Eur. Phys. J. D **44**, 607–617 (2007)
DOI: 10.1140/epjd/e2007-00237-y

THE EUROPEAN
PHYSICAL JOURNAL D

Multi-particle and high-dimension controlled order rearrangement encryption protocols

Y. Cao[a], A.-M. Wang[b], X.-S. Ma, and N.-B. Zhao

Department of Modern Physics, University of Science and Technology of China, Hefei 230026, P.R. China

Received 25 October 2006 / Received in final form 9 January 2007
Published online 20 July 2007 – © EDP Sciences, Società Italiana di Fisica, Springer-Verlag 2007

Abstract. Based on controlled order rearrange encryption (CORE) for quantum key distribution using EPR pairs [Fu.G. Deng, G.L. Long, Phys. Rev. A **68**, 042315 (2003)], we propose generalized controlled order rearrangement encryption (GCORE) protocols of N qubits and N qutrits, and concretely display them in cases using 3-qubit, 2-qutrit maximally entangled basis states. We further show that our protocols will become safer with an increase in dimensions and number of particles. Moreover, we carry out the security analysis using quantum covariant cloning machine. Although the applications of the generalized scheme need to be further studied, GCORE has many distinct features such as large capacity and high efficiency.

PACS. 03.67.Dd Quantum cryptography – 03.67.Hk Quantum communication

1 Introduction

Cryptography is the art of providing secure communication over insecure communication channels. Currently, in the information age, the safe of transmission of secret information is getting more and more important. One essential theme of secure communication is to the distribution of secret keys between sender and receiver. The security of quantum cryptography (QC) stems from the fundamental principles of quantum mechanics rather than classical cryptography. An important application of QC is the quantum key distribution (QKD), which concerns the generation and distribution of secret key between two legitimate users. The security of key distribution is the most important part of the secret communication. QKD exploits quantum mechanics principles for secret communication, which provides a secure way for transmitting the key. To date, there are many quantum secret key protocols such as BB84, Ekt91, B92, six-state protocol etc. [1–6], and new quantum secret key protocols [7–16] are continually suggested.

The security of some QKD protocols in references [1–3, 7, 11–18] is based on a random choices of a different measuring-bias, so randomness is usually a useful ingredient in QC. The security of other QKD protocols in references [8, 9, 19–21] relies on the nonlocality of quantum systems. The Goldenberg-Vaidman scheme [8] first proposed a QKD protocol using two transmission lines. This protocol uses orthogonal states and has full efficiency; all the particles transmitted are used to generate secret keys. Then, the Koashi-Imoto protocol [9] improves upon the Goldenberg-Vaidman scheme by using an asymmetric interferometer to reduce the time delay. However, two factors meant that the time delay of these schemes could not be too short. Subsequently, Deng and Long proposed a controlled order rearrange encryption (CORE) scheme [10] to overcome this drawback and realize secure QKD. In nonlocality based QKD protocols, orthogonal quantum states are used. Security is assured by not allowing an eavesdropper to acquire both parts simultaneously.

Currently, the CORE technique is not only suitable for use with Einstein-Podolsky-Rosen (EPR) pairs, but is also suitable for use with other quantum information carriers (QICs) [10]. In recent years researchers have drawn their attention to QKD protocols that involve multilevel systems with two parties, or multiple parties with two-level systems. The motivation for studying multilevel QKD is that more information can be carried by each particle, and thereby the information flux is increased. As well some multilevel protocols have been shown to have greater security against eavesdropping attacks than their qubit-based counterparts [20, 24, 25]. Thus, the use of multi-particle, maximally entangled states can further guarantee security and has higher efficiency in general.

In this paper, our main purpose is to generalize the CORE of QC to multi-particle and/or high dimension quantum systems. Our generalized protocols have higher efficiency, because the generalized protocols, which are herein referred to as the GCORE here, exploit the flollowing facts that a possible eavesdropper without

[a] e-mail: caoy1209@mail.ustc.edu.cn
[b] e-mail: anmwang@ustc.edu.cn

simultaneous access to the entire quantum system cannot recover all the information without being detected, and the protocols employ a larger alphabet, a few-dimensional orthogonal basis set of pure states. Consequently, we obtain the maximal efficiency from this system. Based on the reasoning that transmitted N-qudit maximally entangled states can send $\log_2 d^N$ bits of information in our schemes, if we assume there are N particles with each being d dimensions, the generalized protocols also have great capacity.

The paper is organized as follows. In Section 2, we review the CORE protocol using EPR pairs provided by Deng and Long. Then we generalize the CORE protocol to the N-qubit case, specially, we present the GCORE protocol using 3-qubit state and check its security by the correlated matrix method. In Section 3, the GCORE protocol using N qutrits is proposed, and the GCORE protocol using 2-qutrit is presented in detail. Moveover, we discuss the security of qutrit GCORE using the quantum covariant cloning machine. In Section 4, we present a uniform expression for a multi-particle and/or high dimension situation. Finally, the advantages of GCORE are explained and concluding remarks are given.

2 GCORE using N-qubit maximally entangled basis states

2.1 Explanation of CORE protocol

To begin, let us briefly review the meaning of CORE. Firstly, we assume that the keys are distributed between Alice and Bob. Before transmission, Alice rearranges the order of correlated particles and sends them to Bob. The aim of random rearrangement is to prevent the eavesdropper from obtaining correlated particles simultaneously from different transmission channels, and an evening process is also required to make the transmission occur in equally spaced time intervals. Once Bob receives these particles, he restores the order of the particles and undoes Alice's operations by synchronizing their measurement devices, repeatedly using a priori shared control key, so that he can make an orthogonal basis measurement. Their measurement outcome is exactly what Alice has prepared. The essence of CORE is the use of a control key as has been used in the modified BB84 scheme [7]. The noncloning nature ensures that it is viable.

The whole process of the CORE protocol using EPR states has been demonstrated clearly in reference [10]. In the following text, we generalize it to multi-particle and high-dimensional cases, and therefore the generalized protocol is denoted as GCORE.

2.2 GCORE protocol using GHZ-basis states

In the following section, we first discuss a concrete GCORE example using 3-qubit GHZ-basis states without loss of generality.

(i) Alice randomly generates a sequence of GHZ-basis states $(a_1, b_1, c_1), \cdots, (a_m, b_m, c_m)$, where (a_i, b_i, c_i) denotes one GHZ-basis state ($1 \leq i \leq m, m$ is an integer) and each eight adjoining triplets are taken as one unit of QIC. Without loss of generality, we consider the first carrier units $[(a_1, b_1, c_1), (a_2, b_2, c_2), \cdots, (a_8, b_8, c_8)]$-which are randomly placed with the eight GHZ-basis states-and that can be expressed as [26]:

$$\left|\psi_j^{\pm}\right\rangle = \frac{1}{\sqrt{2}} \left(|j\rangle_{AB} |0\rangle_C \pm |3-j\rangle_{AB} |1\rangle_C\right), \qquad (1)$$

where $j = j_1 j_2$ denotes binary notations. In their explicit forms, eight GHZ-basis states are:

$$\begin{aligned}
\left|\psi_0^{+}\right\rangle &= \left(|000\rangle + |111\rangle\right)/\sqrt{2} \\
\left|\psi_0^{-}\right\rangle &= \left(|000\rangle - |111\rangle\right)/\sqrt{2} \\
\left|\psi_1^{+}\right\rangle &= \left(|010\rangle + |101\rangle\right)/\sqrt{2} \\
\left|\psi_1^{-}\right\rangle &= \left(|010\rangle - |101\rangle\right)/\sqrt{2} \\
\left|\psi_2^{+}\right\rangle &= \left(|100\rangle + |011\rangle\right)/\sqrt{2} \\
\left|\psi_2^{-}\right\rangle &= \left(|100\rangle - |011\rangle\right)/\sqrt{2} \\
\left|\psi_3^{+}\right\rangle &= \left(|110\rangle + |001\rangle\right)/\sqrt{2} \\
\left|\psi_3^{-}\right\rangle &= \left(|110\rangle - |001\rangle\right)/\sqrt{2}) \qquad (2)
\end{aligned}$$

and we denote them by 000, 001, 010, 011, 100, 101, 110, and 111, respectively.

(ii) Alice sends the three parts out at equal regular time intervals to Bob through three channels. Before these GHZ-basis states enter into the insecure transmission channel, their orders are rearranged by the GCORE system. There are eight choices of GCORE operations; the corresponding relationships are the following:

$$\begin{array}{llll}
E_0 \leftrightarrow 000, & E_1 \leftrightarrow 001, & E_2 \leftrightarrow 010, & E_3 \leftrightarrow 011 \\
E_4 \leftrightarrow 100, & E_5 \leftrightarrow 101, & E_6 \leftrightarrow 110, & E_7 \leftrightarrow 111
\end{array}$$

and the GCORE is done performed for the eight GHZ-basis states. Let us use permutation group notation to express them as follows

$$E_0 = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8 \\ 1\,2\,3\,4\,5\,6\,7\,8 \end{pmatrix} = (1)\,(2)\,(3)\,(4)\,(5)\,(6)\,(7)\,(8)$$

$$E_1 = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8 \\ 2\,1\,4\,3\,6\,5\,8\,7 \end{pmatrix} = (1\,2)\,(3\,4)\,(5\,6)\,(7\,8)$$

$$E_2 = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8 \\ 3\,4\,1\,2\,7\,8\,5\,6 \end{pmatrix} = (1\,3)\,(2\,4)\,(5\,7)\,(6\,8)$$

$$E_3 = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8 \\ 4\,3\,2\,1\,8\,7\,6\,5 \end{pmatrix} = (1\,4)\,(2\,3)\,(5\,8)\,(6\,7)$$

$$E_4 = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8 \\ 5\,6\,7\,8\,1\,2\,3\,4 \end{pmatrix} = (1\,5)\,(2\,6)\,(3\,7)\,(4\,8)$$

$$E_5 = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8 \\ 8\,7\,6\,5\,4\,3\,2\,1 \end{pmatrix} = (1\,8)\,(2\,7)\,(3\,6)\,(4\,5)$$

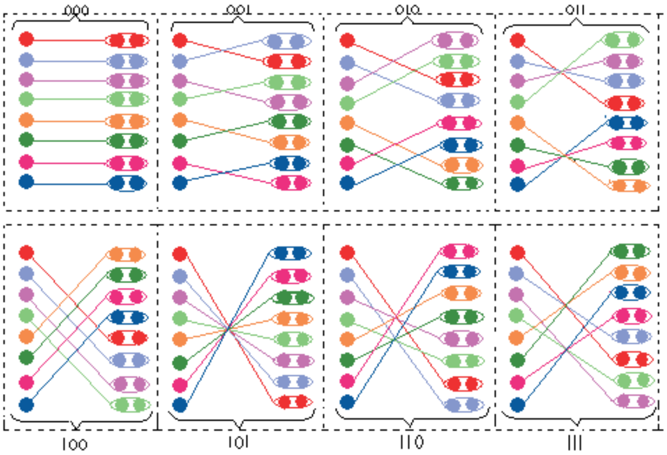

Fig. 1. (Color online) Example of GCORE using GHZ-basis states. There are eight different GCORE operations.

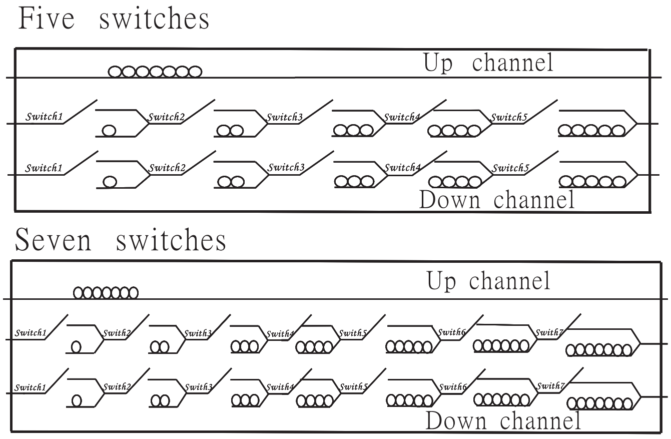

Fig. 2. Devices to perform GCORE operations, the loop represents a time delay of a fixed interval.

$$E_6 = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8 \\ 7\,8\,5\,6\,3\,4\,1\,2 \end{pmatrix} = (1\ 7)\,(2\ 8)\,(3\ 5)\,(4\ 6)$$

$$E_7 = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8 \\ 6\,5\,8\,7\,2\,1\,4\,3 \end{pmatrix} = (1\ 6)\,(2\ 5)\,(3\ 8)\,(4\ 7)$$

we also show this protocol using Figure 1.

The three quantum channels in this GCORE protocol are denoted upper, middle, and lower channels. The upper QIC parts are transmitted according to their temporal orders. A control key is used to rearrange the order of the middle and lower QIC parts. For instance, if the value of control key is 000, the operation E_0 is applied. In Figure 2 there are seven switches and the order of eight GHZ-basis states are unchange when switches 1, 2, 3, 4, 5, 6, 7 are in positions (up, up, up, up, up, up, down). When the value of the control key is 001, the operation E_1 is performed, done by putting the seven switches into positions (down, up, up, up, up, up, down), (up, up, up, up, up, down, up), (down, up, up, up, up, up, down), (up, up, up, up, up, down, up), (down, up, up, up, up, up, down), (up, up, up, up, up, down, up), (down, up, up, up, up, up, down), (up, up, up, up, up, down, up) for the eight particles, respectively. In fact, five switches are enough. The operation E_1 can be performed, by putting the five switches into positions (down, down, up, up, down), (up, down, up, down, up), (down, down, up, up, down), (up, down, up, down, up), (down, down, up, up, down), (up, down, up, down, up), (down, down, up, up, down), (up, down, up, down, up) for the eight particles, respectively. The effect of using seven switches is the same as that of using five switches. Similar combination can be written explicitly for operations $E_2, E_3, E_4, E_5, E_6, E_7$.

(iii) Bob undoes the effect of order rearrangement. At Bob's site, he simply exchanges the upper, middle, and lower parts of Alice's GCORE apparatus, and the GCORE operations performed by Alice will be undone.

(iv) Bob measures these carrier units to obtain the key. After these particles are rearranged, Bob uses the GHZ-basis measurement to read out the information determinatively, which is exactly the same as the one Alice prepared because the measurement is an orthogonal basis one and obviously the eight GHZ-basis states are mutually orthogonal.

Remark: to prevent Eve from stealing, we need an evening process to ensure the same time interval between the travel of different batches of QICs. Now, we need three transmission lines to ensure the application of current proposed scheme because 3-qubit GCORE uses GHZ-basis state, and each particle transmits through a quantum transmission line in equal time intervals. It is obviously different from the case using two-transmission lines in references [8,9]. Detailed analysis will be presented in subsection C below. In addition, the control keys can be used to control the GCORE operation of a group of units to reduce the usage of resources. For example, instead of using GCORE 001 to control operation of one unit of QICs (eight GHZ-basis states), we can use 001 to control more consecutive units of QICs, say 4 units or 32 GHZ-basis states.

2.3 Security of GCORE using GHZ-basis states

Let us look at the security of GCORE using 3-qubit GHZ-basis states. Eve has only a 1/8th chance to guess the right GCORE operation for the eight GHZ-basis states. If she uses the wrong GCORE operation, the three particles measured by her will be anticorrelated. Firstly if we assume that particle A from the first GHZ-basis state, particle B from the second GHZ-basis state and particle C from the third GHZ-basis state are mistreated by Eve as a GHZ-basis state, then the density operator will be

$$\begin{aligned} \rho_{A_1B_2C_3} &= \tilde{\rho}_{A_1} \otimes \tilde{\rho}_{B_2} \otimes \tilde{\rho}_{C_3} \\ &= \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix} \otimes \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix} \otimes \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix} = \frac{1}{8} I_{8\times 8} \end{aligned} \quad (3)$$

where $\tilde{\rho}_{A_1} = \mathrm{Tr}_{B_1C_1}\left(\rho_{A_1B_1C_1}\right), \tilde{\rho}_{B_2} = \mathrm{Tr}_{A_2C_2}\left(\rho_{A_2B_2C_2}\right), \tilde{\rho}_{C_3} = \mathrm{Tr}_{A_3B_3}\left(\rho_{A_3B_3C_3}\right)$. When $\rho_{A_1B_2C_3}$ is measured in the GHZ-basis state, the result can be any one of eight GHZ-basis states with 12.5%

probability each. Thus Eve will introduce a 66.99% error rate in the results. Next, if we assume particle A from the first GHZ-basis state, and particles B C from the second GHZ-basis state are mistreated by Eve as a GHZ-basis state, then the density operator will be

$$\rho_{A_1B_2C_3} = \tilde{\rho}_{A_1} \otimes \tilde{\rho}_{B_2C_3} = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix} \otimes \begin{pmatrix} \frac{1}{2} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{2} \end{pmatrix}. \quad (4)$$

Eve will introduce a 76.56% error rate in these results. In both situations, Alice and Bob can detect Eve easily by checking a sufficiently large subset of randomly chosen results.

Surely, Eve can perform a generalized Bell inequality measurement on the particles, but it will be ineffective in decrypting the control key. Let us choose $\boldsymbol{a}\,(a_x, a_y, a_z)$, $\boldsymbol{b}\,(b_x, b_y, b_z)$, as the directions of Alice and Bob's measurements, and at the same time, $\boldsymbol{c}\,(c_x, c_y, c_z)$ is also Bob's measurement direction. Then the correlation operator can be written as following:

$$\hat{E} = (\hat{\sigma} \cdot \boldsymbol{a}) \otimes (\hat{\sigma} \cdot \boldsymbol{b}) \otimes (\hat{\sigma} \cdot \boldsymbol{c}) \quad (5)$$

where $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

The expectation values $\langle E\,(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c})\rangle_{\psi} = \langle\psi|\,(\hat{\sigma}\cdot\boldsymbol{a})\otimes(\hat{\sigma}\cdot\boldsymbol{b})\otimes(\hat{\sigma}\cdot\boldsymbol{c})\,|\psi\rangle$ are different for different GHZ-basis states. They are

$$\begin{aligned}
\langle E\,(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c})\rangle_{\psi_0^+} &= (a_x - ia_y)\,(b_x - ib_y)\,(c_x - ic_y) \\
&\quad + (a_x + ia_y)\,(b_x + ib_y)\,(c_x + ic_y) \\
\langle E\,(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c})\rangle_{\psi_0^-} &= -\,(a_x - ia_y)\,(b_x - ib_y)\,(c_x - ic_y) \\
&\quad - (a_x + ia_y)\,(b_x + ib_y)\,(c_x + ic_y) \\
\langle E\,(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c})\rangle_{\psi_1^+} &= (a_x - ia_y)\,(b_x + ib_y)\,(c_x - ic_y) \\
&\quad + (a_x + ia_y)\,(b_x - ib_y)\,(c_x + ic_y) \\
\langle E\,(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c})\rangle_{\psi_1^-} &= -\,(a_x - ia_y)\,(b_x + ib_y)\,(c_x - ic_y) \\
&\quad - (a_x + ia_y)\,(b_x - ib_y)\,(c_x + ic_y) \\
\langle E\,(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c})\rangle_{\psi_2^+} &= (a_x + ia_y)\,(b_x - ib_y)\,(c_x - ic_y) \\
&\quad + (a_x - ia_y)\,(b_x + ib_y)\,(c_x + ic_y) \\
\langle E\,(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c})\rangle_{\psi_2^-} &= -\,(a_x + ia_y)\,(b_x - ib_y)\,(c_x - ic_y) \\
&\quad - (a_x - ia_y)\,(b_x + ib_y)\,(c_x + ic_y) \\
\langle E\,(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c})\rangle_{\psi_3^+} &= (a_x + ia_y)\,(b_x + ib_y)\,(c_x - ic_y) \\
&\quad + (a_x - ia_y)\,(b_x - ib_y)\,(c_x + ic_y) \\
\langle E\,(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c})\rangle_{\psi_3^-} &= -\,(a_x + ia_y)\,(b_x + ib_y)\,(c_x - ic_y) \\
&\quad - (a_x - ia_y)\,(b_x - ib_y)\,(c_x + ic_y)\,. \quad (6)
\end{aligned}$$

Note their coefficients are 1/2.

For the product states $|000\rangle$, $|001\rangle$, $|010\rangle$, $|011\rangle$, $|100\rangle$, $|101\rangle$, $|110\rangle$, $|111\rangle$, the expected values are:

$$\begin{aligned}
&a_zb_zc_z, \quad -a_zb_zc_z, \quad -a_zb_zc_z, \quad a_zb_zc_z, \\
&-a_zb_zc_z, \quad a_zb_zc_z, \quad a_zb_zc_z, \quad -a_zb_zc_z \quad (7)
\end{aligned}$$

respectively. If Eve takes a general Bell inequality measurement on three uncorrelated particles, she will get 0 for a large number of measurements when the particles are randomly distributed among the eight GHZ-basis states. If Eve takes three correlated particles, she will also get 0 because eight GHZ-basis states are taken with equal probability. So Eve can gain no information about the control key except for guessing it randomly. Because the control key can be repeatedly used, the probability that Eve by guessing the right control key is $\left(\frac{1}{2}\right)^{3N_k}$, where $3N_k$ is the number of bits in the control key. When $N_k = 100$, the probability is $\left(\frac{1}{8}\right)^{100}$, which is practically zero.

Naturally, the GCORE protocol is suitable to a N-qubit setting scenario, too. N-qubit maximally entangled basis states are defined as follows [26]:

$$|\psi_j^{\pm}\rangle = \frac{1}{\sqrt{2}}\left(|j\rangle\,|0\rangle \pm \left|2^{N-1} - j - 1\right\rangle|1\rangle\right) \quad (8)$$

where $j = j_1j_2\cdots j_{N-1}$ denotes binary notations. Then there are 2^N different control keys, 2^N operations corresponding to $E_0, E_1, \cdots E_{2^{N-1}}$, and we need N quantum channels with $\frac{2^N}{2} + 1 = 2^{N-1} + 1$ switches each. The eavesdropper Eve only guesses the right N-GHZ-basis states with probability $\frac{1}{2^N}$, as the density operation is $\rho_{AB\cdots N} = \frac{1}{2^N} I_{2^N\times 2^N}$.

3 GCORE using N-qutrit maximally entangled basis states

One of the motivations of considering a high dimensional systems for QKD is to increase the amount of information carried per particle. Another context where using a higher dimension space might be advantageous is in key growing. However, the practical limitations might be more severe in realistic high-dimension cryptosystems, in particular the influence of the detector's quantum efficiency and dark count rate [27,28]. This has been discussed in the related reference [29]. We therefor will now consider the case of a qutrit quantum system.

3.1 GCORE protocol using 2-qutrit general Bell-basis states

Let us now consider the simplest scenario, two particles, each particle having three levels, i.e. a 2-qutrit system. On the whole, the four concrete processes are similar to the analysis in Section 2.2. A recapitulation is presented in the following section. As is known, the general Bell-basis states can be written as [30]:

$$|\psi_{nm}\rangle = \sum_j e^{2\pi ij/3}\,|j\rangle \otimes |j + m \bmod 3\rangle\,/\sqrt{3} \quad (9)$$

where $n, m, j = 0, 1, 2$, their explicit expressions are therefore

$$
\begin{aligned}
|\psi_{00}\rangle &= (|00\rangle + |11\rangle + |22\rangle)/\sqrt{3}\\
|\psi_{10}\rangle &= \left(|00\rangle + e^{2i\pi/3}|11\rangle + e^{4i\pi/3}|22\rangle\right)/\sqrt{3}\\
|\psi_{20}\rangle &= \left(|00\rangle + e^{4i\pi/3}|11\rangle + e^{2i\pi/3}|22\rangle\right)/\sqrt{3}\\
|\psi_{01}\rangle &= (|01\rangle + |12\rangle + |20\rangle)/\sqrt{3}\\
|\psi_{11}\rangle &= \left(|01\rangle + e^{2i\pi/3}|12\rangle + e^{4i\pi/3}|20\rangle\right)/\sqrt{3}\\
|\psi_{21}\rangle &= \left(|01\rangle + e^{4i\pi/3}|12\rangle + e^{2i\pi/3}|20\rangle\right)/\sqrt{3}\\
|\psi_{02}\rangle &= (|02\rangle + |10\rangle + |21\rangle)/\sqrt{3}\\
|\psi_{12}\rangle &= \left(|02\rangle + e^{2i\pi/3}|10\rangle + e^{4i\pi/3}|21\rangle\right)/\sqrt{3}\\
|\psi_{22}\rangle &= \left(|02\rangle + e^{4i\pi/3}|10\rangle + e^{2i\pi/3}|21\rangle\right)/\sqrt{3}. \qquad (10)
\end{aligned}
$$

It is clear that these states are orthogonal. They can be represented by 00, 01, 02, 10, 11, 12, 20, 21, 22, respectively. It can be shown that single-body operators U_{ij} $(i, j = 0, 1, 2)$ will transform $|\psi_{00}\rangle$ into the corresponding other eight states. The expressions for these operators are:

$$
U_{00} = \begin{pmatrix} 1&0&0\\ 0&1&0\\ 0&0&1 \end{pmatrix}; \quad U_{10} = \begin{pmatrix} 1&0&0\\ 0&e^{2\pi i/3}&0\\ 0&0&e^{4\pi i/3} \end{pmatrix};
$$

$$
U_{20} = \begin{pmatrix} 1&0&0\\ 0&e^{4\pi i/3}&0\\ 0&0&e^{2\pi i/3} \end{pmatrix}
$$

$$
U_{01} = \begin{pmatrix} 0&0&1\\ 1&0&0\\ 0&1&0 \end{pmatrix}; \quad U_{11} = \begin{pmatrix} 0&0&e^{4\pi i/3}\\ 1&0&0\\ 0&e^{2\pi i/3}&0 \end{pmatrix};
$$

$$
U_{21} = \begin{pmatrix} 0&0&e^{2\pi i/3}\\ 1&0&0\\ 0&e^{4\pi i/3}&0 \end{pmatrix}
$$

$$
U_{02} = \begin{pmatrix} 0&1&0\\ 0&0&1\\ 1&0&0 \end{pmatrix}; \quad U_{12} = \begin{pmatrix} 0&e^{2\pi i/3}&0\\ 0&0&e^{4\pi i/3}\\ 1&0&0 \end{pmatrix};
$$

$$
U_{22} = \begin{pmatrix} 0&e^{4\pi i/3}&0\\ 0&0&e^{2\pi i/3}\\ 1&0&0 \end{pmatrix}. \qquad (11)
$$

The GCORE operations using qutrit states are similar to the qubit cases presented in Section 2. However, there are nine choices of GCORE operations, and the corresponding relations are the following

$$
\begin{array}{lll}
E_0 \leftrightarrow 00, & E_1 \leftrightarrow 01, & E_2 \leftrightarrow 02\\
E_3 \leftrightarrow 10, & E_4 \leftrightarrow 11, & E_5 \leftrightarrow 12\\
E_6 \leftrightarrow 20, & E_7 \leftrightarrow 21, & E_8 \leftrightarrow 22
\end{array}
$$

and the GCORE is done for every nine general Bell-basis states. These operations are denoted by the notation of their permutation group

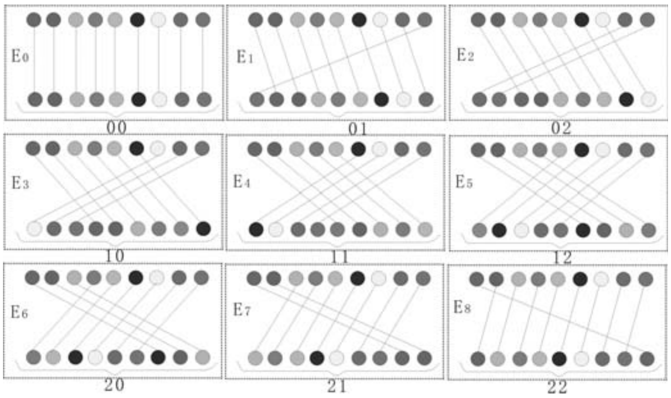

Fig. 3. Example of GCORE using 2-qutrit Bell-basis states; there are nine different GCORE operations.

$$
\begin{aligned}
E_0 &= \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8\,9\\ 1\,2\,3\,4\,5\,6\,7\,8\,9 \end{pmatrix}\\
&= (1\,1)(2\,2)(3\,3)(4\,4)(5\,5)(6\,6)(7\,7)(8\,8)(9\,9)
\end{aligned}
$$

$$
\begin{aligned}
E_1 &= \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8\,9\\ 2\,3\,4\,5\,6\,7\,8\,9\,2 \end{pmatrix}\\
&= (1\,2)(2\,3)(3\,4)(4\,5)(5\,6)(6\,7)(7\,8)(8\,9)(9\,1)
\end{aligned}
$$

$$
\begin{aligned}
E_2 &= \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8\,9\\ 3\,4\,5\,6\,7\,8\,9\,1\,2 \end{pmatrix}\\
&= (1\,3)(2\,4)(3\,5)(4\,6)(5\,7)(6\,8)(7\,9)(8\,1)(9\,2)
\end{aligned}
$$

$$
\begin{aligned}
E_3 &= \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8\,9\\ 4\,5\,6\,7\,8\,9\,1\,2\,3 \end{pmatrix}\\
&= (1\,4)(2\,5)(3\,6)(4\,7)(5\,8)(6\,9)(7\,1)(8\,2)(9\,3)
\end{aligned}
$$

$$
\begin{aligned}
E_4 &= \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8\,9\\ 5\,6\,7\,8\,9\,1\,2\,3\,4 \end{pmatrix}\\
&= (1\,5)(2\,6)(3\,7)(4\,8)(5\,9)(6\,1)(7\,2)(8\,3)(9\,4)
\end{aligned}
$$

$$
\begin{aligned}
E_5 &= \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8\,9\\ 6\,7\,8\,9\,1\,2\,3\,4\,5 \end{pmatrix}\\
&= (1\,6)(2\,7)(3\,8)(4\,9)(5\,1)(6\,2)(7\,3)(8\,4)(9\,5)
\end{aligned}
$$

$$
\begin{aligned}
E_6 &= \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8\,9\\ 7\,8\,9\,1\,2\,3\,4\,5\,6 \end{pmatrix}\\
&= (1\,7)(2\,8)(3\,9)(4\,1)(5\,2)(6\,3)(7\,4)(8\,5)(9\,6)
\end{aligned}
$$

$$
\begin{aligned}
E_7 &= \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8\,9\\ 8\,9\,1\,2\,3\,4\,5\,6\,7 \end{pmatrix}\\
&= (1\,8)(2\,9)(3\,1)(4\,2)(5\,3)(6\,4)(7\,5)(8\,6)(9\,7)
\end{aligned}
$$

$$
\begin{aligned}
E_8 &= \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8\,9\\ 9\,1\,2\,3\,4\,5\,6\,7\,8 \end{pmatrix}\\
&= (1\,9)(2\,1)(3\,2)(4\,3)(5\,4)(6\,5)(7\,6)(8\,7)(9\,8)
\end{aligned}
$$

the permutation has been shown clearly in Figure 3. Figure 4 shows a specific example of the main device necessary to perform GCORE operation.

According to Figure 4, the upper QIC parts are transmitted according to their temporal order. A control key is used to rearrange the order of the lower QIC parts. For

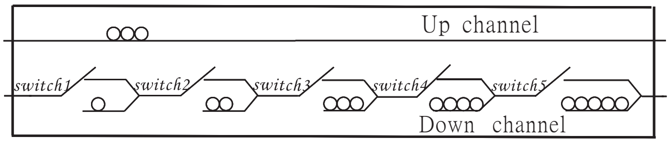

Fig. 4. Devices to perform GCORE operations, the loop represents a time delay of a fixed interval.

instance, if the value of the control key is 00, the operation E_0 is applied. In Figure 4 there are five switches, and the order of the nine general Bell-basis states are unchanged with switches 1, 2, 3, 4 and 5 in position (up, up, down, up, up). When the control key is 01, E_1 is performed, and this is done by putting the nine switches into positions (down, down, up, up, down), (up, down, up, up, up), (up, down, up, up, up), (up, down, up, up, up), (up, down, up, up, up), (up, down, up, up, up), (up, down, up, up, up), (up, down, up, up, up), (up, down, up, up, up) for the nine particles, respectively. Similar combinations can be written explicitly for $E_2, E_3, E_4, E_5, E_6, E_7, E_8$.

Now we can consider the cases of multi-particle and/or high-dimension quantum systems. Firstly the method is generalized to high dimension quantum systems ($d > 3$) of two particles. Note that the d-dimension Bell-basis states in a symmetric channel [9,27,29] are expressed as

$$|\psi_{nm}\rangle = \sum_j e^{2\pi ijn/d} |j\rangle \otimes |j + m \bmod d\rangle / \sqrt{d} \quad (12)$$

where $n, m, j = 0, 1, \cdots d-1$. The unitary operator is

$$U_{nm} = \sum_j e^{2\pi ijn/d} |j + m \bmod d\rangle \langle j| \quad (13)$$

which can transfer d-dimension state

$$|\psi_{00}\rangle = \sum_j |j\rangle \otimes |j\rangle / \sqrt{d} \quad (14)$$

to another d-dimension Bell-basis state $|\psi_{nm}\rangle$, i.e. $U_{nm} |\psi_{00}\rangle = |\psi_{nm}\rangle$. So we can use the same method as in 2-qutrit GCORE to analyze this problem completely.

We have just presented the GCORE for two-particle, high dimensional generalization, and next we will consider the multi-particle situation. Here, we consider a less complicated three particle quantum system, a 3-qutrit quantum system. Its generalized maximally entangled basis states are:

$$\left|\psi_{nm}^k\right\rangle = \sum_j e^{2\pi ijk/3} \times |j\rangle \otimes |j + n \bmod 3\rangle \otimes |j + m \bmod 3\rangle / \sqrt{3} \quad (15)$$

where $n, m, k = 0, 1, 2$, the explicit expressions are then

$$\begin{aligned}
|\psi_{00}^0\rangle &= (|000\rangle + |111\rangle + |222\rangle)/\sqrt{3} \\
|\psi_{01}^0\rangle &= (|001\rangle + |112\rangle + |220\rangle)/\sqrt{3} \\
|\psi_{02}^0\rangle &= (|002\rangle + |110\rangle + |221\rangle)/\sqrt{3} \\
&\cdots \\
|\psi_{22}^2\rangle &= (|022\rangle + e^{4i\pi/3}|100\rangle + e^{2i\pi/3}|222\rangle)/\sqrt{3}. \quad (16)
\end{aligned}$$

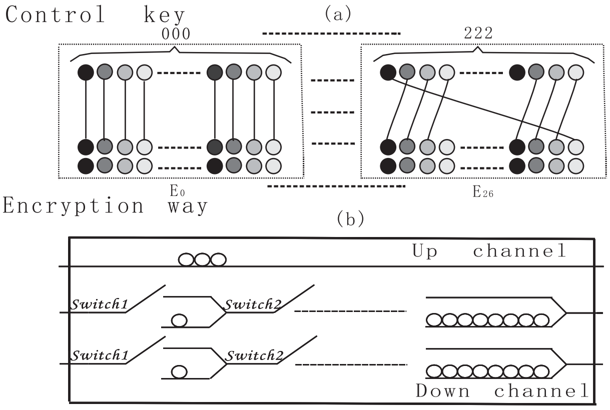

Fig. 5. (a) Example of GCORE using 3-qutrit maximally entangled basis states; (b) devices to perform GCORE operations, the loop represents a time delay of a fixed interval.

There are 27 corresponding GCORE operations, denoted by:

$$\begin{aligned}
&E_0 \leftrightarrow 000, \quad E_1 \leftrightarrow 001, \quad E_2 \leftrightarrow 002, \quad E_3 \leftrightarrow 100, \\
&E_4 \leftrightarrow 101, \quad E_5 \leftrightarrow 102, \quad E_6 \leftrightarrow 200, \quad E_7 \leftrightarrow 201, \\
&E_8 \leftrightarrow 202, \quad E_9 \leftrightarrow 010, \quad E_{11} \leftrightarrow 011, \quad E_{11} \leftrightarrow 012, \\
&E_{12} \leftrightarrow 110, \quad E_{13} \leftrightarrow 111, \quad E_{14} \leftrightarrow 112, \quad E_{15} \leftrightarrow 210, \\
&E_{16} \leftrightarrow 211, \quad E_{17} \leftrightarrow 212, \quad E_{18} \leftrightarrow 020, \quad E_{19} \leftrightarrow 021, \\
&E_{20} \leftrightarrow 022, \quad E_{21} \leftrightarrow 120, \quad E_{22} \leftrightarrow 121, \quad E_{23} \leftrightarrow 122, \\
&E_{24} \leftrightarrow 220, \quad E_{25} \leftrightarrow 221, \quad E_{26} \leftrightarrow 222. \quad (17)
\end{aligned}$$

With an increase of dimension of GCORE operations, more resources are needed, and the security analysis also becomes more complicated. However, its maximal advantage is tremendous increase in the swell of security. And the probability that Eve guesses the right control key is near 0. The corresponding figure is given in Figure 5.

Generally, a uniform expression of N-qutrit maximally entangled basis states can be expressed in the following form

$$|\psi_{i_1,i_2,\cdots,i_{N-1}}^N\rangle = \sum_j e^{2\pi ijN/3}|j\rangle \otimes |j + i_1 \bmod 3\rangle \otimes |j + i_2 \bmod 3\rangle \otimes \cdots \otimes |j + i_{N-1} \bmod 3\rangle\sqrt{3} \quad (18)$$

where $i_1, i_2 \cdots i_N = 0, 1, 2$. Similar analysis can be given, but there is a little difference. In short, there are 3^N different control keys, 3^N operations corresponding to $E_0, E_1, \cdots E_{3^N-1}$, and we need N quantum channels with $3^{N-1}+1$ switches each. The eavesdropper can only guesses the right general Bell-basis state with probability $\frac{1}{3^N}$, as the density operation is $\rho_{AB\cdots N} = \frac{1}{3^N} I_{3^N \times 3^N}$.

3.2 Security of GCORE using 2-qutrit general Bell-basis states

Now, let us look at the security of the above GCORE protocol using 2-qutrit states. Eve has only an 11.1% chance to guess the right GCORE operation for nine general Bell-basis states. If she uses the wrong GCORE operation, the two particles she measured will be anticorrelated. Assume that particle A from the general Bell-basis state and particle B from the second general Bell-basis state are mistreated by Eve as a general Bell-basis state, then the density operator will be

$$\rho_{A_1B_2} = \bar{\rho}_{A_1} \otimes \bar{\rho}_{B_2} = \begin{pmatrix} \frac{1}{3} & 0 & 0 \\ 0 & \frac{1}{3} & 0 \\ 0 & 0 & \frac{1}{3} \end{pmatrix} \otimes \begin{pmatrix} \frac{1}{3} & 0 & 0 \\ 0 & \frac{1}{3} & 0 \\ 0 & 0 & \frac{1}{3} \end{pmatrix} = \frac{1}{9} I_{9\times 9} \tag{19}$$

where $\bar{\rho}_{A_1} = \mathrm{Tr}_{B_1}\left(\rho_{A_1B_1}\right)$, $\bar{\rho}_{B_2} = \mathrm{Tr}_{A_2}\left(\rho_{A_2B_2}\right)$. The result indicates that any one of the nine general Bell-basis states appears with a probability of 11.1%. Thus, Eve will introduce an error rate of 79.01% in the result. Alice and Bob can detect Eve easily by checking a sufficiently large subset of randomly chosen results. Surely, Eve can take a generalized Bell inequality measurement on the particles, but it will be ineffective in decrypting the control key.

There are eight (Hermitian) generators of $SU\left(3\right)$, i.e. eight Gell-Mann matrices, which are defined by

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -i & 0 \\ i & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 0 & -i \\ 0 & 0 & 0 \\ i & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & -i \\ 0 & i & 0 \end{pmatrix}, \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -2 \end{pmatrix}.$$

Let us choose directions $\boldsymbol{M}$ and $\boldsymbol{N}$ as the measurement of directions of Alice and Bob where measurements satisfy the orthogonality. The correlation operator can then be written as:

$$\hat{E} = \hat{S} \cdot \boldsymbol{M} \otimes \hat{S} \cdot \boldsymbol{N} \cdot \tag{20}$$

The expectation values $\langle E\left(\boldsymbol{M},\boldsymbol{N}\right)\rangle_{\psi} = \langle\psi|\, \hat{S} \cdot \boldsymbol{M} \otimes \hat{S} \cdot \boldsymbol{N}\, |\psi\rangle$ are not equal for different general Bell-basis states

$$\langle E\left(\boldsymbol{M},\boldsymbol{N}\right)\rangle_{\psi_{00}} = \frac{2}{3}\begin{pmatrix} M_1N_1 - M_2N_2 + M_3N_3 + M_4N_4 - M_5N_5 \\ +M_6N_6 - M_7N_7 + M_8N_8 \end{pmatrix}$$

$$\langle E\left(\boldsymbol{M},\boldsymbol{N}\right)\rangle_{\psi_{01}} = \frac{1}{3}\begin{pmatrix} 2M_4N_1 + 2M_5N_2 - M_3N_3 - \sqrt{3}M_8N_3 + 2M_6N_4 \\ +2M_7N_5 + 2M_1N_6 - 2M_2N_7 + \sqrt{3}M_3N_8 - M_8N_8 \end{pmatrix}$$

$$\langle E\left(\boldsymbol{M},\boldsymbol{N}\right)\rangle_{\psi_{02}} = \frac{1}{3}\begin{pmatrix} 2M_6N_1 - 2M_7N_2 - M_3N_3 + \sqrt{3}M_8N_3 + 2M_1N_4 \\ +2M_2N_5 + 2M_4N_6 + 2M_5N_7 - \sqrt{3}M_3N_8 - M_8N_8 \end{pmatrix}$$

$$\begin{aligned}\langle E\left(\boldsymbol{M},\boldsymbol{N}\right)\rangle_{\psi_{10}} = {}& \\ & \frac{-1+i\sqrt{3}}{3}M_1N_1 - \frac{-1+i\sqrt{3}}{3}M_2N_2 + \frac{1-i\sqrt{3}}{6}M_3N_3 \\ & + \frac{\sqrt{3}+i}{6}M_8N_3 - \frac{1+i\sqrt{3}}{3}M_4N_4 + \frac{1+i\sqrt{3}}{3}M_5N_5 \\ & + \frac{2}{3}M_6N_6 - \frac{2}{3}M_7N_7 + \frac{\sqrt{3}+i}{6}M_3N_8 - \frac{1-i\sqrt{3}}{6}M_8N_8\end{aligned}$$

$$\begin{aligned}\langle E\left(\boldsymbol{M},\boldsymbol{N}\right)\rangle_{\psi_{11}} = {}& -\frac{1+i\sqrt{3}}{3}M_4N_1 - \frac{1+i\sqrt{3}}{3}M_5N_2 \\ & -\frac{1}{3}M_3N_3 - \frac{i}{3}M_8N_3 + \frac{2}{3}M_6N_4 + \frac{2}{3}M_7N_5 + \frac{-1+i\sqrt{3}}{3}M_1N_6 \\ & + \frac{1-i\sqrt{3}}{3}M_2N_7 - \frac{i}{3}M_3N_8 + \frac{1}{3}M_8N_8\end{aligned}$$

$$\begin{aligned}\langle E\left(\boldsymbol{M},\boldsymbol{N}\right)\rangle_{\psi_{12}} = {}& \frac{2}{3}M_6N_1 - \frac{2}{3}M_7N_2 + \frac{1+i\sqrt{3}}{6}M_3N_3 \\ & - \frac{\sqrt{3}-i}{6}M_8N_3\,d - \frac{1-i\sqrt{3}}{3}M_1N_4 - \frac{1-i\sqrt{3}}{3}M_2N_5 \\ & - \frac{1+i\sqrt{3}}{3}M_4N_6 - \frac{1+i\sqrt{3}}{3}M_5N_7 \\ & - \frac{\sqrt{3}-i}{6}M_3N_8 - \frac{1+i\sqrt{3}}{6}M_8N_8\end{aligned}$$

$$\begin{aligned}\langle E\left(\boldsymbol{M},\boldsymbol{N}\right)\rangle_{\psi_{20}} = {}& -\frac{1+i\sqrt{3}}{3}M_1N_1 + \frac{1+i\sqrt{3}}{3}M_2N_2 \\ & + \frac{1+i\sqrt{3}}{6}M_3N_3 + \frac{\sqrt{3}-i}{6}M_8N_3 - \frac{1-i\sqrt{3}}{3}M_4N_4 \\ & + \frac{1-i\sqrt{3}}{3}M_5N_5 + \frac{2}{3}M_6N_6 - \frac{2}{3}M_7N_7 \\ & + \frac{\sqrt{3}-i}{6}M_3N_8 - \frac{1+i\sqrt{3}}{6}M_8N_8\end{aligned}$$

$$\begin{aligned}\langle E\left(\boldsymbol{M},\boldsymbol{N}\right)\rangle_{\psi_{21}} = {}& \frac{-1+i\sqrt{3}}{3}M_4N_1 + \frac{-1+i\sqrt{3}}{3}M_5N_2 \\ & -\frac{1}{3}M_3N_3 + \frac{i}{3}M_8N_3 + \frac{2}{3}M_6N_4 + \frac{2}{3}M_7N_5 - \frac{1+i\sqrt{3}}{3}M_1N_6 \\ & + \frac{1+i\sqrt{3}}{3}M_2N_7 + \frac{i}{3}M_3N_8 + \frac{1}{3}M_8N_8\end{aligned}$$

$$\begin{aligned}\langle E\left(\boldsymbol{M},\boldsymbol{N}\right)\rangle_{\psi_{22}} = {}& \frac{2}{3}M_6N_1 - \frac{2}{3}M_7N_2 + \frac{1-i\sqrt{3}}{6}M_3N_3 \\ & - \frac{\sqrt{3}+i}{6}M_8N_3 - \frac{1+i\sqrt{3}}{3}M_1N_4 - \frac{1+i\sqrt{3}}{3}M_2N_5 \\ & - \frac{1-i\sqrt{3}}{3}M_4N_6 - \frac{1-i\sqrt{3}}{3}M_5N_7 \\ & - \frac{\sqrt{3}+i}{6}M_3N_8 - \frac{1-i\sqrt{3}}{6}M_8N_8\end{aligned} \tag{21}$$

For product states $|00\rangle$, $|01\rangle$, $|02\rangle$, $|10\rangle$, $|11\rangle$, $|12\rangle$, $|20\rangle$, $|21\rangle$, $|22\rangle$, the expectation values are

$$\begin{gathered}\left(M_3+\frac{M_8}{\sqrt{3}}\right)\left(N_3+\frac{N_8}{\sqrt{3}}\right),\ \left(M_3+\frac{M_8}{\sqrt{3}}\right)\left(-N_3+\frac{N_8}{\sqrt{3}}\right),\\ -\left(M_3+\frac{M_8}{\sqrt{3}}\right)\frac{N_8}{\sqrt{3}},\left(-M_3+\frac{M_8}{\sqrt{3}}\right)\left(N_3+\frac{N_8}{\sqrt{3}},\right),\\ \left(\frac{M_8}{\sqrt{3}}-M_3\right)\left(\frac{N_8}{\sqrt{3}}-N_3\right),-\frac{2}{\sqrt{3}}\left(-M_3+\frac{M_8}{\sqrt{3}}\right)N_8,\\ -\frac{2}{\sqrt{3}}\left(N_3+\frac{N_8}{\sqrt{3}}\right)N_8,-\frac{2}{\sqrt{3}}\left(-N_3+\frac{N_8}{\sqrt{3}}\right)M_8,\frac{4}{3}M_8N_8\end{gathered}$$

respectively. A similar analysis like CORE using EPR pairs is straitforward.

The experimental realization of qutrit used in quantum cryptography is important. Much progress has recently been realized in achieving the production of general Bell-basis state [31]. For example, in order to produce the state

$$|\psi_{00}\rangle=(|00\rangle+|11\rangle+|22\rangle)/\sqrt{3} \tag{22}$$

one uses an unbiased six-port beam splitter [31] which is a device with the following property: if a photon enters any single input port (of the three ports), there is an equal probability that it will leave from each of the three output ports,thus producing the desired state. In fact, one can always construct a configuration of a six-port beam splitter with the distinguishing trait that the elements of its unitary transition matrix, T, are solely powers of the complex number, $\alpha=\exp(i\frac{2\pi}{3})$, namely, $T_{kl}=\frac{1}{\sqrt{3}}\alpha^{(k-1)(l-1)}$. It has been shown in reference [28] that any six-port beam splitter can be constructed from the above-mentioned one by adding appropriate phase shifters at its exit and input ports (and by a trivial relabeling of the output ports). The phase shifters in front of the input ports of beam splitter can be tunable and used to change the phase of the incoming photon.

3.3 Security analysis of qutrit GCORE using the quantum cloning machine

At this point, we will analyze the security of qutrit GCORE against individual attacks (where Eve monitors the qutrit separately). To date, much importan work has been done on the analysis of security for BB84 or generalized BB84 protocols using cloning machines [24,25,32]. Fortunately, GCORE protocols are also a propitious example for analysis using these methods. For this case, we consider a fairly general class of eavesdropping attack based on — not necessarily universal — quantum cloning machine. An appropriate measurement of the clone (and the ancilla system) after disclosure of the basis enables Eve to gain the maximal possible information on Alice's key bit.

We use a general class of cloning transformations as is defined in references [24,25], and the resulting joint state of the two clones (noted A and B) and of the cloning machine (noted C) is

$$\begin{aligned}|\psi\rangle\rightarrow&\sum_{m,n=0}^{N-1}a_{m,n}U_{m,n}\,|\psi\rangle_A\,|B_{m,-n}\rangle_{B,C}\\ =&\sum_{m,n=0}^{N-1}b_{m,n}U_{m,n}\,|\psi\rangle_B\,|B_{m,-n}\rangle_{A,C}\end{aligned} \tag{23}$$

where

$$U_{m,n}=\sum_{k=0}^{N-1}e^{2\pi i(kn/N)}\,|k+m\rangle\,\langle k| \tag{24}$$

$U_{m,n}$ forms a group of qudit error operators, generalizing the Pauli matrices for qubit: m labels the shift errors (extending the bit flip σ_x), while n labels the phase errors (extending the phase flip σ_z). And

$$|B_{m,n}\rangle=N^{-\frac{1}{2}}\sum_{k=0}^{N-1}e^{2\pi i(kn/N)}\,|k\rangle\,|k+m\rangle \tag{25}$$

with $0\leq m,n\leq N-1$. Equation $|B_{m,n}\rangle$ defines the N^2 generalized Bell states for a pair of N-dimensional systems. The final states of clones A and B are

$$\begin{aligned}\rho_A&=\sum_{m,n=0}^{N-1}p_{m,n}\,|\psi_{m,n}\rangle\,\langle\psi_{m,n}|\\ &=\sum_{m,n=0}^{N-1}p_{m,n}U_{m,n}\,|\psi\rangle\,\langle\psi|\,U^{\dagger}_{m,n}\\ \rho_B&=\sum_{m,n=0}^{N-1}q_{m,n}\,|\psi_{m,n}\rangle\,\langle\psi_{m,n}|\\ &=\sum_{m,n=0}^{N-1}q_{m,n}U_{m,n}\,|\psi\rangle\,\langle\psi|\,U^{\dagger}_{m,n}\ \cdot\end{aligned} \tag{26}$$

In addition, the weight functions of the two clones are related by the Fourier transform

$$p_{m,n}=|a_{m,n}|^2,\quad q_{m,n}=|b_{m,n}|^2 \tag{27}$$

where $a_{m,n}$, $b_{m,n}$ are two (complex) amplitude functions that are dual under a Fourier transformation:

$$b_{m,n}=\frac{1}{N}\sum_{x,y=0}^{N-1}e^{2\pi i(nx-my)/N}a_{m,n}. \tag{28}$$

We first assume that Eve clones the qutrit state that is sent to Bob. Eve will then measure her clone in the same basis as Bob and her ancilla in the conjugate basis. To derive Eve's information, we need first to rewrite the cloning transformation of these bases. If Alice sends any state $|k\rangle$ in the computational basis, the phase errors clearly do not play any role in the mixture ρ_B, so the fidelity can be expressed as:

$$F=\langle k|\,\rho_B\,|k\rangle=\sum_{n=0}^{N-1}|a_{0,n}|^2. \tag{29}$$

In the rest of this subsection, we will use this general characterization of cloning in order to investigate the state-dependent cloning of qutrits, Alice sends the input state $|\psi\rangle$ which belongs to a 3-dimensional space. For the cloner to copy equally well the states of the computational bases, we choose the amplitude $a_{m,n}$ characterizing the cloner, which must be of the form

$$(a_{m,n}) = \begin{pmatrix} v & x & x \\ y & y & y \\ z & z & z \end{pmatrix}. \tag{30}$$

Such a cloner is phase covariant, which means it acts identically on each state of the computational base.

The fidelity of the first clone (the one that is sent to Bob) when copying a state $|\psi\rangle$ can be written, in general, as

$$\begin{aligned} F_A = \langle\psi|\,\rho_A\,|\psi\rangle &= \sum_{m,n=0}^{N-1} |a_{m,n}|^2\,|\langle\psi|\;\psi_{m,n}\rangle|^2 \\ &= \sum_{m,n=0}^{N-1} |\langle\psi|\,U_{m,n}\,|\psi_{m,n}\rangle|^2. \end{aligned} \tag{31}$$

That is $F_A = v^2 + y^2 + z^2$. The disturbances $D_{A_1}$and $D_{A_2}$of the first clone are:

$$D_{A_1} = D_{A_2} = x^2 + y^2 + z^2. \tag{32}$$

Through use of the

$$b_{m,n} = \frac{1}{N}\sum_{x,y=0}^{N-1} e^{2\pi i(nx-my)/N} a_{m,n} \tag{33}$$

we can obtain that the second clone is maximal when $y = z$, and the fidelity is given by

$$F_B = \left(v^2 + 2x^2 + 12y^2 + 8xy + 4vy\right)/3. \tag{34}$$

Again, we get the same disturbances (minimal when $y = z$) given by

$$D_{B_1} = D_{B_2} = \left(v^2 + 2x^2 + 3y^2 - 4xy - 2vy\right)/3. \tag{35}$$

For simplicity, one can consider the following amplitude matrix [25]

$$(a_{m,n}) = \begin{pmatrix} v & x & x \\ x & x & x \\ x & x & x \end{pmatrix} \tag{36}$$

where v, x are real parameters which satisfy the normalization condition $v^2 + 8x^2 = 1$. It's easily verified that this cloner's results achieve the same fidelity and same disturbance for any qutrit state:

$$F = v^2 + 2x^2, \qquad D_1 = D_2 = 3x^2. \tag{37}$$

Of course we have the relation: $F + D_1 + D_2 = 1$. It can therefore be stated that the symmetric universal qutrit cloner is characterized by a fidelity of 3/4.

Now, it is simple to analyze its security against an incoherent attack. Bob's fidelity is $F = v^2 + 2x^2$ and the corresponding mutual information between Alice and Bob (if the latter measures his clone in the correct basis) [24] is given by

$$I_{AB} = \log_2 3 + F\log_2 F + (1-F)\log_2\frac{1-F}{2} \tag{38}$$

since two possible errors are equiprobable. The cloning fidelity for Eve is given by

$$F_E = \frac{(v+8x)^2 + 2\,(v-x)^2}{9}\cdot \tag{39}$$

Maximizing Eve's fidelity using the normalization relation $v^2 + 8x^2 = 1$ yields the optimal cloner

$$x = \sqrt{\frac{F\,(1-F)}{2}}, \qquad v = F. \tag{40}$$

The corresponding optimal fidelity for Eve is

$$F_E = \frac{F}{3} + \frac{2}{3}\,(1-F) + \frac{2}{3}\sqrt{2F\,(1-F)}. \tag{41}$$

Let us now see how Eve can maximize her information on Alice's state. If Alice sends the state $|k\rangle\,(k = 0, 1, 2)$, then it is clear that Eve can obtain Bob's error simply by performing a practical Bell measurement (measuring only the m index) on BC. In order to infer Alice's state, Eve must distinguish between three states ($|0\rangle$, $|1\rangle$, $|2\rangle$) with the same scalar product $\frac{3F-1}{2}$ for all pairs of states, regardless of the measured value of m. Consequently, Eve's information [24] is

$$I_{AE} = \log_2 3 + F_E\log_2 F_E + (1-F_E)\log_2\frac{1-F_E}{2}\cdot \tag{42}$$

As a result, Bob and Eve's information curves intersect exactly where the fidelities coincide, that is, at $F = F_E = \frac{1}{2}\left(1 + \frac{1}{\sqrt{3}}\right)$.

Using the theorem given by Csiszar and Korner [27], one can obtain a lower bound on the secret key rate. Concretely, it is sufficient to require $I_{AB} > I_{AC}$ in order to establish a secret key with a nonzero rate. If the one-way communication on a classical channel is used, this is actually a necessary condition. Consequently, the GCORE protocols cease to generate secret key bits precisely at the point where Eve attains Bob's information.

We compute the disturbance $D_{qutrit} = 1 - F = \frac{1}{2}\left(1 - \frac{1}{\sqrt{3}}\right)$ (or error rate) at which $I_{AB} = I_{AE}$ (or $F = F_E$), that is, above which Alice and Bob can not distill a secret key any more through by use of a one-way privacy amplification protocol. While the disturbance for the protocol using qubits is $D_{qubit} = \frac{1}{2}\left(1 - \frac{1}{\sqrt{2}}\right)$, we can easily see $D_{qubit} < D_{qutrit}$. Thus we can say that disturbance increases with the dimension, suggesting that mutual information between Alice and Eve qutrit cryptosystem is smaller than that in the qubit cryptosystem under the same conditions. In other words, Eve obtains less information in the qutrit scheme. Our analysis thus confirms a seemingly general property that a qutrit scheme for QKD is more robust against eavesdropping than the corresponding qubit scheme.

4 Analysis and conclusion

For m particles and/or higher dimension quantum systems, we can provide the uniform expression of maximally entangled basis states. Assuming that the number of particles is n, and that the number of dimension is d, the maximally entangled basis states are

$$\left|\psi^n_{i_1,i_2,\cdots i_n}\right\rangle = \sum_j e^{2\pi ijn/d} \left|j\right\rangle \otimes \left|j+i_1 \bmod d\right\rangle \otimes \left|j+i_2 \bmod d\right\rangle \otimes \cdots \left|j+i_n \bmod d\right\rangle / \sqrt{d}. \quad (43)$$

A similar analysis can be done for dimensions other than 2 or 3. If the dimension is not limited to 2, 3. If Eve can measure the states without disturbing the system, then they are eigenstates of the measuring operator, otherwise, she will produce errors most of time. Otherwise, Eve can only guess the control key randomly, she has no means to decipher the control key. In other words, the security of the GCORE operation for multi-particle and/or higher dimension quantum systems is even greater.

Compared to other QKD protocols using orthogonal states, one distinct feature of our scheme is its high efficiency. The information-theoretic efficiency defined in reference [20] is:

$$\eta = \frac{b_s}{q_t + b_t} \quad (44)$$

where b_s is the number of secret bits received by Bob, q_t is the number of qubits used, and b_t is the number of classical bits exchanged between Alice and Bob during the QKD process. The efficiency of any QKD protocol, defined as the number of secret (i.e. allowing eavesdropping detection) bits per transmitted bit plus qubit, satisfies $\eta \leq 1$. The efficiency of the presented protocol becomes 100%, because $b_s = \log_2 d^N$, $q_t = \log_2 d^N$, $b_t = 0$. In this way, one can calculate out that the efficiency of BB84 is 25%, and similarly, the efficiency of the EPR protocol is 50%. To the best of our knowledge, two protocols reach the limit value of $\eta = 1$. One protocol is provided by Cabello (high capacity Cabello protocol, HCCP) [20] and the other is proposed by Long and Liu (high capacity Long Liu protocol HCLLP) [21]. Both protocols exploit the fact that a possible eavesdropper with no simultaneous access to the entire quantum system, cannot recover all the information without being detected, and both employ a larger alphabet, a few-dimensional orthogonal basis of pure states. In addition, some modifications of BB84 and EPR protocols [22,23] also can achieve 100% efficiency according to equation (44), such as the known efficient BB84 protocol provided by Lo, Chau and Ardehali [22]. The GCORE has the same characteristics, so it can also achieve full efficiency from this point of view.

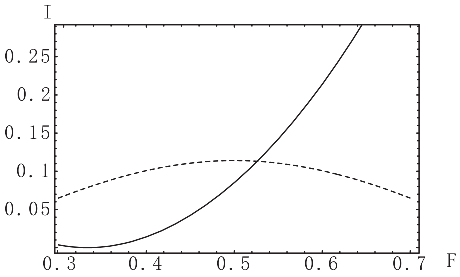

Fig. 6. Relationship between fidelity and mutual information in which solid curve represents the mutual information between Alice and Eve; the dashed curve represents the mutual information between Alice and Bob.

Another feature of the scheme is its high capacity, since the four possible states of the EPR pairs carry two bits of information ($\log_2 4 = 2$), eight possible states of GHZ-basis states carry three bits of information ($\log_2 2^3 = 3$). Similarly, the nine possible states of the 2-qutrit general Bell-basis states carry $\log_2 9$ bits of information, the 27 possible states of the 3-qutrit general maximally entangled basis states carry $\log_2 3^3$ bits of information, and we can state that the possible states of the N-qudit maximally entangled basis state carry $\log_2 d^N$ bits of information. In short, the number of pairs of transmitted qubits in a GCORE carrier unit is $\log_2 d^N$. Whereas in the EPR scheme each adopted EPR pair (particles) encodes one bit of information, only one qubit is transmitted from Alice to Bob for each pair, so the amount of information per carrier particle is one bit. However, if we use the control key to control the GCORE operation of a group of units, we can save greatly reduce resource usage. From a resource usage perspective, therefore, the GCORE protocol is superior.

In QKD, our scheme is just a one-to-one protocol, but/and there are other protocols using different ways to distribute secret keys [1–3,7–21]. As we know, Townsend's protocol [33] is a one-to-any protocol, where Alice acts as a single controller to establish and update a distinct secret key with each network user. An any-to-any protocol has been proposed to allow any two users to establish a secret key over an optical network by Phoenix et al. [34]. The present scheme can be generalized to distribute secret keys to multiple legitimate users. It is different from Townsend and Phoenix's protocol in that the secret keys are common to all legitimate users. We demonstrate the concrete protocol using EPR pairs for simplicity: after Alice has sent the keys to Bob, Bob can create using EPR pairs sequence that carries the raw keys. Then he sends this EPR pair sequence to another legitimate user, Clare, using the same procedure and device as before. The key protocols common to Alice, Bob and Clare are those Bell-basis measurement results that are not chosen to check eavesdropping. In this way, the protocol can be generalized to a multiparty common key distribution protocol.

Note that all of the GCORE protocols have a final step, i.e. error correction and privacy amplification [33]. We shall not discuss these points, which are the same as those in all cryptographic protocols, except that we have to use qutrits (qudits) instead of bits, and therefore parity checks becomes triality checks, that is sums of modulo 3 (d).

In summary, we have extended the concept of CORE to N-qubit, N-qutrit quantum systems. We have proposed the protocols in detail and have given the corresponding security analysis of 3-qubit, 2-qutrit maximally entangled states. Finally, in this paper, we have demonstrated repeatedly the GCORE using a general expression of multi-particle and high dimension maximally entangled basis state by using repeatedly a priori shared control key. The generalized version has great capacity and high efficiency. In addition, the control key can be used to control the GCORE operation of a group of units, which greatly simplifies the experimental realization and enables quantum key distribution in a more efficient way.

We thank Feng Xu, Ren-Gui Zhu, Xiao-Qiang Su, Liang Qiu, De-Hui Zhan, Xue-Chao Li and Zhu-Qiang Zhang for useful discussions. This project was supported by the National Basic Research Programme of China under Grant No. 2001CB309310, the National Natural Science Foundation of China under Grant No. 60573008.

References

1. C.H. Bennett, G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, IEEE,* New York, 1984, pp. 175–179
2. A.K. Ekert, Phys. Rev. Lett. **67**, 661 (1991)
3. C.H. Bennett, G. Brassard, N.D. Mermin, Phys. Rev Lett. **68**, 557 (1992)
4. C.H. Bennett, Phys. Rev. Lett. **8**, 3121 (1992)
5. C.H. Bennett, S.J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992)
6. D. Brub, Phys. Rev. A **65**, 032118 (2002); D. Brub, Phys. Rev. Lett. **81**, 3018 (1998); H. Bechmann-Pasquinucci, N. Gisin, Phys. Rev. A **59**, 4238 (1999)
7. W.Y. Hwang, I.G. Koh, Y.D. Han, Phys. Lett. A **244**, 489 (1998)
8. L. Goldenberg, L. Vaidman, Phys. Rev. Lett. **75**, 1239 (1995); A. Peres, Phys. Rev. Lett. **77**, 3264 (1996); L. Goldenberg, L. Vaidmann, Phys. Rev. Lett. **77**, 3265 (1996)
9. M. Koashi, N. Imoto, Phys. Rev. Lett. **79**, 2383 (1999)
10. F.-G. Deng, G.L. Long, Phys. Rev. A **68** 042315 (2003)
11. H. Bechmann-Pasquinucci, A. Peres, Phys. Rev. Lett. **85**, 3313 (2000)
12. H. Bechmann-Pasquinucci, W. Tittel, Phys. Rev. A **61**, 062308 (2000)
13. Mohamed Bourennane, A. Karlsson, Gunnar Bjork, Phys. Rev. A **64**, 012306 (2001)
14. J.C. Boileau, K. Tamaki, J. Batuwantudawe, R. Laflamme, J.M. Renes, Phys. Rev. Lett. **94**, 040503 (2005)
15. J.M. Renes, Phys. Rev. A **70**, 052314 (2004)
16. J.C. Boileau, K. Tamaki, J. Batuwantudawe, R. Laflamme, J.M. Renes, Phys. Rev. Lett. **94**, 040503 (2005)
17. P. Xue, C.-F. Li, G.-C. Guo, Phy. Rev. A **64**, 032305 (2001)
18. P. Xue, Ch.-F. Li, G.-C. Guo, Phy. Rev. A **65**, 034302 (2002)
19. K. Tamaki, M. Koashi, N. Imoto, Phys. Rev. Lett. **90**, 167904 (2003)
20. A. Cabello, Phys. Rev. Lett. **85**, 5635 (2000)
21. G.L. Long, X.S. Liu, Phys. Rev. A **65**, 032302 (2002)
22. H.-K. Lo, H.F. Chau, M. Ardehali, J. Cryptol. **18**, 133 (2005); e-print `arXiv:quant-ph/0011056`
23. J. Wang, Q. Zhong, C.-J. Tang, e-print `arXiv:quant-ph/0510208`
24. N.J. Cerf, M. Bourennane, A. Karlsson, N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002)
25. N.J. Cerf, T. Durt, N. Gisin J. Mod. Opt. **49**, 1355 (2002); e-print `arXiv:quant-ph/0110092`
26. W. Dur, J.I. Cirac, Phys. Rev. A **61**, 042314 (2000); e-print `arXiv:quant-ph/9911044`
27. I. Csiszar, J. Korner, IEEE Trans. Inf. Theory **24**, 339 (1978)
28. M. Bourennane, A. Karlsson, G. Bjork, N. Gisin, N.J. Cerf, J. Phys. A **35**, 10065 (2002); e-print `quant-ph/0106049`
29. C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, W.K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993)
30. X.S. Liu, G.L. Long, D.M.Tong, F. Li, Phys. Rev. A **65**, 022304 (2002)
31. M. Zukowski, A. Zeilinger, M.A. Horne, Phys. Rev. A **55**, (1997) 2564
32. N.J. Cerf, Phys. Rev. Lett. **84**, (2000) 4497; N.J. Cerf, J. Mod. Opt. **47**, 187 (2000); N.J. Cerf, Acta Phas. Slovaca **48**, 115 (1998)
33. P.D. Townsend, Nature **385**, 47 (1997)
34. S.J.D. Phoenix, S.M. Bnnett, P.D. Twensend, K.J. Blow, J. Mod. Opt. **42**, 1155 (1995)