that, in general,  $U_2^A \neq U_2^B$  and  $U_3^A \neq U_3^B$ . In particular, when  $a = \pm b = \pm 1/\sqrt{2}$ ,  $U_1^A = c_1 U_1^B$ ,  $U_2^A = c_2 U_2^B$ , and  $U_3^A = c_3 U_3^B$ , where  $c_1$ ,  $c_2$ , and  $c_3$  are complex numbers with modulus 1, and the four GBell states are the four Bell states. Therefore, Bell states are the special cases of the GBell states, and Pauli operators are the special cases of the two types of generalized Pauli operators. Furthermore, when  $a = \pm b = \pm 1/\sqrt{2}$ ,  $e^{i\theta_0} = e^{i\theta'_0} = 1/2\bar{a}\bar{b}$ ,  $e^{i\theta_4} = e^{i\theta'_4} = 1$ , and  $e^{i\theta_8} = e^{i\theta'_8} = 1/2\bar{a}\bar{b}$ , the two types of generalized Pauli operations obtained are the corresponding Pauli operators.

Note that, the global phase factors of quantum states are unobservable. Therefore, we can ignore the global phase factors of quantum states. Similarly, we



can ignore the global phase shifts of unitary operations. Thereafter, for simplicity, in the local unitary operations, we ignore some global phase shifts, i.e.,  $U_0^A = U_0^B = \sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ ,  $U_1^A = U_1^B = \sigma_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ ,  $U_2^A = \begin{pmatrix} 0 & 2ab \\ 2\bar{a}\bar{b} & 0 \end{pmatrix}$ ,  $U_2^B = \sigma_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ ,  $U_3^A = \begin{pmatrix} 0 & 2\bar{b}^2 \\ -2\bar{a}^2 & 0 \end{pmatrix}$ , and  $U_3^B = \sigma_3 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ .

#### IV. MEASUREMENT-DEVICE-INDEPENDENT QUANTUM SECURE DIRECT COMMUNICATION USING THE GBELL STATES

In this section, we use the GBell states, the two types of generalized Pauli operators obtained, and the entanglement swapping between a GBell state and a Bell state to design a class of MDIQSDC protocols. The entanglement swapping between a GBell state and a Bell state can be described as (the construction process of the entanglement swapping between a GBell state and a Bell state is detailed in Appendix B)

$$|\alpha_2\rangle_{13} \otimes |\beta_2\rangle_{24} = \frac{1}{2}|\alpha_0\rangle_{12}|\beta_0\rangle_{12} - ab|\alpha_1\rangle_{12}|\beta_1\rangle_{12} + \frac{1}{2}|\alpha_2\rangle_{12}|\beta_2\rangle_{12} - ab|\alpha_3\rangle_{12}|\beta_3\rangle_{12}. \quad (21)$$

According to Eq. (21), when we perform the Bell-basis measurement on the third and fourth particles, the first and second particles will be entangled. For example, we prepare the state  $|\alpha_2\rangle$  of the first and third particles, and the state  $|\beta_2\rangle$  of the second and fourth particles. If the Bell-basis measurement result of the third and fourth particles is  $|\beta_3\rangle$ , then the state of the first and second particles will be  $|\alpha_3\rangle$ .

In the class of designed MDIQSDC protocols, Alice sends secret messages to Bob with the help of an untrusted third party, Charlie, who performs quantum measurement. The steps followed in the class of designed MDIQSDC protocols are given in Fig. 1. The steps are as follows:

**Step 1:** Alice prepares  $n$  GBell states,  $|\alpha_2\rangle^{\otimes n}$ . She takes the first particle from each GBell state to form an ordered particle sequence  $S_A = [S_A^1, S_A^2, \dots, S_A^n]$ , and the second particles to form another ordered particle sequence  $C_A = [C_A^1, C_A^2, \dots, C_A^n]$ . Then, Alice prepares  $m$  decoy single-particle states, each randomly in one of the four states  $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ . She randomly inserts them into the sequence  $C_A$  to form the sequence  $C'_A$ . Similarly, Bob prepares  $n$  Bell states,  $|\beta_2\rangle^{\otimes n}$ . He takes the first particle from each Bell state to form an ordered particle sequence  $S_B = [S_B^1, S_B^2, \dots, S_B^n]$ , and the second particles to form another ordered particle sequence  $C_B = [C_B^1, C_B^2, \dots, C_B^n]$ . Then, Bob prepares  $m$  decoy single-particle states, each randomly in one of the four states  $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ . He

randomly inserts them into the sequence  $C_B$  to form the sequence  $C'_B$ .

**Step 2:** Alice and Bob send  $C'_A$  and  $C'_B$  to Charlie, and keep  $S_A$  and  $S_B$  in their hands, respectively.

**Step 3:** After receiving  $C'_A$  and  $C'_B$ , Charlie performs the Bell-basis measurement on the  $i$ th particle of  $C'_A$  and the  $i$ th particle of  $C'_B$ ,  $i = 1, 2, \dots, n + m$ , and announces the measurement results. According to the measurements on different combinations of particles, they are assigned three different functions.

(a) For two single particles, they are used for eavesdropping check, which is described in the next step.

(b) For each pair of particles, one from a GBell state on Alice's hand and the other one from a Bell state on Bob's hand, the measurements will make the corresponding partner particles in  $S_A$  and  $S_B$  entangled, as shown in Eq. (21). The corresponding partner particle pairs will be used for encoding secret messages in *Step 5*.

(c) For those, a single particle and a partner particle of GBell state or Bell state, these instances are discarded.

**Step 4:** After Charlie announces the measurement results, Alice and Bob announce the positions and the states of the decoy single particles in  $C'_A$  and  $C'_B$ . Then, they use the results of the Bell-basis measurements performed on two single-particle states to check security. In detail, they use the cases in Eqs. (5)–(12) to estimate the error rate for security check, and ignore the other cases. If the error rate is below the predefined threshold, Alice and Bob implement the next step; otherwise, the protocol will be aborted.

**Step 5:** Alice and Bob will discard the particles in  $S_A$  and  $S_B$  that are not entangled. Suppose that the number of remaining particles of  $S_A$  ( $S_B$ ) is  $l$ , which is about  $n^2/(m+n)$ . The remaining particles of  $S_A$  form an ordered sequence  $M_A$  while the remaining particles of  $S_B$  form an ordered sequence  $M_B$ . Each pair, the  $i$ th particle of  $M_A$  and the  $i$ th particle of  $M_B$ ,  $i = 1, 2, \dots, l$ , is in the GBell state determined by the entanglement swapping as Eq. (21) and the corresponding measurement result. To ensure the integrity of the secret message, Alice encodes some random check numbers at random positions in  $M_A$  by performing  $U_0^A$  for 00,  $U_1^A$  for 01,  $U_2^A$  for 10 and  $U_3^A$  for 11. Furthermore, to send her secret message, Alice performs the encoding operations on the remaining particles in  $M_A$  to encode her message by the same encoding method as that of encoding random check numbers. The sequence  $M_A$  encoded the check number series and the secret message will form the sequence  $M'_A$ . In order to prevent anyone else from decoding Alice's secret message, Bob randomly implements one of operations  $\{U_0^B, U_1^B, U_2^B, U_3^B\}$  on each particle of  $M_B$  to form  $M'_B$ . Then, Alice and Bob send  $M'_A$  and  $M'_B$  to Charlie, respectively.

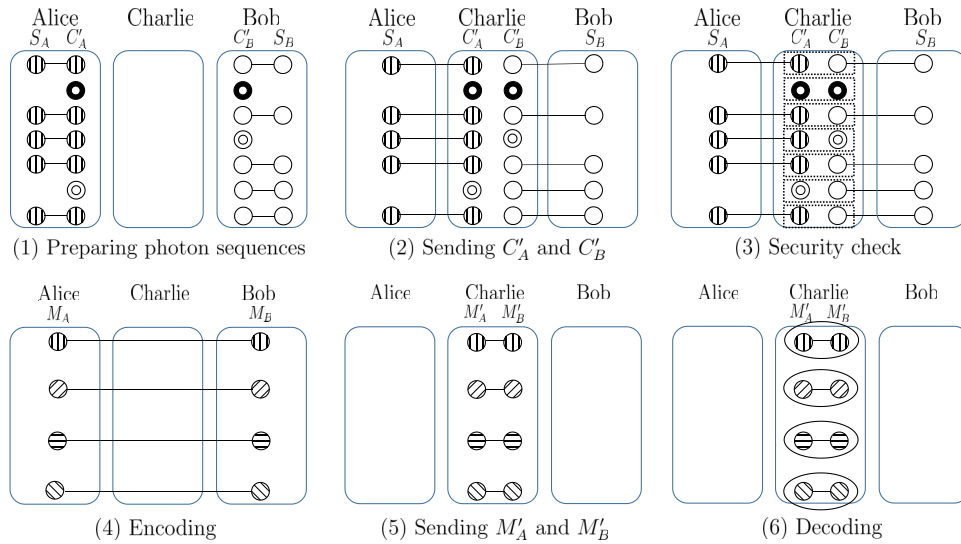


FIG. 1. The class of designed MDIQSDC protocols. The white pellets linked by the solid lines represent the Bell state in  $|\beta_2\rangle$ ; the nonwhite pellets linked by the solid lines represent the GBell states; the black concentric circles and the white concentric circles represent decoy particles; the dashed matrix boxes represent the Bell-basis measurements; the solid line ellipse represents the GBell basis measurements.

Step 6: After Charlie receives  $M'_A$  and  $M'_B$ , Charlie performs the GBell basis  $\{|\alpha_0\rangle, |\alpha_1\rangle, |\alpha_2\rangle, |\alpha_3\rangle\}$  measurements and publishes the measurement results. Bob uses these measurement results to decode the secret message and random check numbers sent by Alice. Then, Alice announces the positions and values of the random check numbers. Bob compares them with the results he deduced to check the integrity of the secret message. If the random number series has a high error rate, it means an eavesdropper has disturbed one of  $M'_A$  and  $M'_B$ , or both. Note that, the attacker's actions cannot obtain any useful information on the secret message. On the other hand, if the random number series is correct at an acceptable error rate, the transmission of message is correct at an acceptable error rate, also. Bob can use the error-correction code, predetermined by Alice and Bob, to correct the errors of the secret message. The communication process is completed.

*Remark 1.* The class of designed MDIQSDC protocols can be used not only for Alice to send secret messages to Bob, but also for Bob to send secret messages to Alice. That is to say, we can regard Alice's operations as random operations and Bob's operations as encoding operations in Step 5. Accordingly, the class of protocols exchanges Alice and Bob in Step 6.

*Remark 2.* The class of designed MDIQSDC protocols can realize BQSDC between Alice and Bob by some minor changes as follows.

*Steps 1\*–4\** are the same as *Steps 1–4* in the original protocol.

Step 5\*: After Alice and Bob discard the particles in  $S_A$  and  $S_B$  that are not entangled. Alice encodes some random check numbers at random positions in  $M_A$  and encodes her secret message on the remaining particles in  $M_A$  by randomly executing operation  $U_0^A$  or  $U_1^A$  for 0,  $U_2^A$  or  $U_3^A$  for 1, to form sequence  $M'_A$ . Comparatively, Bob encodes some random check numbers at random positions in  $M_B$  and encodes his secret message on the remaining particles in  $M_B$  by randomly executing operation  $U_0^B$  or  $U_2^B$  for 0,  $U_1^B$  or  $U_3^B$  for 1, to form sequence  $M'_B$ . Then, Alice and Bob then send the new sequences  $M'_A$  and  $M'_B$  to Charlie, respectively.

Step 6\*: Charlie performs the GBell basis measurement on the  $i$ th particle of  $M'_A$  and the  $i$ th particle of  $M'_B$ ,  $i = 1, 2, \dots, l$ , and announces the measurement results publicly. Then, Alice and Bob announce the positions and values of their random check numbers, respectively. They compare the random check numbers with the results they deduced, to check the integrity of their secret messages. If any random number series has a high error rate, it means an eavesdropper has disturbed one of  $M'_A$  and  $M'_B$ , or both. Note that, the eavesdropper's actions can not obtain any useful information on the secret messages. On the other hand, if both random number series are correct at an acceptable error rate, the transmissions of two messages are correct at an acceptable error rate, also. Alice and Bob can use the error-correction code they predetermined, to correct the errors

of the two secret messages. The communication process is completed.

### V. SECURITY UNDER SOME KNOWN ATTACKS

This section shows that the class of designed MDIQSDC protocols have no information leakage problem. Furthermore, it also shows that the class of designed protocols can resist intercept-and-resend attacks, measure-resend attacks, and collective attacks.

(1) *The class of designed protocols leak no information.* Before Charlie announces the measurement results, Bob randomly implements one of operations  $\{U_0^B, U_1^B, U_2^B, U_3^B\}$  on each particle of  $M_B$ . Bob's operations are only known by himself, and that will protect the encoded message from leaking to eavesdroppers. For example, suppose the joint state of the  $i$ th particle of  $M_A$  and the  $i$ th particle of  $M_B$  is  $|\alpha_0\rangle$  before encoding, and Alice's secret message is 00. Then, Alice will perform  $U_0^A$  operation on the  $i$ th particle of  $M_A$ . In addition, Bob randomly implements one of operations  $\{U_0^B, U_1^B, U_2^B, U_3^B\}$  on the  $i$ th particle of  $M_B$ . This will lead to one of four random measurement results when Charlie measures the  $i$ th particle of  $M'_A$  and the  $i$ th particle of  $M'_B$  with the GBell basis in *Step 6*. It can be seen from Table II, before Bob decoding, all the four GBell states can randomly arise after Alice encoding any two-bit message. Accordingly, each of Charlie's measurement results involves four kinds of possibilities on Alice's secret classical bits. From the viewpoint of Shannon's information theory [50], four equal possibilities contain

$$-\sum_{i=1}^4 p_i \log p_i = -4 \times \frac{1}{4} \log \frac{1}{4} = 2 \quad (22)$$

bits information for the eavesdropper. That is to say, although Charlie published his measurement results of each pair of particles, the eavesdropper cannot extract any useful information about Alice's secret message from the knowledge of the measurement results.

(2) *The class of designed protocols can resist intercept-and-resend attacks.* Attackers have two chances to perform intercept-and-resend attacks in *Step 2* and *Step 5* of the class of designed MDIQSDC protocols. Note that, the attacker cannot obtain any useful information on the secret message if he/she attacks only on  $M'_A$  and  $M'_B$  in *Step 5*. Therefore, we need only to show that intercept-and-resend attacks performed in *Step 2* can be detected. If an attacker intercepts a decoy particle in  $C'_A$  ( $C'_B$ ) and sends a fake particle instead of the original particle to Charlie in *Step 2*, the probability for he/she to be detected in *Step 4* is  $1/2$  when the decoy particle in  $C'_A$  ( $C'_B$ ) is used to detect error. Therefore, for this attack, the total error rate in the class of designed MDIQSDC protocols is  $1 - (1/2)^{m^2/(n+m)}$ . When  $m = n$  and  $n$  is large enough, the total error rate caused by

TABLE II. The encoding and decoding table when the  $i$ th joint state of  $M_A$  and  $M_B$  is  $|\alpha_0\rangle$ .

Alice's secret message	Bob's operation	Charlie's measurement result
00	$U_0^B$	$ \alpha_0\rangle$
	$U_1^B$	$ \alpha_1\rangle$
	$U_2^B$	$ \alpha_2\rangle$
	$U_3^B$	$ \alpha_3\rangle$
01	$U_0^B$	$ \alpha_1\rangle$
	$U_1^B$	$ \alpha_0\rangle$
	$U_2^B$	$ \alpha_3\rangle$
	$U_3^B$	$ \alpha_2\rangle$
10	$U_0^B$	$ \alpha_2\rangle$
	$U_1^B$	$ \alpha_3\rangle$
	$U_2^B$	$ \alpha_0\rangle$
	$U_3^B$	$ \alpha_1\rangle$
11	$U_0^B$	$ \alpha_3\rangle$
	$U_1^B$	$ \alpha_2\rangle$
	$U_2^B$	$ \alpha_1\rangle$
	$U_3^B$	$ \alpha_0\rangle$

this attack is approximately 100%. If the error rate is higher than the predefined threshold, the protocol will be aborted. This attack will be found in *Step 4*.

(3) *The class of designed protocols can resist measure-resend attacks.* Similar to the discussion of intercept-and-resend attacks, we need only to show that measure-resend attacks performed in *Step 2* can be detected. In *Step 2*, if an attacker measures the sequences  $C'_A$  and  $C'_B$  with random basis  $\{|0\rangle, |1\rangle\}$  or  $\{|+\rangle, |-\rangle\}$ , and sends quantum state sequences of measurement results to Charlie, he/she will be found with a high probability in *Step 4*. If the attacker uses a different base to measure a decoy particle in  $C'_A$  or a decoy particle in  $C'_B$ , this attack will always result in an error rate of  $1/2$  when it is used to detect error. Note that, the attacker has a half chance of using the wrong measurement basis. For this attack, the total error rate in the class of designed MDIQSDC protocols is  $1 - (3/4)^{m^2/(n+m)}$ . When  $m = n$  and  $n$  is large enough, the total error rate caused by this attack is approximately 100%. If the error rate is higher than the predefined threshold, the protocol will be abort. This attack will be found in *Step 4*.

If an attacker performs Bell-basis measurements on the sequences  $C'_A$  and  $C'_B$  in *Step 2*, and sends the states of measurement results to Charlie, Charlie will announce the same measurement results as the attacker in *Step 3*. Therefore, the attacker cannot obtain any useful information from this attack. Note that, it is showed that the class

of designed MDIQSDC protocols have no information leakage.

(4) *The class of designed protocols can resist collective attacks.* Similar to the discussion of intercept-and-resend attacks, we need only to show that collective attacks performed in *Step 2* can be detected. Attackers may steal partial information by entangling his/her auxiliary particles  $\varepsilon = \{|\varepsilon_1\rangle, |\varepsilon_2\rangle, \dots, |\varepsilon_{n+m}\rangle\}$  with the particles in sequences  $C'_A$  and  $C'_B$ . Without losing generality, we can assume  $|\varepsilon_i\rangle = |00\rangle$ , where  $i = 1, 2, \dots, n + m$ . Then, the attacker attacks with  $U$  on the  $i$ th particle of  $C'_A$  and the  $i$ th particle of  $C'_B$ , an operator which acts on basis states as follows:

$$\begin{aligned} &U(|00\rangle_{AB}|\varepsilon_i\rangle_E) \\ &= b_0|00\rangle|f_0\rangle + b_1|01\rangle|f_1\rangle + b_2|10\rangle|f_2\rangle + b_3|11\rangle|f_3\rangle \\ &= \frac{1}{\sqrt{2}}(|\beta_0\rangle(b_0|f_0\rangle + b_3|f_3\rangle) + |\beta_1\rangle(b_0|f_0\rangle - b_3|f_3\rangle) + \\ &|\beta_2\rangle(b_1|f_1\rangle + b_2|f_2\rangle) + |\beta_3\rangle(b_1|f_1\rangle - b_2|f_2\rangle)), \end{aligned} \quad (23)$$

$$\begin{aligned} &U(|01\rangle_{AB}|\varepsilon_i\rangle_E) \\ &= c_0|00\rangle|g_0\rangle + c_1|01\rangle|g_1\rangle + c_2|10\rangle|g_2\rangle + c_3|11\rangle|g_3\rangle \\ &= \frac{1}{\sqrt{2}}(|\beta_0\rangle(c_0|g_0\rangle + c_3|g_3\rangle) + |\beta_1\rangle(c_0|g_0\rangle - c_3|g_3\rangle) + \\ &|\beta_2\rangle(c_1|g_1\rangle + c_2|g_2\rangle) + |\beta_3\rangle(c_1|g_1\rangle - c_2|g_2\rangle)), \end{aligned} \quad (24)$$

$$\begin{aligned} &U(|10\rangle_{AB}|\varepsilon_i\rangle_E) \\ &= d_0|00\rangle|h_0\rangle + d_1|01\rangle|h_1\rangle + d_2|10\rangle|h_2\rangle + d_3|11\rangle|h_3\rangle \\ &= \frac{1}{\sqrt{2}}(|\beta_0\rangle(d_0|h_0\rangle + d_3|h_3\rangle) + |\beta_1\rangle(d_0|h_0\rangle - d_3|h_3\rangle) + \\ &|\beta_2\rangle(d_1|h_1\rangle + d_2|h_2\rangle) + |\beta_3\rangle(d_1|h_1\rangle - d_2|h_2\rangle)), \end{aligned} \quad (25)$$

$$\begin{aligned} &U(|11\rangle_{AB}|\varepsilon_i\rangle_E) \\ &= e_0|00\rangle|j_0\rangle + e_1|01\rangle|j_1\rangle + e_2|10\rangle|j_2\rangle + e_3|11\rangle|j_3\rangle \\ &= \frac{1}{\sqrt{2}}(|\beta_0\rangle(e_0|j_0\rangle + e_3|j_3\rangle) + |\beta_1\rangle(e_0|j_0\rangle - e_3|j_3\rangle) + \\ &|\beta_2\rangle(e_1|j_1\rangle + e_2|j_2\rangle) + |\beta_3\rangle(e_1|j_1\rangle - e_2|j_2\rangle)). \end{aligned} \quad (26)$$

Furthermore, by calculating, we can get the following equations:

$$\begin{aligned} &U(|++\rangle_{AB}|\varepsilon_i\rangle_E) \\ &= \frac{1}{2\sqrt{2}}(|\beta_0\rangle(b_0|f_0\rangle + b_3|f_3\rangle + c_0|g_0\rangle + c_3|g_3\rangle) + \end{aligned}$$

$$\begin{aligned} &d_0|h_0\rangle + d_3|h_3\rangle + e_0|j_0\rangle + e_3|j_3\rangle) + \\ &|\beta_1\rangle(b_0|f_0\rangle - b_3|f_3\rangle + c_0|g_0\rangle - c_3|g_3\rangle) + \\ &d_0|h_0\rangle - d_3|h_3\rangle + e_0|j_0\rangle - e_3|j_3\rangle) + \\ &|\beta_2\rangle(b_1|f_1\rangle + b_2|f_2\rangle + c_1|g_1\rangle + c_2|g_2\rangle) + \\ &d_1|h_1\rangle + d_2|h_2\rangle + e_1|j_1\rangle + e_2|j_2\rangle) + \\ &|\beta_3\rangle(b_1|f_1\rangle - b_2|f_2\rangle + c_1|g_1\rangle - c_2|g_2\rangle) + \\ &d_1|h_1\rangle - d_2|h_2\rangle + e_1|j_1\rangle - e_2|j_2\rangle)), \end{aligned} \quad (27)$$

$$\begin{aligned} &U(|--\rangle_{AB}|\varepsilon_i\rangle_E) \\ &= \frac{1}{2\sqrt{2}}(|\beta_0\rangle(b_0|f_0\rangle + b_3|f_3\rangle - c_0|g_0\rangle - c_3|g_3\rangle - \\ &d_0|h_0\rangle - d_3|h_3\rangle + e_0|j_0\rangle + e_3|j_3\rangle) + \\ &|\beta_1\rangle(b_0|f_0\rangle - b_3|f_3\rangle - c_0|g_0\rangle + c_3|g_3\rangle - \\ &d_0|h_0\rangle + d_3|h_3\rangle + e_0|j_0\rangle - e_3|j_3\rangle) + \\ &|\beta_2\rangle(b_1|f_1\rangle + b_2|f_2\rangle - c_1|g_1\rangle - c_2|g_2\rangle - \\ &d_1|h_1\rangle - d_2|h_2\rangle + e_1|j_1\rangle + e_2|j_2\rangle) + \\ &|\beta_3\rangle(b_1|f_1\rangle - b_2|f_2\rangle - c_1|g_1\rangle + c_2|g_2\rangle - \\ &d_1|h_1\rangle + d_2|h_2\rangle + e_1|j_1\rangle - e_2|j_2\rangle)), \end{aligned} \quad (28)$$

$$\begin{aligned} &U(|-+\rangle_{AB}|\varepsilon_i\rangle_E) \\ &= \frac{1}{2\sqrt{2}}(|\beta_0\rangle(b_0|f_0\rangle + b_3|f_3\rangle + c_0|g_0\rangle + c_3|g_3\rangle - \\ &d_0|h_0\rangle - d_3|h_3\rangle - e_0|j_0\rangle - e_3|j_3\rangle) + \\ &|\beta_1\rangle(b_0|f_0\rangle - b_3|f_3\rangle + c_0|g_0\rangle - c_3|g_3\rangle - \\ &d_0|h_0\rangle + d_3|h_3\rangle - e_0|j_0\rangle + e_3|j_3\rangle) + \\ &|\beta_2\rangle(b_1|f_1\rangle + b_2|f_2\rangle + c_1|g_1\rangle + c_2|g_2\rangle - \\ &d_1|h_1\rangle - d_2|h_2\rangle - e_1|j_1\rangle - e_2|j_2\rangle) + \\ &|\beta_3\rangle(b_1|f_1\rangle - b_2|f_2\rangle + c_1|g_1\rangle - c_2|g_2\rangle - \\ &d_1|h_1\rangle + d_2|h_2\rangle - e_1|j_1\rangle + e_2|j_2\rangle)), \end{aligned} \quad (29)$$

$$\begin{aligned} &U(|+-\rangle_{AB}|\varepsilon_i\rangle_E) \\ &= \frac{1}{2\sqrt{2}}(|\beta_0\rangle(b_0|f_0\rangle + b_3|f_3\rangle - c_0|g_0\rangle - c_3|g_3\rangle + \\ &d_0|h_0\rangle + d_3|h_3\rangle - e_0|j_0\rangle - e_3|j_3\rangle) + \\ &|\beta_1\rangle(b_0|f_0\rangle - b_3|f_3\rangle - c_0|g_0\rangle + c_3|g_3\rangle + \\ &d_0|h_0\rangle - d_3|h_3\rangle - e_0|j_0\rangle + e_3|j_3\rangle) + \\ &|\beta_2\rangle(b_1|f_1\rangle + b_2|f_2\rangle - c_1|g_1\rangle - c_2|g_2\rangle + \\ &d_1|h_1\rangle + d_2|h_2\rangle - e_1|j_1\rangle - e_2|j_2\rangle) + \end{aligned}$$



$$\begin{aligned}
 & |\beta_3\rangle(b_1|f_1\rangle - b_2|f_2\rangle - c_1|g_1\rangle + c_2|g_2\rangle + \\
 & d_1|h_1\rangle - d_2|h_2\rangle - e_1|j_1\rangle + e_2|j_2\rangle). \quad (30)
 \end{aligned}$$

Since  $U$  being a unitary operation,  $|b_0|^2 + |b_1|^2 + |b_2|^2 + |b_3|^2 = 1$ ,  $|c_0|^2 + |c_1|^2 + |c_2|^2 + |c_3|^2 = 1$ ,  $|d_0|^2 + |d_1|^2 + |d_2|^2 + |d_3|^2 = 1$ , and  $|e_0|^2 + |e_1|^2 + |e_2|^2 + |e_3|^2 = 1$ . If the attacker wants to escape the security check in *Step 4* of the class of designed MDIQSDC protocols, we can know that Eqs. (23)–(30) need to meet the following conditions:  $b_1 = b_2 = c_0 = c_3 = d_0 = d_3 = e_1 = e_2 = 0$ ,  $b_0|f_0\rangle - b_3|f_3\rangle + e_0|j_0\rangle - e_3|j_3\rangle = \mathbf{0}$ ,  $b_0|f_0\rangle + b_3|f_3\rangle - e_0|j_0\rangle - e_3|j_3\rangle = \mathbf{0}$ ,  $c_1|g_1\rangle - c_2|g_2\rangle + d_1|h_1\rangle - d_2|h_2\rangle = \mathbf{0}$ , and  $c_1|g_1\rangle + c_2|g_2\rangle - d_1|h_1\rangle - d_2|h_2\rangle = \mathbf{0}$ . Then, we have  $b_0|f_0\rangle = e_3|j_3\rangle$ ,  $b_3|f_3\rangle = e_0|j_0\rangle$ ,  $c_1|g_1\rangle = d_2|h_2\rangle$ , and  $c_2|g_2\rangle = d_1|h_1\rangle$ . Thus, the attacker cannot get any useful information without any error by this attack.

*Remark 3.* Similarly, the class of designed BQSDC protocols have no information leakage problem, and can resist intercept-and-resend attacks, measure-resend attacks and collective attacks.

## VI. UNCONDITIONAL SECURITY

In this section, we analyze the unconditional security of the class of designed MDIQSDC protocols by applying Wyner's wiretap channel theory [51–53]. The message transmission in the quantum channel between Alice and Bob is modeled as a main channel while the eavesdropping and environmental noises are modeled as wiretap channels. According to Wyner's wiretap channel theory [51–53], there is an encoding method that allows information to be securely transmitted at any rate lower than the secrecy capacity when the secrecy capacity is positive. The secrecy capacity,  $C_s$ , can be calculated as

$$C_s = C_M - C_W, \quad (31)$$

where  $C_M$  and  $C_W$  are the main channel capacity and the wiretap channel capacity, respectively. Note that,  $C_M = I(A : B)$  and  $C_W = \max I(A : E)$ , where the maximum is over all collective attacks that the error rates caused by Eve's attack is in the allowable range of the protocol, and  $I(A : B)$  ( $I(A : E)$ ) is the mutual information between Alice and Bob (Eve). After the protocol is performed, i.e., Eve has performed her attack, Eve's attack needs to satisfy that the error rates caused by the attack are consistent with the statistics observed during parameter estimation.

First, we use Niu *et al.*'s method [54] to estimate the wiretap channel capacity. We are not concerned with the measurement processes and strategies that Eve might utilize, so we focus on the system after entanglement swapping, i.e., the joint state  $\rho_{AB}^{jnt}$  consisting of photon pairs shared between Alice and Bob. We assume Eve performs

a coherent attack. For every round of communication, Eve attaches her auxiliary system  $E$  to the system  $A$  and the system  $B$  in state  $E$ , respectively. Eve performs the unitary operation  $U_A$  on the system  $A$  and the system  $E$  and performs the unitary operation  $U_B$  on the system  $B$  and the system  $E$ . According to the quantum De Finetti theorem [55], we can use a direct product of independent and identically distributed (IID) subsystems  $\rho_{AB}^{\otimes n}$  to approximate  $\rho_{AB}^{jnt}$  asymptotically. In this case, Eve's attacks can be considered as the collective attack. The entire state of the systems  $A$  and  $B$  before the operation is the direct product of IID systems,

$$\rho_0^{AB} = (|\alpha_2\rangle\langle\alpha_2|_{13} \otimes |\beta_2\rangle\langle\beta_2|_{24})^{\otimes n}. \quad (32)$$

After Eve's attack, the joint state of Alice, Bob, and Eve changes to

$$\begin{aligned}
 \rho_1^{ABE} = & \left( U_A(|\alpha_2\rangle\langle\alpha_2|_{13}|E\rangle\langle E|_E) U_A^\dagger \otimes \right. \\
 & \left. U_B(|\beta_2\rangle\langle\beta_2|_{24}|E\rangle\langle E|_E) U_B^\dagger \right)^{\otimes n}. \quad (33)
 \end{aligned}$$

In *Step 4*, Alice and Bob use the results of the Bell-basis measurements performed on two single-particle states to check security. We use  $\varepsilon_X$  ( $\varepsilon_Z$ ) to denote the quantum bit error rate (QBER) obtained by comparing Charlie's measurement result with the initial states of the two particles prepared by Alice and Bob in the  $X$  basis ( $Z$  basis). After the security check, Alice and Bob remove the particles that were discarded and used for eavesdropping check. Due to the fact that Eve's  $n - l$  corresponding auxiliary particles will not carry any secret message, we remove them. Accordingly, in *Step 4*, after the security check, the joint state of Alice, Bob, and Eve changes to

$$\begin{aligned}
 \rho_1^{ABE} = & \left( U_A(|\alpha_2\rangle\langle\alpha_2|_{13}|E\rangle\langle E|_E) U_A^\dagger \otimes \right. \\
 & \left. U_B(|\beta_2\rangle\langle\beta_2|_{24}|E\rangle\langle E|_E) U_B^\dagger \right)^{\otimes l}. \quad (34)
 \end{aligned}$$

According to Ref. [54], if we assume the main channel is a symmetric channel, the capacity of the main channel is

$$C_M = 2 - h_4(\mathbf{e}), \quad (35)$$

where  $\mathbf{e}$  is the error rate distribution of the main channel and  $h_4(\mathbf{e})$  the four-array Shannon entropy.

In *Step 1*, Alice and Bob send one of the entangled particles to Charlie, respectively. The quantum channel, Alice sending the second particle of  $|\alpha_2\rangle$  and decoy particles to Charlie, is modeled as the depolarizing channel

$$\mathcal{E}_0 : \rho \rightarrow \frac{p_0}{2} I_2 + (1 - p_0)\rho. \quad (36)$$

The quantum channel, Bob sending the second particle of  $|\beta_2\rangle$  and decoy particles to Charlie, is modeled as the

depolarizing channel

$$\mathcal{E}_1 : \rho' \rightarrow \frac{p_1}{2}I_2 + (1 - p_1)\rho'. \quad (37)$$

Note that,  $\varepsilon_X$  ( $\varepsilon_Z$ ) denotes the QBER obtained by comparing Charlie's measurement result with the initial states of the two particles prepared by Alice and Bob in the  $X$  basis ( $Z$  basis). For example, if both the  $i$ th particles in the sequence  $C'_A$  and the sequence  $C'_B$  are in the state  $|0\rangle$ , and the result state of Charlie's Bell-basis measurement is  $|\beta_2\rangle$  or  $|\beta_3\rangle$ , then, according to Eq. (5), this is an  $X$  error. Alice's (Bob's) state  $|0\rangle$  evolves to the state  $|1\rangle$  with a probability of  $p_0/2$  ( $p_1/2$ ) after going through the depolarizing channel  $\mathcal{E}_0$  ( $\mathcal{E}_1$ ), leaving the original state unchanged with a probability of  $1 - p_0/2$  ( $1 - p_1/2$ ). Therefore, an  $X$  error occurs when the result state of Charlie's Bell-basis measurement is  $|\beta_2\rangle$  or  $|\beta_3\rangle$  with a probability of  $p_0/2 \times (1 - p_1/2) + p_1/2 \times (1 - p_0/2) = (p_0 + p_1 - p_0p_1)/2$ . Similarly, we get

$$\varepsilon_Z = \varepsilon_X = \frac{p_0 + p_1 - p_0p_1}{2}. \quad (38)$$

Thus, we can set  $q = \varepsilon_Z = \varepsilon_X = (p_0 + p_1 - p_0p_1)/2$ .

In *Step 3*, the evolution channel of the entangled state shared by Alice and Bob (the second particle of  $|\alpha_2\rangle$  being transmitted by the depolarizing channel  $\mathcal{E}_0$ , the second particle of  $|\beta_2\rangle$  being transmitted by the depolarizing channel  $\mathcal{E}_1$ , and Charlie's Bell-basis measurement) is modeled as (see Appendix C for details)

$$\mathcal{E}' : \rho \rightarrow \frac{1 - q_0q_1}{4}I_4 + q_0q_1\rho. \quad (39)$$

In *Step 5*, Alice and Bob send the remaining entangled particles to Charlie through the depolarizing channel  $\mathcal{E}_0$  and the depolarizing channel  $\mathcal{E}_1$ , respectively. The whole evolution channel of the joint state is (see Appendix C for details)

$$\mathcal{E}' : \rho \rightarrow \frac{1 - q_0^2q_1^2}{4}I_4 + q_0^2q_1^2\rho. \quad (40)$$

According to  $q = (p_0 + p_1 - p_0p_1)/2$ , the error-rate distribution of the main channel is

$$\mathbf{e} = (1 - 3q + 3q^2, q - q^2, q - q^2, q - q^2), \quad (41)$$

where  $\mathbf{e}(0)$  is the correct probability,  $\mathbf{e}(1)$ ,  $\mathbf{e}(2)$ , and  $\mathbf{e}(3)$  are the  $X$ -type,  $Y$ -type, and  $Z$ -type errors, respectively. The  $X$ -type,  $Y$ -type, and  $Z$ -type errors are represented by the

following transformations:

$$\begin{aligned} X\text{-type: } & |\alpha_0\rangle \mapsto |\alpha_1\rangle, |\alpha_1\rangle \mapsto |\alpha_0\rangle, |\alpha_2\rangle \mapsto |\alpha_3\rangle, |\alpha_3\rangle \mapsto |\alpha_2\rangle; \\ Y\text{-type: } & |\alpha_0\rangle \mapsto |\alpha_2\rangle, |\alpha_1\rangle \mapsto |\alpha_3\rangle, |\alpha_2\rangle \mapsto |\alpha_0\rangle, |\alpha_3\rangle \mapsto |\alpha_1\rangle; \\ Z\text{-type: } & |\alpha_0\rangle \mapsto |\alpha_3\rangle, |\alpha_1\rangle \mapsto |\alpha_2\rangle, |\alpha_2\rangle \mapsto |\alpha_1\rangle, |\alpha_3\rangle \mapsto |\alpha_0\rangle. \end{aligned} \quad (42)$$

Therefore, the capacity of the main channel is

$$C_M = 2 - h_4(\mathbf{e}) = 2 + 3(q - q^2) \log(q - q^2) + (1 - 3q + 3q^2) \log(1 - 3q + 3q^2). \quad (43)$$

Now, we estimate  $C_W$  using the technique in Refs. [54,56]. After entanglement swapping, consider a purification of joint state of Alice and Bob is

$$|\phi^{ABE}\rangle = \sum_{i=0}^3 \sqrt{\delta_i} |\alpha_i\rangle |E_i\rangle, \quad (44)$$

where  $\{|E_0\rangle, |E_1\rangle, |E_2\rangle, |E_3\rangle\}$  is a set of orthogonal states of Eve's auxiliary system and  $\sum_{i=0}^3 \delta_i = 1$ . Then, Alice carries out the message encoding while Bob performs the cover operation in *Step 5*. We first consider that Bob performs the cover operation,

$$\begin{aligned} \rho_{\text{cover}}^{ABE} = & \frac{1}{4} \left( (I \otimes U_0^B \otimes I) |\phi^{ABE}\rangle \langle \phi^{ABE}| (I \otimes U_0^B \otimes I)^\dagger \right. \\ & + (I \otimes U_1^B \otimes I) |\phi^{ABE}\rangle \langle \phi^{ABE}| (I \otimes U_1^B \otimes I)^\dagger \\ & + (I \otimes U_2^B \otimes I) |\phi^{ABE}\rangle \langle \phi^{ABE}| (I \otimes U_2^B \otimes I)^\dagger \\ & \left. + (I \otimes U_3^B \otimes I) |\phi^{ABE}\rangle \langle \phi^{ABE}| (I \otimes U_3^B \otimes I)^\dagger \right). \end{aligned} \quad (45)$$

Tracing out the system  $B$  from the joint system  $ABE$ , we get

$$\rho^{AE} = \text{Tr}_B(\rho_{\text{cover}}^{ABE}) = \frac{1}{4} \sum_{i=0}^3 (P_{|\varphi_i\rangle} + P_{|\phi_i\rangle}), \quad (46)$$

where

$$\begin{aligned} |\varphi_0\rangle = |\varphi_2\rangle = & |0\rangle (a\sqrt{\delta_0}|E_0\rangle + \bar{b}\sqrt{\delta_1}|E_1\rangle) \\ & + |1\rangle (b\sqrt{\delta_2}|E_2\rangle - \bar{a}\sqrt{\delta_3}|E_3\rangle), \end{aligned} \quad (47)$$

$$\begin{aligned} |\varphi_1\rangle = |\varphi_3\rangle = & |0\rangle (\bar{b}\sqrt{\delta_0}|E_0\rangle + a\sqrt{\delta_1}|E_1\rangle) \\ & + |1\rangle (-\bar{a}\sqrt{\delta_2}|E_2\rangle + b\sqrt{\delta_3}|E_3\rangle), \end{aligned} \quad (48)$$

$$\begin{aligned} |\phi_0\rangle = |\phi_2\rangle = & |0\rangle (a\sqrt{\delta_2}|E_2\rangle + \bar{b}\sqrt{\delta_3}|E_3\rangle) \\ & + |1\rangle (b\sqrt{\delta_0}|E_0\rangle - \bar{a}\sqrt{\delta_1}|E_1\rangle), \end{aligned} \quad (49)$$

$$\begin{aligned}
 |\phi_1\rangle = |\phi_3\rangle = & |0\rangle(\bar{b}\sqrt{\delta_2}|E_2\rangle + a\sqrt{\delta_3}|E_3\rangle) \\
 & + |1\rangle(-\bar{a}\sqrt{\delta_0}|E_0\rangle + b\sqrt{\delta_1}|E_1\rangle), \quad (50)
 \end{aligned}$$

and  $P_{|\phi_i\rangle}$  and  $P_{|\phi_i\rangle}$  are the projection operators of the states  $|\phi_i\rangle$  and  $|\phi_i\rangle$ , respectively.

Considering that Alice's message encoding operation,  $\rho^{AE}$  becomes

$$\rho_j^{AE} = (U_j^A)\rho^{AE}(U_j^A)^\dagger, j = 0, 1, 2, \text{ or } 3. \quad (51)$$

According to Ref. [56], we denote the string that Alice encodes as  $\mathcal{C} = \zeta_1, \dots, \zeta_m$ , where  $\zeta_i \in \{0, 1, 2, 3\}$ ,  $i = 1, 2, \dots, m$ . Note that, 0, 1, 2, and 3 correspond to the codewords 00, 01, 10, and 11, respectively. The probability of  $\mathcal{C}$  is denoted by  $p_{\mathcal{C}}$ . Employing Holevo's bound [57], we can calculate the mutual information  $I(A : E)$  of the joint system  $AE$ . Suppose that each symbol in  $\{\zeta_i\}$  has the same distribution  $p_{\zeta_i} = 1/4$ . Thus, we have

$$\begin{aligned}
 I(A : E) & \leq S\left(\sum_{\mathcal{C}} p_{\mathcal{C}} \rho_{\mathcal{C}}^{AE}\right) - \sum_{\mathcal{C}} p_{\mathcal{C}} S(\rho_{\mathcal{C}}^{AE}) \\
 & \leq m\left(S\left(\sum_j p_{\zeta_j} \rho_j^{AE}\right) - 1\right), \quad (52)
 \end{aligned}$$

where  $\rho_{\mathcal{C}}^{AE}$  is the system  $AE$  encoded with string  $\mathcal{C}$ ,  $S(\cdot)$  the von Neumann entropy. According to Eq. (52), we have the average mutual information

$$C_W = \max I(A : E) \leq S\left(\sum_j p_{\zeta_j} \rho_j^{AE}\right) - 1. \quad (53)$$

By calculation, we have

$$\begin{aligned}
 \sum_j p_{\zeta_j} \rho_j^{AE} & = \frac{1}{2}(\delta_0(|0\rangle\langle 0| + |1\rangle\langle 1|)|E_0\rangle\langle E_0| \\
 & + \delta_1(|0\rangle\langle 0| + |1\rangle\langle 1|)|E_1\rangle\langle E_1| \\
 & + \delta_2(|0\rangle\langle 0| + |1\rangle\langle 1|)|E_2\rangle\langle E_2| \\
 & + \delta_3(|0\rangle\langle 0| + |1\rangle\langle 1|)|E_3\rangle\langle E_3|). \quad (54)
 \end{aligned}$$

Since  $\{|E_0\rangle, |E_1\rangle, |E_2\rangle, |E_3\rangle\}$  are mutually orthogonal, the eigenvalues of  $\sum_j p_{\zeta_j} \rho_j^{AE}$  are  $\delta_0/2$ ,  $\delta_0/2$ ,  $\delta_1/2$ ,  $\delta_1/2$ ,  $\delta_2/2$ ,  $\delta_2/2$ ,  $\delta_3/2$ , and  $\delta_3/2$ . Then, we have

$$\begin{aligned}
 S\left(\sum_j p_{\zeta_j} \rho_j^{AE}\right) & = -2 \sum_j^3 \frac{\delta_j}{2} \log \frac{\delta_j}{2} \\
 & = - \sum_j^3 \delta_j \log \delta_j + 1. \quad (55)
 \end{aligned}$$

According to Eq. (39), the probability distribution of  $\{\delta_0, \delta_1, \delta_2, \delta_3\}$  is  $(1 - \frac{3}{2}q, \frac{1}{2}q, \frac{1}{2}q, \frac{1}{2}q)$ . According to Eqs.

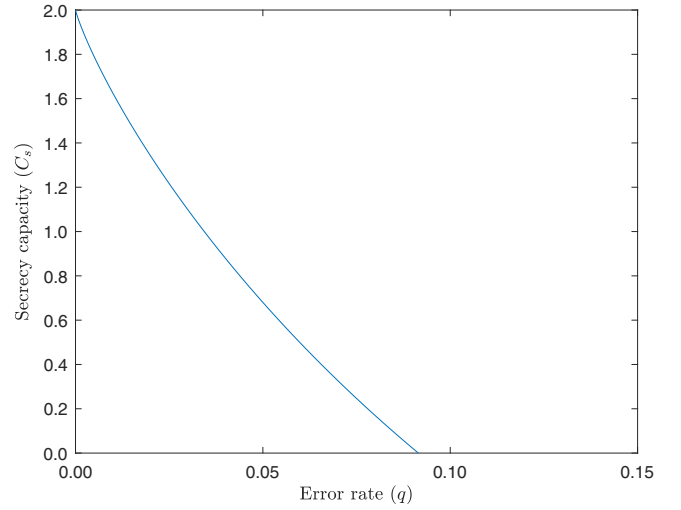


FIG. 2. The relationship between the lower bound of the secrecy capacity and the error rate. The error-rate threshold is 9.1494%.

(53) and (55), the capacity of the wiretap channel is

$$C_W \leq -\frac{3}{2}q \log\left(\frac{1}{2}q\right) - \left(1 - \frac{3}{2}q\right) \log\left(1 - \frac{3}{2}q\right). \quad (56)$$

Thus, according to Eqs. (31), (43), and (56), the secrecy capacity of the class of designed MDIQSDC protocols satisfies

$$\begin{aligned}
 C_s & \geq 2 + 3(q - q^2) \log(q - q^2) \\
 & + (1 - 3q + 3q^2) \log(1 - 3q + 3q^2) \\
 & + \frac{3}{2}q \log\left(\frac{1}{2}q\right) + \left(1 - \frac{3}{2}q\right) \log\left(1 - \frac{3}{2}q\right). \quad (57)
 \end{aligned}$$

The relationship between the lower bound of the secrecy capacity in Eq. (57) and the error rate  $q$  is illustrated in Fig. 2. The error-rate threshold of the class of designed MDIQSDC protocols is 9.1494%.

## VII. CONCLUSION

In this paper, by parameterizing the coefficients of Bell states, we constructed four GBell states,  $|\alpha_0\rangle = a|00\rangle + b|11\rangle$ ,  $|\alpha_1\rangle = \bar{b}|00\rangle - \bar{a}|11\rangle$ ,  $|\alpha_2\rangle = a|01\rangle + b|10\rangle$ , and  $|\alpha_3\rangle = \bar{b}|01\rangle - \bar{a}|10\rangle$ , where  $a$  and  $b$  are two complex numbers with  $|a| = |b| = 1/\sqrt{2}$ ,  $\bar{a}$  and  $\bar{b}$  the conjugate complex numbers of  $a$  and  $b$ , respectively. By calculation, we also obtained two types of generalized Pauli operators to realize the mutual transformation of the four GBell states as that of Pauli operators acting on one particle of a Bell state. Interestingly, the local unitary operations on the two particles of Bell states are identical, whereas

for the GBell states, they must differ in certain cases. In particular, Bell states are the special cases of the above four GBell states when  $a = \pm b = \pm 1/\sqrt{2}$ . In addition, Pauli operators are the special cases of the two types of generalized Pauli operators. Furthermore, we illustrated the entanglement swapping between a GBell state and a Bell state. Based on the entanglement swapping, we designed a class of MDIQSDC protocols with the GBell states. The class of designed MDIQSDC protocols have no information leakage problem, and can resist intercept-and-resend attacks, measure-resend attacks and collective attacks. In addition, the unconditional security of the class of designed MDIQSDC protocols is proved. Moreover, the class of designed MDIQSDC protocols can also realize BQSDC between Alice and Bob by some minor changes.

### ACKNOWLEDGMENTS

This work was supported in part by the Joint Research and Development Fund of Wuyi University, Hong Kong and Macao (Grant No. 2021WGALH16), the National Natural Science Foundations of China (Grants No. 61871205 and No. 11874312), Guangdong Provincial Quantum Science Strategic Initiative (Grant No. GDZX2200001), the Innovation Program for Quantum Science and Technology (Grant No. 2021ZD0302900), the Guangdong Basic and Applied Basic Research Foundation (Grant No. 2021A1515012623), the Innovation Project of Department of Education of Guangdong Province of China (Grant No. 2017KTSCX180), the Science and Technology Project of Jiangmen City of China (Grant No. 2021030101270004596), and the Special Foundation in Key Fields for Universities of Guangdong Province (Grant No. 2023ZDZX4060).

### APPENDIX A: THE CONSTRUCTION OF GENERALIZED PAULI OPERATIONS

Now, we explore local unitary operations to realize the mutual transformation of the four states as that of Pauli operators acting on one particle of a Bell state. We first explore four local unitary operations for the  $A$  particle (i.e., the first particle) of the constructed maximum entangled states. Obviously, similar to  $\sigma_0 = I$ , we can set the identical operation  $U_0^A = I$ .

We suppose that the local unitary operation  $U_1^A$  realizes the mutual transformation like Eq. (14), i.e.,

$$U_1^A: |\alpha_0\rangle \mapsto |\alpha_1\rangle, |\alpha_1\rangle \mapsto |\alpha_0\rangle, |\alpha_2\rangle \mapsto |\alpha_3\rangle, |\alpha_3\rangle \mapsto |\alpha_2\rangle. \quad (\text{A1})$$

Note that, in Eq. (A1), the results of  $U_1^A$  acting on the first particle of the four constructed states are allowed some

global phase shifts, which modulus are 1. Thereby,  $U_1^A \otimes I$  can be expressed as

$$\begin{aligned} U_1^A \otimes I &= e^{i\theta_0} |\alpha_1\rangle \langle \alpha_0| + e^{i\theta_1} |\alpha_0\rangle \langle \alpha_1| + e^{i\theta_2} |\alpha_3\rangle \langle \alpha_2| + e^{i\theta_3} |\alpha_2\rangle \langle \alpha_3| \\ &= \begin{pmatrix} \lambda_0 & 0 & 0 & \lambda_1 \\ 0 & \lambda_2 & \lambda_3 & 0 \\ 0 & \lambda_4 & -\lambda_2 & 0 \\ \lambda_5 & 0 & 0 & -\lambda_0 \end{pmatrix}, \end{aligned} \quad (\text{A2})$$

where  $\theta_0, \theta_1, \theta_2$ , and  $\theta_3$  are four real numbers,  $\lambda_0 = e^{i\theta_0} \bar{a}\bar{b} + e^{i\theta_1} ab$ ,  $\lambda_1 = e^{i\theta_0} \bar{b}^2 - e^{i\theta_1} a^2$ ,  $\lambda_2 = e^{i\theta_2} \bar{a}\bar{b} + e^{i\theta_3} ab$ ,  $\lambda_3 = e^{i\theta_2} \bar{b}^2 - e^{i\theta_3} a^2$ ,  $\lambda_4 = e^{i\theta_3} b^2 - e^{i\theta_2} \bar{a}^2$  and  $\lambda_5 = -e^{i\theta_0} \bar{a}^2 + e^{i\theta_1} b^2$ . Set  $U_1^A = (a_{ij})$ ,  $i, j \in \{1, 2\}$ , then

$$U_1^A \otimes I = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \otimes I = \begin{pmatrix} a_{11} & 0 & a_{12} & 0 \\ 0 & a_{11} & 0 & a_{12} \\ a_{21} & 0 & a_{22} & 0 \\ 0 & a_{21} & 0 & a_{22} \end{pmatrix}. \quad (\text{A3})$$

Combining Eqs. (A2) and (A3), we obtain

$$\begin{aligned} e^{i\theta_0} \bar{b}^2 - e^{i\theta_1} a^2 &= -e^{i\theta_0} \bar{a}^2 + e^{i\theta_1} b^2 = 0, \\ e^{i\theta_2} \bar{b}^2 - e^{i\theta_3} a^2 &= e^{i\theta_3} b^2 - e^{i\theta_2} \bar{a}^2 = 0, \\ a_{11} &= e^{i\theta_0} \bar{a}\bar{b} + e^{i\theta_1} ab = e^{i\theta_2} \bar{a}\bar{b} + e^{i\theta_3} ab, \\ a_{22} &= -e^{i\theta_0} \bar{a}\bar{b} - e^{i\theta_1} ab = -e^{i\theta_2} \bar{a}\bar{b} - e^{i\theta_3} ab, \\ a_{12} &= a_{21} = 0. \end{aligned} \quad (\text{A4})$$

Solving Eqs. (A4), we get  $e^{i\theta_0} = e^{i\theta_2}$  and  $e^{i\theta_1} = e^{i\theta_3} = e^{i\theta_0} \frac{\bar{b}^2}{\bar{a}^2} = e^{i\theta_0} \frac{\bar{a}^2}{b^2}$ . Note that, when the condition  $|a| = |b| = 1/\sqrt{2}$  holds,  $\bar{b}^2/a^2 = \bar{a}^2/b^2$  holds, too. Then, we have

$$U_1^A = e^{i\theta_0} \begin{pmatrix} \frac{\bar{b}}{a} & 0 \\ 0 & -\frac{\bar{b}}{a} \end{pmatrix} = 2\bar{a}\bar{b}e^{i\theta_0} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \quad (\text{A5})$$

In particular, when  $e^{i\theta_0} = 1/2\bar{a}\bar{b}$ ,

$$U_1^A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \sigma_1. \quad (\text{A6})$$

Similarly, we suppose that the local unitary operation  $U_2^A$  realizes the mutual transformation like Eq. (15), i.e.,

$$U_2^A: |\alpha_0\rangle \mapsto |\alpha_2\rangle, |\alpha_1\rangle \mapsto |\alpha_3\rangle, |\alpha_2\rangle \mapsto |\alpha_0\rangle, |\alpha_3\rangle \mapsto |\alpha_1\rangle. \quad (\text{A7})$$

Similar to  $U_1^A \otimes I$ ,  $U_2^A \otimes I$  can be expressed as

$$\begin{aligned} U_2^A \otimes I &= e^{i\theta_4} |\alpha_2\rangle\langle\alpha_0| + e^{i\theta_5} |\alpha_3\rangle\langle\alpha_1| + e^{i\theta_6} |\alpha_0\rangle\langle\alpha_2| + e^{i\theta_7} |\alpha_1\rangle\langle\alpha_3| \\ &= \begin{pmatrix} 0 & \mu_0 & \mu_1 & 0 \\ \mu_2 & 0 & 0 & \mu_3 \\ \mu_4 & 0 & 0 & \mu_2 \\ 0 & \mu_5 & \mu_0 & 0 \end{pmatrix}, \end{aligned} \quad (\text{A8})$$

where  $\theta_4, \theta_5, \theta_6$ , and  $\theta_7$  are four real numbers,  $\mu_0 = (e^{i\theta_6} + e^{i\theta_7})/2$ ,  $\mu_1 = e^{i\theta_6} \bar{a}b - e^{i\theta_7} a\bar{b}$ ,  $\mu_2 = (e^{i\theta_4} + e^{i\theta_5})/2$ ,  $\mu_3 = e^{i\theta_4} a\bar{b} - e^{i\theta_5} \bar{a}b$ ,  $\mu_4 = e^{i\theta_4} \bar{a}b - e^{i\theta_5} \bar{a}b$ ,  $\mu_5 = e^{i\theta_6} \bar{a}b - e^{i\theta_7} \bar{a}b$ . Set  $U_2^A = (b_{ij})$ ,  $i, j \in \{1, 2\}$ , then

$$U_2^A \otimes I = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \otimes I = \begin{pmatrix} b_{11} & 0 & b_{12} & 0 \\ 0 & b_{11} & 0 & b_{12} \\ b_{21} & 0 & b_{22} & 0 \\ 0 & b_{21} & 0 & b_{22} \end{pmatrix}. \quad (\text{A9})$$

Combining Eqs. (A8) and (A9), we obtain

$$\begin{aligned} e^{i\theta_4} + e^{i\theta_5} &= e^{i\theta_6} + e^{i\theta_7} = 0, \\ b_{12} &= e^{i\theta_6} \bar{a}b - e^{i\theta_7} a\bar{b} = e^{i\theta_4} \bar{a}b - e^{i\theta_5} a\bar{b}, \\ b_{21} &= e^{i\theta_4} \bar{a}b - e^{i\theta_5} \bar{a}b = e^{i\theta_6} \bar{a}b - e^{i\theta_7} \bar{a}b, \\ b_{11} &= b_{22} = 0. \end{aligned} \quad (\text{A10})$$

Solving Eqs. (A10), we get  $e^{i\theta_4} = e^{i\theta_6}$  and  $e^{i\theta_5} = e^{i\theta_7} = -e^{i\theta_4} |a|^2/|b|^2 = -e^{i\theta_4} |b|^2/|a|^2$ . Note that, when  $|a| = |b| = 1/\sqrt{2}$ ,  $-|a|^2/|b|^2 = -|b|^2/|a|^2 = -1$ . Then we have

$$U_2^A = e^{i\theta_4} \begin{pmatrix} 0 & \frac{a}{b} \\ \frac{\bar{a}}{b} & 0 \end{pmatrix} = e^{i\theta_4} \begin{pmatrix} 0 & 2a\bar{b} \\ 2\bar{a}b & 0 \end{pmatrix}. \quad (\text{A11})$$

In particular, when  $e^{i\theta_4} = 1$ ,

$$U_2^A = \begin{pmatrix} 0 & 2a\bar{b} \\ 2\bar{a}b & 0 \end{pmatrix}. \quad (\text{A12})$$

Last, we suppose that the local unitary operation  $U_3^A$  realizes the mutual transformation like Eq. (16), i.e.,

$$U_3^A: |\alpha_0\rangle \mapsto |\alpha_3\rangle, |\alpha_1\rangle \mapsto |\alpha_2\rangle, |\alpha_2\rangle \mapsto |\alpha_1\rangle, |\alpha_3\rangle \mapsto |\alpha_0\rangle. \quad (\text{A13})$$

Similar to  $U_1^A \otimes I$ ,  $U_3^A \otimes I$  can be expressed as

$$\begin{aligned} U_3^A \otimes I &= e^{i\theta_8} |\alpha_3\rangle\langle\alpha_0| + e^{i\theta_9} |\alpha_2\rangle\langle\alpha_1| + e^{i\theta_{10}} |\alpha_1\rangle\langle\alpha_2| + e^{i\theta_{11}} |\alpha_0\rangle\langle\alpha_3| \\ &= \begin{pmatrix} 0 & v_0 & v_1 & 0 \\ v_2 & 0 & 0 & v_3 \\ v_4 & 0 & 0 & -v_2 \\ 0 & v_5 & -v_0 & 0 \end{pmatrix}, \end{aligned} \quad (\text{A14})$$

where  $\theta_8, \theta_9, \theta_{10}$ , and  $\theta_{11}$  are four real numbers,  $v_0 = e^{i\theta_{10}} \bar{a}b + e^{i\theta_{11}} ab$ ,  $v_1 = e^{i\theta_{10}} \bar{b}^2 - e^{i\theta_{11}} a^2$ ,  $v_2 = e^{i\theta_8} \bar{a}b + e^{i\theta_9} ab$ ,  $v_3 = e^{i\theta_8} \bar{b}^2 - e^{i\theta_9} a^2$ ,  $v_4 = -e^{i\theta_8} \bar{a}^2 + e^{i\theta_9} b^2$ ,  $v_5 = -e^{i\theta_{10}} \bar{a}^2 + e^{i\theta_{11}} b^2$ . Set  $U_3^A = (c_{ij})$ ,  $i, j \in \{1, 2\}$ , then

$$U_3^A \otimes I = \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} \otimes I = \begin{pmatrix} c_{11} & 0 & c_{12} & 0 \\ 0 & c_{11} & 0 & c_{12} \\ c_{21} & 0 & c_{22} & 0 \\ 0 & c_{21} & 0 & c_{22} \end{pmatrix}. \quad (\text{A15})$$

Combining Eqs. (A14) and (A15), we obtain

$$\begin{cases} e^{i\theta_8} \bar{a}b + e^{i\theta_9} ab = 0, \\ e^{i\theta_{10}} \bar{a}b + e^{i\theta_{11}} ab = 0, \\ c_{12} = e^{i\theta_{10}} \bar{b}^2 - e^{i\theta_{11}} a^2 = e^{i\theta_8} \bar{b}^2 - e^{i\theta_9} a^2, \\ c_{21} = -e^{i\theta_8} \bar{a}^2 + e^{i\theta_9} b^2 = -e^{i\theta_{10}} \bar{a}^2 + e^{i\theta_{11}} b^2, \\ c_{11} = c_{22} = 0. \end{cases} \quad (\text{A16})$$

Solving Eqs. (A16), we get  $e^{i\theta_8} = e^{i\theta_{10}}$  and  $e^{i\theta_9} = e^{i\theta_{11}} = -e^{i\theta_8} \bar{a}b/ab$ . Then we have

$$U_3^A = e^{i\theta_8} \begin{pmatrix} 0 & \frac{\bar{b}}{a} \\ -\frac{\bar{a}}{a} & 0 \end{pmatrix}. \quad (\text{A17})$$

Note that, when  $|a| = |b| = 1/\sqrt{2}$ ,

$$U_3^A = e^{i\theta_8} \begin{pmatrix} 0 & \frac{\bar{b}}{a} \\ -\frac{\bar{a}}{a} & 0 \end{pmatrix} = e^{i\theta_8} \begin{pmatrix} 0 & 2\bar{b}^2 \\ -2\bar{a}^2 & 0 \end{pmatrix}. \quad (\text{A18})$$

In particular, when  $e^{i\theta_8} = 1$ ,

$$U_3^A = \begin{pmatrix} 0 & 2\bar{b}^2 \\ -2\bar{a}^2 & 0 \end{pmatrix}. \quad (\text{A19})$$

Clearly, when  $|a| = |b| = 1/\sqrt{2}$ , all  $U_1^A$ ,  $U_2^A$ , and  $U_3^A$  are unitary.

Now, we explore four local unitary operations for the  $B$  particle (i.e., the second particle) of the constructed maximum entangled states. Obviously, similar to  $\sigma_0 = I$ , we can set the identical operation  $U_0^B = I$ .

We suppose that the local unitary operations  $U_1^B, U_2^B$ , and  $U_3^B$  realize the mutual transformations like Eqs. (14), (15), and (16), respectively, i.e.,

$$U_1^B: |\alpha_0\rangle \mapsto |\alpha_1\rangle, |\alpha_1\rangle \mapsto |\alpha_0\rangle, |\alpha_2\rangle \mapsto |\alpha_3\rangle, |\alpha_3\rangle \mapsto |\alpha_2\rangle; \quad (\text{A20})$$

$$U_2^B: |\alpha_0\rangle \mapsto |\alpha_2\rangle, |\alpha_1\rangle \mapsto |\alpha_3\rangle, |\alpha_2\rangle \mapsto |\alpha_0\rangle, |\alpha_3\rangle \mapsto |\alpha_1\rangle; \quad (\text{A21})$$

$$U_3^B: |\alpha_0\rangle \mapsto |\alpha_3\rangle, |\alpha_1\rangle \mapsto |\alpha_2\rangle, |\alpha_2\rangle \mapsto |\alpha_1\rangle, |\alpha_3\rangle \mapsto |\alpha_0\rangle. \quad (\text{A22})$$



Via similar processes getting  $U_1^A$ ,  $U_2^A$ , and  $U_3^A$ , we can obtain  $U_1^B$ ,  $U_2^B$ , and  $U_3^B$  as

$$U_1^B = e^{i\theta'_0} \begin{pmatrix} \frac{\bar{b}}{a} & 0 \\ 0 & -\frac{\bar{b}}{a} \end{pmatrix} = 2\bar{a}\bar{b}e^{i\theta'_0} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad (\text{A23})$$

$$U_2^B = e^{i\theta'_4} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad (\text{A24})$$

$$U_3^B = e^{i\theta'_8} \begin{pmatrix} 0 & -\frac{\bar{b}}{a} \\ \frac{\bar{b}}{a} & 0 \end{pmatrix} = 2\bar{a}\bar{b}e^{i\theta'_8} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}. \quad (\text{A25})$$

Clearly, when  $|a| = |b| = 1/\sqrt{2}$ , both  $U_1^B$  and  $U_3^B$  are unitary.

In particular, when  $e^{i\theta'_0} = 1/2\bar{a}\bar{b}$ ,  $e^{i\theta'_4} = 1$ , and  $e^{i\theta'_8} = 1/2\bar{a}\bar{b}$ ,

$$U_1^B = \sigma_1, \quad (\text{A26})$$

$$U_2^B = \sigma_2, \quad (\text{A27})$$

and

$$U_3^B = i\sigma_3, \quad (\text{A28})$$

respectively.

### APPENDIX B: ENTANGLEMENT SWAPPING BETWEEN A GBELL STATE AND A BELL STATE

For clarity, we choose  $|\alpha_2\rangle$  in Eq. (17) and  $|\beta_2\rangle$  as an example to specify entanglement swapping, and analyze the result of entanglement swapping. After calculation, we get

$$|\alpha_2\rangle_{13} \otimes |\beta_2\rangle_{24} = \frac{1}{\sqrt{2}}(a|00\rangle_{12}|11\rangle_{34} + a|01\rangle_{12}|10\rangle_{34} + b|10\rangle_{12}|01\rangle_{34} + b|11\rangle_{12}|00\rangle_{34}). \quad (\text{B1})$$

Note that, the terms on the right side of Eq. (B1) exist only in  $|\alpha_2\rangle_{12}|\beta_2\rangle_{34}$ ,  $|\alpha_2\rangle_{12}|\beta_3\rangle_{34}$ ,  $|\alpha_3\rangle_{12}|\beta_2\rangle_{34}$ ,  $|\alpha_3\rangle_{12}|\beta_3\rangle_{34}$ ,  $|\alpha_0\rangle_{12}|\beta_0\rangle_{34}$ ,  $|\alpha_0\rangle_{12}|\beta_1\rangle_{34}$ ,  $|\alpha_1\rangle_{12}|\beta_0\rangle_{34}$ , and  $|\alpha_1\rangle_{12}|\beta_1\rangle_{34}$ .

Hence, we set

$$|\alpha_2\rangle_{13} \otimes |\beta_2\rangle_{24} = a_0|\alpha_2\rangle_{12}|\beta_2\rangle_{34} + a_1|\alpha_2\rangle_{12}|\beta_3\rangle_{34} + a_2|\alpha_3\rangle_{12}|\beta_2\rangle_{34} + a_3|\alpha_3\rangle_{12}|\beta_3\rangle_{34} + a_4|\alpha_0\rangle_{12}|\beta_0\rangle_{34} + a_5|\alpha_0\rangle_{12}|\beta_1\rangle_{34} + a_6|\alpha_1\rangle_{12}|\beta_0\rangle_{34} + a_7|\alpha_1\rangle_{12}|\beta_1\rangle_{34}. \quad (\text{B2})$$

Furthermore, we expand the items on the right hand of Eq. (B2) to obtain

$$\begin{aligned} & |\alpha_2\rangle_{13} \otimes |\beta_2\rangle_{24} \\ &= \frac{1}{\sqrt{2}}[(a_0a + a_1a + a_2\bar{b} + a_3\bar{b})|01\rangle_{12}|01\rangle_{34} \\ &+ (a_0a - a_1a + a_2\bar{b} - a_3\bar{b})|01\rangle_{12}|10\rangle_{34} \\ &+ (a_0b + a_1b - a_2\bar{a} - a_3\bar{a})|10\rangle_{12}|01\rangle_{34} \\ &+ (a_0b - a_1b - a_2\bar{a} + a_3\bar{a})|10\rangle_{12}|10\rangle_{34} \\ &+ (a_4a + a_5a + a_6\bar{b} + a_7\bar{b})|00\rangle_{12}|00\rangle_{34} \\ &+ (a_4a - a_5a + a_6\bar{b} - a_7\bar{b})|00\rangle_{12}|11\rangle_{34} \\ &+ (a_4b + a_5b - a_6\bar{a} - a_7\bar{a})|11\rangle_{12}|00\rangle_{34} \\ &+ (a_4b - a_5b - a_6\bar{a} + a_7\bar{a})|11\rangle_{12}|11\rangle_{34}]. \quad (\text{B3}) \end{aligned}$$

Comparing Eqs. (B1) and (B3), we have

$$\begin{cases} a_0a - a_1a + a_2\bar{b} - a_3\bar{b} = a, \\ a_0b + a_1b - a_2\bar{a} - a_3\bar{a} = b, \\ a_4a - a_5a + a_6\bar{b} - a_7\bar{b} = a, \\ a_4b + a_5b - a_6\bar{a} - a_7\bar{a} = b, \\ a_0a + a_1a + a_2\bar{b} + a_3\bar{b} = 0, \\ a_0b - a_1b - a_2\bar{a} + a_3\bar{a} = 0, \\ a_4a + a_5a + a_6\bar{b} + a_7\bar{b} = 0, \\ a_4b - a_5b - a_6\bar{a} + a_7\bar{a} = 0. \end{cases} \quad (\text{B4})$$

By solving the Eqs. (B4), we obtain  $a_0 = 1/2$ ,  $a_1 = 0$ ,  $a_2 = 0$ ,  $a_3 = -ab$ ,  $a_4 = 1/2$ ,  $a_5 = 0$ ,  $a_6 = 0$ , and  $a_7 = -ab$ . Substituting them into Eq. (B2), we get

$$\begin{aligned} |\alpha_2\rangle_{13} \otimes |\beta_2\rangle_{24} &= \frac{1}{2}|\alpha_0\rangle_{12}|\beta_0\rangle_{34} - ab|\alpha_1\rangle_{12}|\beta_1\rangle_{34} \\ &+ \frac{1}{2}|\alpha_2\rangle_{12}|\beta_2\rangle_{34} - ab|\alpha_3\rangle_{12}|\beta_3\rangle_{34}. \quad (\text{B5}) \end{aligned}$$

Furthermore, we can obtain the entangled swapping of any GBell state with any Bell state. For example,

$$\begin{aligned} |\alpha_2\rangle_{13} \otimes |\beta_3\rangle_{24} &= ab|\alpha_1\rangle_{12}|\beta_0\rangle_{34} - \frac{1}{2}|\alpha_0\rangle_{12}|\beta_1\rangle_{34} \\ &- ab|\alpha_3\rangle_{12}|\beta_2\rangle_{34} + \frac{1}{2}|\alpha_2\rangle_{12}|\beta_3\rangle_{34}, \quad (\text{B6}) \end{aligned}$$

$$\begin{aligned} |\alpha_3\rangle_{13} \otimes |\beta_2\rangle_{24} &= \frac{1}{2}|\alpha_1\rangle_{12}|\beta_0\rangle_{34} - \bar{a}\bar{b}|\alpha_0\rangle_{12}|\beta_1\rangle_{34} \\ &+ \frac{1}{2}|\alpha_3\rangle_{12}|\beta_2\rangle_{34} - \bar{a}\bar{b}|\alpha_2\rangle_{12}|\beta_3\rangle_{34}, \quad (\text{B7}) \end{aligned}$$

and

$$\begin{aligned}
 |\alpha_3\rangle_{13} \otimes |\beta_3\rangle_{24} = & \bar{a}\bar{b}|\alpha_0\rangle_{12}|\beta_0\rangle_{34} - \frac{1}{2}|\alpha_1\rangle_{12}|\beta_1\rangle_{34} \\
 & - \bar{a}\bar{b}|\alpha_2\rangle_{12}|\beta_2\rangle_{34} + \frac{1}{2}|\alpha_3\rangle_{12}|\beta_3\rangle_{34}. \quad (\text{B8})
 \end{aligned}$$

According to Eqs. (B5)–(B8), when we perform the Bell-basis measurement on the third and fourth particles, the first and second particles will be entangled.

In particular, if the coefficients  $a$  and  $b$  of the GBell states satisfy  $a = b = \pm 1/\sqrt{2}$ , then the entanglement swapping in Eqs. (B5)–(B8) exactly correspond to the entanglement swapping of Bell states  $|\beta_2\rangle$  and  $|\beta_3\rangle$  [38].

### APPENDIX C: THE CALCULATION OF EVOLUTION CHANNEL

According to Eq. (37), after the second particle of  $|\alpha_2\rangle$  being transmitted by the depolarizing channel  $\mathcal{E}_0$ , the evolution of  $|\alpha_2\rangle$  is

$$I_2 \otimes \mathcal{E}_0 : |\alpha_2\rangle\langle\alpha_2| \rightarrow \frac{p_0}{4}I_4 + (1-p_0)|\alpha_2\rangle\langle\alpha_2|, \quad (\text{C1})$$

i.e.,

$$I_2 \otimes \mathcal{E}_0 (|\alpha_2\rangle\langle\alpha_2|) = \frac{p_0}{4} \left( \sum_{i=0}^3 |\alpha_i\rangle\langle\alpha_i| \right) + (1-p_0)|\alpha_2\rangle\langle\alpha_2|. \quad (\text{C2})$$

Similarly, according to Eq. (36), after the second particle of  $|\beta_2\rangle$  being transmitted by the depolarizing channel  $\mathcal{E}_1$ , the evolution of  $|\beta_2\rangle$  is

$$I_2 \otimes \mathcal{E}_1 : |\beta_2\rangle\langle\beta_2| \rightarrow \frac{p_1}{4}I_4 + (1-p_1)|\beta_2\rangle\langle\beta_2|, \quad (\text{C3})$$

i.e.,

$$I_2 \otimes \mathcal{E}_1 (|\beta_2\rangle\langle\beta_2|) = \frac{p_1}{4} \left( \sum_{i=0}^3 |\beta_i\rangle\langle\beta_i| \right) + (1-p_1)|\beta_2\rangle\langle\beta_2|. \quad (\text{C4})$$

According to Eqs. (C2) and (C4), before entanglement swapping, the evolution of the joint state of Alice, Bob, and Charlie via  $\mathcal{E}_2 = I_2 \otimes \mathcal{E}_0 \otimes I_2 \otimes \mathcal{E}_1$  is

$$\begin{aligned}
 \mathcal{E}_2 : |\alpha_2\rangle\langle\alpha_2|_{13} \otimes |\beta_2\rangle\langle\beta_2|_{24} \rightarrow & (1-p_0)(1-p_1)|\alpha_2\rangle\langle\alpha_2|_{13} \otimes |\beta_2\rangle\langle\beta_2|_{24} \\
 & + \frac{p_1-p_0p_1}{4} |\alpha_2\rangle\langle\alpha_2|_{13} \otimes \left( \sum_{i=0}^3 |\beta_i\rangle\langle\beta_i| \right)_{24}
 \end{aligned}$$

$$\begin{aligned}
 & + \frac{p_0-p_0p_1}{4} \left( \sum_{i=0}^3 |\alpha_i\rangle\langle\alpha_i| \right)_{13} \otimes |\beta_2\rangle\langle\beta_2|_{24} \\
 & + \frac{p_0p_1}{16} \left( \sum_{i=0}^3 |\alpha_i\rangle\langle\alpha_i| \right)_{13} \otimes \left( \sum_{i=0}^3 |\beta_i\rangle\langle\beta_i| \right)_{24}, \quad (\text{C5})
 \end{aligned}$$

i.e.,

$$\begin{aligned}
 \mathcal{E}_2 : |\alpha_2\rangle\langle\alpha_2|_{13} \otimes |\beta_2\rangle\langle\beta_2|_{24} \rightarrow & (q_0q_1|\alpha_0\rangle\langle\alpha_0| + \frac{1-q_0q_1}{4} \sum_{i=0}^3 |\alpha_i\rangle\langle\alpha_i|)_{12} \otimes |\beta_0\rangle\langle\beta_0|_{34} \\
 & + (q_0q_1|\alpha_1\rangle\langle\alpha_1| + \frac{1-q_0q_1}{4} \sum_{i=0}^3 |\alpha_i\rangle\langle\alpha_i|)_{12} \otimes |\beta_1\rangle\langle\beta_1|_{34} \\
 & + (q_0q_1|\alpha_2\rangle\langle\alpha_2| + \frac{1-q_0q_1}{4} \sum_{i=0}^3 |\alpha_i\rangle\langle\alpha_i|)_{12} \otimes |\beta_2\rangle\langle\beta_2|_{34} \\
 & + (q_0q_1|\alpha_3\rangle\langle\alpha_3| + \frac{1-q_0q_1}{4} \sum_{i=0}^3 |\alpha_i\rangle\langle\alpha_i|)_{12} \otimes |\beta_3\rangle\langle\beta_3|_{34} \\
 & + \mathcal{O}, \quad (\text{C6})
 \end{aligned}$$

where  $q_0 = 1 - p_0$ ,  $q_1 = 1 - p_1$ , and  $\mathcal{O}$  represents the remaining term that cannot be measured. According to Eq. (C6), the evolution channel of the entangled state shared by Alice and Bob (the second particle of  $|\alpha_2\rangle$  being transmitted by the depolarizing channel  $\mathcal{E}_0$ , the second particle of  $|\beta_2\rangle$  being transmitted by the depolarizing channel  $\mathcal{E}_1$ , and Charlie's Bell-basis measurement) is modeled as

$$\mathcal{E} : \rho \rightarrow \frac{1-q_0q_1}{4}I_4 + q_0q_1\rho. \quad (\text{C7})$$

In Step 5, Alice and Bob send remaining entangled particles to Charlie through the depolarizing channel  $\mathcal{E}_0$  and the depolarizing channel  $\mathcal{E}_1$ , respectively. The joint evolution of the GBell states is

$$\mathcal{E}_0 \otimes \mathcal{E}_1 : \rho \rightarrow (I_2 \otimes \mathcal{E}_1)(\mathcal{E}_0 \otimes I_2)(\rho). \quad (\text{C8})$$

Let  $\mathcal{E}_4 = \mathcal{E}_0 \otimes \mathcal{E}_1$ , then

$$\begin{aligned}
 \mathcal{E}_4(\rho) = & (I_2 \otimes \mathcal{E}_1)(\mathcal{E}_0 \otimes I_2)(\rho) \\
 = & (I_2 \otimes \mathcal{E}_1) \left( \frac{p_0}{4} \sum_{i=0}^3 (U_i^A \otimes I_2) \rho (U_i^A \otimes I_2)^\dagger + (1-p_0)\rho \right) \\
 = & \frac{p_0p_1}{16} \sum_{i=0}^3 \sum_{j=0}^3 (U_i^A \otimes U_j^B) \rho (U_i^A \otimes U_j^B)^\dagger
 \end{aligned}$$

$$\begin{aligned}
 & + \frac{p_1 q_0}{4} \sum_{i=0}^3 (I_2 \otimes U_i^B) \rho (I_2 \otimes U_i^B)^\dagger \\
 & + \frac{p_0 q_1}{4} \sum_{i=0}^3 (U_i^A \otimes I_2) \rho (U_i^A \otimes I_2)^\dagger + q_0 q_1 \rho \\
 & = \frac{p_0 p_1}{16} (4I_4) + \frac{p_1 q_0}{4} I_4 + \frac{p_0 q_1}{4} I_4 + q_0 q_1 \rho \\
 & = \frac{1 - q_0 q_1}{4} I_4 + q_0 q_1 \rho. \tag{C9}
 \end{aligned}$$

Let  $\mathcal{E}' = \mathcal{E}_4 \circ \mathcal{E}$  be the channel of whole evolution, then

$$\begin{aligned}
 \mathcal{E}'(\rho) & = \mathcal{E}_4(\mathcal{E}_3(\rho)) \\
 & = \mathcal{E}_4\left(\frac{1 - q_0 q_1}{4} I_4 + q_0 q_1 \rho\right) \\
 & = (1 - q_0 q_1) \mathcal{E}_4\left(\frac{1}{4} I_4\right) + q_0 q_1 \mathcal{E}_4(\rho) \\
 & = \frac{1 - q_0 q_1}{4} I_4 + q_0 q_1 \mathcal{E}_4(\rho) \\
 & = \frac{1 - q_0 q_1}{4} I_4 + q_0 q_1 \left(\frac{1 - q_0 q_1}{4} I_4 + q_0 q_1 \rho\right) \\
 & = \frac{1 - q_0^2 q_1^2}{4} I_4 + q_0^2 q_1^2 \rho. \tag{C10}
 \end{aligned}$$

- 
- [1] Albert Einstein, Boris Podolsky, and Nathan Rosen, Can quantum-mechanical description of physical reality be considered complete?, *Phys. Rev.* **47**, 777 (1935).
  - [2] Erwin Schrödinger, Discussion of probability relations between separated systems, *Math. Proc. Camb. Philos. Soc.* **31**, 555 (1935).
  - [3] John S. Bell, On the Einstein Podolsky Rosen paradox, *Phys. Physique Fizika* **1**, 195 (1964).
  - [4] Stuart J. Freedman and John F. Clauser, Experimental test of local hidden-variable theories, *Phys. Rev. Lett.* **28**, 938 (1972).
  - [5] Alain Aspect, Jean Dalibard, and Gérard Roger, Experimental test of Bell's inequalities using time-varying analyzers, *Phys. Rev. Lett.* **49**, 1804 (1982).
  - [6] Marissa Giustina *et al.*, Significant-loophole-free test of Bell's theorem with entangled photons, *Phys. Rev. Lett.* **115**, 250401 (2015).
  - [7] Dik Bouwmeester, Jian-Wei Pan, Klaus Mattle, Manfred Eibl, Harald Weinfurter, and Anton Zeilinger, Experimental quantum teleportation, *Nature* **390**, 575 (1997).
  - [8] Jian-Wei Pan, Dik Bouwmeester, Harald Weinfurter, and Anton Zeilinger, Experimental entanglement swapping: entangling photons that never interacted, *Phys. Rev. Lett.* **80**, 3891 (1998).
  - [9] Xiongfeng Ma, Chi-Hang Fred Fung, and Hoi-Kwong Lo, Quantum key distribution with entangled photon sources, *Phys. Rev. A* **76**, 012307 (2007).
  - [10] Gui-Lu Long and Xiao-Shu Liu, Theoretically efficient high-capacity quantum-key-distribution scheme, *Phys. Rev. A* **65**, 032302 (2002).
  - [11] Fu-Guo Deng, Gui Lu Long, and Xiao-Shu Liu, Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block, *Phys. Rev. A* **68**, 042317 (2003).
  - [12] Fu-Guo Deng and Gui Lu Long, Secure direct communication with a quantum one-time pad, *Phys. Rev. A* **69**, 052319 (2004).
  - [13] Gui-Lu Long, Fu-Guo Deng, Chuan Wang, Xi-Han Li, Kai Wen, and Wan-Ying Wang, Quantum secure direct communication and deterministic secure quantum communication, *Front. Phys. China* **2**, 251 (2007).
  - [14] Charles H. Bennett and Stephen J. Wiesner, Communication via one-and two-particle operators on Einstein-Podolsky-Rosen states, *Phys. Rev. Lett.* **69**, 2881 (1992).
  - [15] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters, Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels, *Phys. Rev. Lett.* **70**, 1895 (1993).
  - [16] Lov K. Grover, in *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing* (ACM, Philadelphia PA, 1996), p. 212.
  - [17] Peter W. Shor, in *Proceedings 35th Annual Symposium on the Foundations of Computer Science* (IEEE, Santa Fe, NM, 1994), p. 124.
  - [18] Robert Raussendorf and Hans J. Briegel, A one-way quantum computer, *Phys. Rev. Lett.* **86**, 5188 (2001).
  - [19] C. H. Bennett and G Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, Bangalore India, 1984), p. 175.
  - [20] Charles H. Bennett, Quantum cryptography using any two nonorthogonal states, *Phys. Rev. Lett.* **68**, 3121 (1992).
  - [21] Hoi-Kwong Lo, Hoi Fung Chau, Unconditional security of quantum key distribution over arbitrarily long distances, *Science* **283**, 2050 (1999).
  - [22] Peter W. Shor and John Preskill, Simple proof of security of the BB84 quantum key distribution protocol, *Phys. Rev. Lett.* **85**, 441 (2000).
  - [23] Dominic Mayers, Unconditional security in quantum cryptography, *J. ACM (JACM)* **48**, 351 (2001).
  - [24] Lluís Masanes, Stefano Pironio, and Antonio Acín, Secure device-independent quantum key distribution with causally independent measurement devices, *Nat. Commun.* **2**, 1 (2011).
  - [25] Hoi-Kwong Lo, Marcos Curty, and Bing Qi, Measurement-device-independent quantum key distribution, *Phys. Rev. Lett.* **108**, 130503 (2012).
  - [26] Marcos Curty, Feihu Xu, Wei Cui, Charles Ci Wen Lim, Kiyoshi Tamaki, and Hoi-Kwong Lo, Finite-key analysis for measurement-device-independent quantum key distribution, *Nat. Commun.* **5**, 1 (2014).
  - [27] Chuan Wang, Fu-Guo Deng, Yan-Song Li, Xiao-Shu Liu, and Gui Lu Long, Quantum secure direct communication with high-dimension quantum superdense coding, *Phys. Rev. A* **71**, 044305 (2005).
  - [28] Chao Zheng and GuoFei Long, Quantum secure direct dialogue using Einstein-Podolsky-Rosen pairs, *Sci. China Phys., Mech. Astron.* **57**, 1238 (2014).

- [29] Yu-Bo Sheng, Lan Zhou, and Gui-Lu Long, One-step quantum secure direct communication, *Sci. Bull.* **67**, 367 (2022).
- [30] Zhengwen Cao, Lei Wang, Kexin Liang, Geng Chai, and Jinye Peng, Continuous-variable quantum secure direct communication based on Gaussian mapping, *Phys. Rev. Appl.* **16**, 024012 (2021).
- [31] Kexin Liang, Zhengwen Cao, Xinlei Chen, Lei Wang, Geng Chai, and Jinye Peng, A quantum secure direct communication scheme based on intermediate-basis, *Front. Phys.* **18**, 51301 (2023).
- [32] Dong Pan, Gui-Lu Long, Liuguo Yin, Yu-Bo Sheng, Dong Ruan, Soon Xin Ng, Jianhua Lu, and Lajos Hanzo, The evolution of quantum secure direct communication: On the road to the qinternet, *IEEE Commun. Surv. Tutor.* (2024).
- [33] Ruoyang Qi, Zhen Sun, Zaisheng Lin, Penghao Niu, Wentao Hao, Liyuan Song, Qin Huang, Jiancun Gao, Liuguo Yin, and Gui-Lu Long, Implementation and security analysis of practical quantum secure direct communication, *Light: Sci. Appl.* **8**, 22 (2019).
- [34] Zhantong Qi, Yuanhua Li, Yiwen Huang, Juan Feng, Yuanlin Zheng, and Xianfeng Chen, A 15-user quantum secure direct communication network, *Light: Sci. Appl.* **10**, 183 (2021).
- [35] Xin Liu, Di Luo, Guangshen Lin, Zihao Chen, Chunfeng Huang, Shizhuo Li, Chengxian Zhang, Zhenrong Zhang, and Kejin Wei, Fiber-based quantum secure direct communication without active polarization compensation, *Sci. China Phys. Mech. Astron.* **65**, 120311 (2022).
- [36] Haoran Zhang, Zhen Sun, Ruoyang Qi, Liuguo Yin, Gui-Lu Long, and Jianhua Lu, Realization of quantum secure direct communication over 100 km fiber with time-bin and phase quantum states, *Light: Sci. Appl.* **11**, 83 (2022).
- [37] Zhengwen Cao, Yuan Lu, Geng Chai, Hao Yu, Kexin Liang, and Lei Wang, Realization of quantum secure direct communication with continuous variable, *Research* **6**, 0193 (2023).
- [38] Peng-Hao Niu, Zeng-Rong Zhou, Zai-Sheng Lin, Yu-Bo Sheng, Liu-Guo Yin, and Gui-Lu Long, Measurement-device-independent quantum communication without encryption, *Sci. Bull.* **63**, 1345 (2018).
- [39] Zikai Gao, Tao Li, and Zhenhua Li, Long-distance measurement-device-independent quantum secure direct communication, *Europhys. Lett.* **125**, 40004 (2019).
- [40] Lan Zhou, Yu-Bo Sheng, and Gui-Lu Long, Device-independent quantum secure direct communication against collective attacks, *Sci. Bull.* **65**, 12 (2020).
- [41] Lan Zhou and Yu-Bo Sheng, One-step device-independent quantum secure direct communication, *Sci. China Phys. Mech. Astron.* **65**, 250311 (2022).
- [42] Lan Zhou, Bao-Wen Xu, Wei Zhong, and Yu-Bo Sheng, Device-independent quantum secure direct communication with single-photon sources, *Phys. Rev. Appl.* **19**, 014036 (2023).
- [43] Hui Zeng, Ming-Ming Du, Wei Zhong, Lan Zhou, and Yu-Bo Sheng, High-capacity device-independent quantum secure direct communication based on hyper-encoding, *Fundam. Res.* (2024).
- [44] ZengRong Zhou, YuBo Sheng, PengHao Niu, LiuGuo Yin, GuiLu Long, and Lajos Hanzo, Measurement-device-independent quantum secure direct communication, *Sci. China Phys. Mech. Astron.* **63**, 1 (2020).
- [45] Xu-Dong Wu, Lan Zhou, Wei Zhong, and Yu-Bo Sheng, High-capacity measurement-device-independent quantum secure direct communication, *Quantum Inf. Process.* **19**, 1 (2020).
- [46] Nayana Das and Goutam Paul, Measurement device-independent quantum secure direct communication with user authentication, *Quantum Inf. Process.* **21**, 260 (2022).
- [47] Jia-Wei Ying, Lan Zhou, Wei Zhong, and Yu-Bo Sheng, Measurement-device-independent one-step quantum secure direct communication, *Chin. Phys. B* **31**, 120303 (2022).
- [48] Michael A. Nielsen and Isaac Chuang, Quantum computation and quantum information, (2002).
- [49] Charles H. Bennett, David P. DiVincenzo, John A. Smolin, and William K. Wootters, Mixed-state entanglement and quantum error correction, *Phys. Rev. A* **54**, 3824 (1996).
- [50] Claude E. Shannon, Communication theory of secrecy systems, *The Bell System Technical Journal* **28**, 656 (1949).
- [51] Aaron D. Wyner, The wire-tap channel, *Bell System Technical Journal* **54**, 1355 (1975).
- [52] Andrew Thangaraj, Souvik Dihadar, A. Robert Calderbank, Steven W. McLaughlin, and Jean-Marc Merolla, Applications of LDPC codes to the wiretap channel, *IEEE Trans. Inf. Theory* **53**, 2933 (2007).
- [53] Himanshu Tyagi and Alexander Vardy, Universal hashing for information-theoretic security, *Proc. IEEE* **103**, 1781 (2015).
- [54] Peng-Hao Niu, Jia-Wei Wu, Liu-Guo Yin, and Gui-Lu Long, Security analysis of measurement-device-independent quantum secure direct communication, *Quantum Inf. Process.* **19**, 356 (2020).
- [55] Renato Renner, Symmetry of large physical systems implies independence of subsystems, *Nat. Phys.* **3**, 645 (2007).
- [56] Jiawei Wu, Zaisheng Lin, Liuguo Yin, and Gui-Lu Long, Security of quantum secure direct communication based on Wyner's wiretap channel theory, *Quantum Eng.* **1**, e26 (2019).
- [57] Alexander Semenovich Holevo, Bounds for the quantity of information transmitted by a quantum communication channel, *Problemy Peredachi Informatsii* **9**, 3 (1973).