Vol 15 No 10, October 2006
1009-1963/2006/15(10)/2228-08

Chinese Physics

© 2006 Chin. Phys. Soc.
and IOP Publishing Ltd

High-dimension multiparty quantum secret sharing scheme with Einstein–Podolsky–Rosen pairs*

Chen Pan(陈 攀)[a)b)], Deng Fu-Guo(邓富国)[b)c)d)], and Long Gui-Lu (龙桂鲁)[a)b)e)†]

[a)] *Department of Physics, Tsinghua University, Beijing* 100084, *China*
[b)] *Key Laboratory For Quantum Information and Measurements, Beijing* 100084, *China*
[c)] *The Key Laboratory of Beam Technology and Material Modification of Ministry of Education, and Institute of Low Energy Nuclear Physics, Beijing Normal University, Beijing* 100875, *China*
[d)] *Beijing Radiation Center, Beijing* 100875, *China*
[e)] *Key Laboratory of Atomic and Molecular Sciences, Tsinghua University, Beijing* 100084, *China*

(Received 14 March 2006; revised manuscript received 3 April 2006)

In this paper a high-dimension multiparty quantum secret sharing scheme is proposed by using Einstein–Podolsky–Rosen pairs and local unitary operators. This scheme has the advantage of not only having higher capacity, but also saving storage space. The security analysis is also given.

Keywords: high−dimension, quantum secret sharing, EPR, qubit, qutrit

PACC: 0365

1. Introduction

Security of information has always been an important issue in human life. Nowadays, human life and communication are getting closer and closer, and an increasing amount of information is stored or transmitted through the electronic technology. The security of the information storage and transmission is entirely dependent on the security of the key used in encrypting the information. Thus, the management of the key will become a crucial issue. Suppose that we use different keys to encrypt different files, and all those keys are protected by a master key in a large-scale system in which there are many files. If the master key is just kept by one system supervisor, it may be lost or illegally used by himself. If the master key is kept by many system supervisors, the risk mentioned above can actually be reduced, but the system security will be challenged by more uncertainties. For instance, to keep the safety of precious books in the famous private library, Tian-Yi-Ge, which was built in the Ming dynasty in 1561, the library door has been co-locked by many keys, and it is only when all the key holders are present, that the library can be opened.

In 1979, Blakley[1] and Shamir[2] respectively proposed secret sharing to the above problem. The idea is to divide the master key into n pieces and distribute to n members at different remote places of the legal group. Only with all the n legal members' sharing parts, can one reconstruct the master key. In other words, any member of the group can get the master key only when all the members come to an agreement so that illegal action can be prevented by any one of the other members. Now secret sharing has become one hot spot in the cryptography in the information security field.

The quantum counterpart of the secret sharing scheme is quantum secret sharing (QSS). In 1999, Hillery, Bužek, and Berthiaume[3] brought forward the first QSS scheme, the HBB99 scheme. In this scheme, a three-particle entangled Greenberger–Horne–Zeilinger (GHZ) state is used and the three particles are sent to three participants, say Alice, Bob and Charlie, respectively. Each party chooses randomly two measuring bases (MBs), called x-measuring-basis (x-MB) and y-measuring-basis (y-MB), to measure the particle in his (or her) own hand independently. If one or three of them choose the x-MB, they can get a correlated result which satisfies the basic request of the secret sharing. But if one or three of them choose the y-MB, they will discard

*Project supported by the National Fundamental Research Program (Grant No 001CB309308), China National Natural Science Foundation (Grant Nos 60433050, 10325521, 10447106), the Hang-Tian Science Fund, the SRFDP program of Education Ministry of China and Beijing Education Committee (Grant No XK100270454).

†Corresponding author. E-mail: gllong@mail.tsinghua.edu.cn

the result. After the transmission process, Alice distributes a private key between two agents, Bob and Charlie. If Bob and Charlie cooperate, they can deduce Alice's result and get the entire private key. Otherwise, none of them can get the key. The scheme has been generalized into multi-parties with increased efficiency by some of us.[16]. If each participant is allowed to choose the x-MB or y-MB, then a valid round of transmission is one with even participants who choose the y-MB so that their results are correlated. The secret key distributed among the participants are the parity of the binary numbers of their measured values. By far, there have been a lot of works focused on QSS,[4−21] including those for sharing an unknown quantum state.[22−24]

Recently, a multiparty quantum secret sharing (MQSS) protocol is proposed by Zhang, Li and Man[25] with single photons following some ideas in the Ref.[26]. In their protocol, the single photon is prepared by one of the two agents, Bob, and the other one Charlie performs one of the four local unitary operations $\{I, H, \mathrm{i}\sigma_y, H \otimes \mathrm{i}\sigma_y\}$ on the photons for coding the information or preventing the eavesdropping from an vicious eavesdropper Eve.[27] Here H represents the Hadamard operation. Each of the photons can carry one bit of information and the efficiency for usable qubits approaches the maximal value of 100%. In this paper, we will present a protocol for multiparty quantum secret sharing with Einstein–Podolsky–Rosen (EPR) pairs following some ideas from the Zhang-Li-Man MQSS scheme,[25] and then generalize this protocol to high dimensional Hilbert space. With the local unitary operations, each of the photons can carry $2\log_2 d$ bits of information.

2. Two-dimensional three-party quantum secret sharing scheme with EPR pairs

2.1. The QSS scheme

In a two-dimensional Hilbert space, the four Bell states can be written as follows:

$$|\phi^{\pm}\rangle_{HT} = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)_{HT}, \tag{1}$$

$$|\psi^{\pm}\rangle_{HT} = \frac{1}{\sqrt{2}}(|01\rangle_{\pm}|10\rangle)_{HT}, \tag{2}$$

where $|0\rangle$ and $|1\rangle$ are the two eigenstates of the Pauli operator σ_z and the subscripts HT refer to the home (H) and travelling (T) qubits in the pair. The four local unitary operations U_i, which represent the two-bit classical information 00, 01, 10 and 11, respectively, can transfer each of the four Bell states into another one.

$$U_0 = I = |0\rangle\langle 0| + |1\rangle\langle 1|, \quad U_1 = \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|, \tag{3}$$

$$U_2 = \sigma_x = |1\rangle\langle 0| + |0\rangle\langle 1|, \quad U_3 = i\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|. \tag{4}$$

For simplicity, we first describe our scheme in a two-dimensional quantum system. We use one EPR pair as the quantum information carrier, instead of N pairs as that in Ref.[25]. This three-party MQSS scheme has the following steps:

1) Bob prepares an EPR pair in the Bell state $|\psi^-\rangle_{HT}$. He sends the travelling qubit T to Charlie and keeps the home qubit H for himself.

2) After receiving the T qubit, Charlie can choose between the 'message mode' and 'check mode' with the probabilities p_{bc} and $(1-p_{\mathrm{bc}})$, respectively. When Charlie switches to check mode, he randomly selects one of the two bases, σ_z and σ_x, to measure the received qubit. Then he tells Bob to measure the correlated photon H by choosing the two MBs randomly. They publish their outcomes together with their MB. They compare their results.

Under ideal condition, if Bob is honest and no eavesdropping exists, their results should be completely opposite when they choose the same MB. That is, if Charlie's result is 0 (1), then Bob 's result must be 1 (0). Charlie saves the contrastive result, and continues to carry on the next round transmission.

3) If he chooses the message mode, Charlie randomly performs one of the four local unitary operations U_i $(i = 0, 1, 2, 3)$, say U_{C}, on the photon T. Moreover, he should choose randomly one of the two operations $\{I, H\}$ to encrypt it, the same as in

Ref.[25], before he sends this photon to Alice.

4) After reception of photon T, Alice chooses the two modes, similar to Bob, with the probabilities $p_{\rm ca}$ and $1-p_{\rm ca}$, respectively. When she chooses the message mode, she chooses randomly one of the local unitary operations U_i $(i=0,1,2,3)$, noted as $U_{\rm A}$, to encrypt the photon and then she sends this photon to Charlie. Otherwise she measures the photon with σ_z or σ_x randomly, and then tells Bob to do a single-photon measurement on the photon H, same as Charlie.

5) After receiving the photon T, Charlie decrypts the photon T with the operation I or H same as that encrypted by him, and then requires Bob to send the photon H to him after he operates it with one of the four local unitary operations, say $U_{\rm B}$. Charlie performs a Bell measurement on those two photons and publishes the outcome.

6) After all the above steps repeat N (a number which is beforehand decided by Alice, Bob and Charlie) turns, they stop the transmitting process and make the security analysis.

For the samples chosen by Alice with single-photon measurements on the photons T, she divides it into two parts. One is used for checking the eavesdropping done by Bob. That is, Alice requires Bob to publish his MB and the outcome of the measurement on the photon H first and then Charlie tell Alice his operation chosen on the photon T. For the other one, Charlie should first publish his operation and then Bob tells Alice his MB and his outcome. Just those two eavesdropping checks, Alice can prevent Bob and Charlie from stealing the information about her operations $U_{\rm A}$ independently, same as that in Ref.[27]. With the information of the Bell-basis measurement published by Bob, each of the three parties can get the combined information of the operations done by the other two parties, i.e. $U_{\rm A}=U_{\rm B}\otimes U_{\rm C}$.

In order to determine whether there is an eavesdropper in the line when the photon T returns to Bob from Alice, Bob should sample some of the outcomes to estimate the error rate. Even though Bob and Charlie cannot deduce the operation done by Alice independently, the error rate is useful for doing error correction and privacy amplification in the last process for distilling a private key.

Different from Refs.[25,27], only Bob, not all the parties, needs to store the quantum state, in our scheme. Charlie and Alice can complete their operations at the moment they receive the photon T either they choose the message mode or the check mode. Moreover, each EPR pair can carry two bits of information in this scheme and it can be made to be secure in a noise quantum channel with entanglement purification.[28−30]

2.2. Its security

In fact, the process for eavesdropping check is the same as that in the Bennett–Brassard–Mermin 1992 (BBM92) quantum key distribution (QKD) protocol[31] which was proved to be secure in an ideal condition[32] and in a practical condition.[33]. So this scheme is also secure.

We can evaluate the error rate and the corresponding maximal amount of information obtainable from an eventual eavesdropper in this QSS scheme, same as that in Ref.[34], following the ideas in Refs.[35 – 46]. Now, let us discuss the case that the eavesdropper is Charlie. The other case that the eavesdropper is Bob or Eve is similar to this one with or without a little of modification. In this time, the process for eavesdropping check is same as that in the high-capacity Ping-Pong protocol.[47]

The security is simplified to the fact that Bob and Alice forbid Charlie to eavesdropping the operations done by Alice, say $U_{\rm A}$. For Charlie, the state of the travelling photon T is in either state $|0\rangle$ or $|1\rangle$ with equal probability 50% when the reduced density matrix is $\rho_T = Tr_H(\rho_{TH}) = \frac{1}{2}\begin{pmatrix}1&0\\0&1\end{pmatrix}$. As Bob and Alice check eavesdropping with choosing the two MBs σ_z and σ_x randomly, same as the BBM92 QKD protocol, the best individual attack done by Bob may be same as that in Ref.[46], i.e. Charlie can perform an unitary transformation $\hat{E}$ on the photon T and the ancilla[44] whose state is initially in $|0\rangle$ for stealing some information with small error rate in the results.

$$\hat{E}\,|0\rangle\,|0\rangle = |0\rangle\,|0\rangle \equiv |00\rangle\,, \tag{5}$$

$$\begin{aligned}\hat{E}\,|1\rangle\,|0\rangle &= \cos\theta\,|1\rangle\,|0\rangle + \sin\theta\,|0\rangle\,|1\rangle \\ &\equiv \cos\theta\,|10\rangle + \sin\theta\,|01\rangle\,,\end{aligned} \tag{6}$$

$$d = \frac{1}{2}\sin^2\theta, \tag{7}$$

where $\theta\in[0,\pi/4]$ characterizes the strength of Bob's attack,[46], and d is the probability that Bob's action is detected. This eavesdropping is just a POVM superoperator[35] and it does not violate the no-cloning theorem. As the photon T is in a maximally

mixed state for Charlie, Charlie can only get the information about the bit value of the operation $U_{\rm A}$, not that for the phase with the unitary operation $\hat{E}$. As the symmetry, the information stolen by Charlie is less than the twice of the information about the bit value of the operation $U_{\rm A}$.

After Charlie does the unitary operation $\hat{E}$ and Alice performs the unitary operations $U_{\rm A}$ with the probabilities P_i $(i = 0, 1, 2, 3)$, the final state of the quantum system composed of the photon T and the ancilla e is described by the trace preserving quantum operation[41] ε,

$$\varepsilon(\rho_T) = \sum_{i=0}^{3} P_i \varepsilon_{U_i}(\rho_T), \tag{8}$$

where P_i is the probability that Alice chooses the operation U_i for encoding the message, and ε_{U_i} is quantum operation describing the evolution of the initial state ρ_{TH}, i.e.,

$$\varepsilon_{U_i}(\rho_T) = U_i \hat{E} \rho_T \otimes |e\rangle\langle e| \hat{E}^{+} U_i. \tag{9}$$

The accessible information I which can be extracted from the state $\varepsilon(\rho_T)$ is no more than the Holevo bound,[36,41,48], i.e.

$$I \leq S(\varepsilon(\rho_T)) - \sum_{i=0}^{3} P_i S(\varepsilon_{U_i}(\rho_T)) \equiv I_0, \tag{10}$$

where $S(\rho)$ is the von-Neumann entropy of the state ρ, i.e.

$$S(\rho) = -{\rm Tr}\{\rho \log_2 \rho\} = \sum_{i=0}^{3} -\lambda_i \log_2 \lambda_i, \tag{11}$$

where λ_i are the roots of the characteristic polynomial $\det(\rho - \lambda I)$.[36]

Define an orthonormal base $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ which spans the generic subspace of the Hilbert space $H_{\rm C} \otimes H_{\rm e}$ support of $\varepsilon(\hat{\rho}_T)$. With Eqs.(5)–(11), we can obtain the relation between I_0 and the probability d in the case that Charlie chooses the four local unitary operations with the same probability $P_i = \dfrac{1}{4}$ as follows:

$$\begin{aligned} I_0 &= 1 - \frac{\sin^2\theta}{2} \log_2 \sin^2\theta - \frac{1+\cos^2\theta}{2} \log_2 (1+\cos^2\theta) \\ &= -d \log_2 d - (1-d) \log_2 (1-d). \end{aligned} \tag{12}$$

When $d = 0.25$, the information that Charlie can obtain with the best individual attack $I_{\rm C} \leq 2I_0 = 1.62 < 2$. That is, $I_{\rm C}$ is less than the mutual information between Alice and Bob if the eavesdropping operator $\hat{E}$ is unitary. Bob and Alice can forbid Charlie to steal the quantum communication. With some postprocessing techniques, such as error correction and privacy amplification, this QSS scheme is secure and similar to QKD.[48,49]

3. High-dimensional three-party quantum secret sharing scheme with EPR pairs

The above scheme is realized in two-dimensional Hilbert space. We can generalize this scheme to a d-dimensional ($d \geq 3$) Hilbert space. To be more concise, we want to begin our scheme with the example of $d = 3$.

In three-dimensional Hilbert space, the general Bell basis of two particles can be described as follows:[50–55]

$$|\Psi_{nm}\rangle_{HT} = \sum_j e^{2\pi {\rm i} jn/3} |j\rangle \otimes |j + m \bmod 3\rangle / \sqrt{3}, \tag{13}$$

where $n, m, j = 0, 1, 2$. When $n, m = 0$ and $j = 0, 1, 2$, we have

$$\begin{aligned} |\Psi_{00}\rangle_{HT} &= \sum_j |j\rangle \otimes |j\rangle / \sqrt{3} \\ &= (|00\rangle + |11\rangle + |22\rangle) / \sqrt{3}. \end{aligned} \tag{14}$$

The unitary operators

$$U_{nm} = \sum_j e^{2\pi {\rm i} jn/3} \ |j + m \bmod 3\rangle \otimes \langle j| \tag{15}$$

can transform $|\Psi_{00}\rangle_{HT}$ into the corresponding states $|\Psi_{nm}\rangle_{HT}$ respectively. That is to say,

$$U_{nm} |\Psi_{00}\rangle_{HT} = |\Psi_{nm}\rangle_{HT}. \tag{16}$$

In three-dimensional Hilbert space, there are four conjugate MB.[56] The Z-MB is composed of the following three eigenvectors:

$$|Z_{-1}\rangle = |0\rangle\,, \quad |Z_0\rangle = |1\rangle\,, \quad |Z_{+1}\rangle = |2\rangle\,. \tag{17}$$

The three eigenvectors of the X-MB can also be described as following

$$\begin{aligned} |X_{-1}\rangle &= \frac{1}{\sqrt{3}}\left(|0\rangle + |1\rangle + |2\rangle\right), \\ |X_0\rangle &= \frac{1}{\sqrt{3}}\left(|0\rangle + \mathrm{e}^{2\pi \mathrm{i}/3}\,|1\rangle + \mathrm{e}^{-2\pi \mathrm{i}/3}\,|2\rangle\right), \\ |X_{+1}\rangle &= \frac{1}{\sqrt{3}}\left(|0\rangle + \mathrm{e}^{-2\pi \mathrm{i}/3}\,|1\rangle + \mathrm{e}^{2\pi \mathrm{i}/3}\,|2\rangle\right), \end{aligned} \tag{18}$$

and the operation

$$H_t = \begin{bmatrix} \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} \\ \frac{1}{\sqrt{3}} & \frac{\mathrm{e}^{2\pi \mathrm{i}/3}}{\sqrt{3}} & \frac{\mathrm{e}^{-2\pi \mathrm{i}/3}}{\sqrt{3}} \\ \frac{1}{\sqrt{3}} & \frac{\mathrm{e}^{-2\pi \mathrm{i}/3}}{\sqrt{3}} & \frac{\mathrm{e}^{2\pi \mathrm{i}/3}}{\sqrt{3}} \end{bmatrix} \tag{19}$$

can realize the transformation between the Z-MB and the X-MB.

Now we can realize the three-dimensional three-party QSS scheme with EPR pairs as following:

First, similar to the two-dimensional scheme, Bob prepares an EPR photon pair in Bell states $|\Psi_{00}\rangle_{HT}$, and then he sends the travelling qutrit T to Charlie and keeps the other one H for himself.

After receiving the qutrit T, Charlie randomly chooses the message mode or check mode with probability p_{bc} or $(1-p_{\mathrm{bc}})$ respectively. If Charlie chooses the check mode, then he randomly selects one of the two bases, Z-MB and X-MB, to measure the received qutrit. Then he asks Bob to measure the qutrit H by choosing the two MBs randomly. They publish their outcomes together with their MB and compare their results. Charlie saves the contrastive result, and continues to carry on the next round transmission. If Charlie chooses the message mode, then he randomly chooses one of the above unitary operations U_{nm} $(n, m = 0, 1, 2)$, say U_{C}, to encode this qutrit. After doing this, Charlie randomly chooses one of the two operations $\{I, H_t\}$ to encrypt the qutrit T and sends it to Alice.

When Alice receives this qutrit, she also randomly chooses the message mode or check mode with probability p_{ca} or $(1-p_{\mathrm{ca}})$ respectively. If she chooses the check mode, she randomly chooses one MB from Z-MB and X-MB to measure the qutrit T, and then asks Bob to measure the qutrit H. So, she asks Bob to publish the MB chosen by him to measure the qutrit H and the measurement outcomes, and then asks Charlie to tell her which unitary operation he has performed on the qutrit T; or she firstly asks Charlie to publish the unitary operation performed by him, and then asks Bob to tell her the MB and the outcomes.

After receiving the necessary information, Alice first performs the same unitary operation on the qutrit T as Charlie has done and then measures the qutrit T by using the same MB as that used by Bob. Then, she compares the measurement result with the outcomes which has been told by Bob. In ideal condition, if Bob and Charlie are honest and no eavesdropping exists, their results should be completely the same. Alice saves the contrastive result and continues to carry on the next round transmission.

If Alice chooses the message mode, then she chooses randomly one of the local unitary operations U_{nm} $(n, m = 0, 1, 2)$, noted as U_{A}, to encrypt the qutrit T and then she sends it to Charlie. After receiving this qutrit, Charlie performs the operation I or H_t^+ as she has done on the qutrit T, and then requires Bob to send the qutrit H to her after he operates it with one of the local unitary operations U_{nm} $(n, m = 0, 1, 2)$, say U_{B}. Charlie performs a Bell measurement on those two qutrits and publishes the outcome.

All the above steps will be repeated N turns, and the security analysis is the same as that in the two-dimensional case. Through cooperation, both Bob and Charlie can obtain the information of Alice's operations; otherwise, neither of them can get anything.

In three-dimensional Hilbert space, the number of the above local unitary operations U_{nm} is 9. Then, through only one operation, we can encode $\log_2 9$ bits of information on one qutrit.

From the above scheme, we can also generalize it to a d-dimensional $(d \geq 4)$ scheme. In d-dimensional Hilbert space, the general Bell bases are[50−55]

$$|\Psi_{nm}^d\rangle_{HT} = \sum_j e^{2\pi \mathrm{i} jn/d} |j\rangle \otimes |j + m \bmod d\rangle/\sqrt{d}, \tag{20}$$

where $n, m, j = 0, 1, ..., d-1$. The unitary operations

$$U_{nm}^d = \sum_j e^{2\pi \mathrm{i} jn/d} |j + m \bmod d\rangle \otimes \langle j| \tag{21}$$

can transform $|\Psi_{00}^d\rangle_{HT} = \sum_j |j\rangle \otimes |j\rangle/\sqrt{d}$ into the corresponding states $|\Psi_{nm}^d\rangle_{HT}$. So, if we use an EPR

pair, we can encode $\log_2 d^2$ bits of information on one photon through only one operation.

In d-dimensional Hilbert space, we can also define the Z_d-MB which has d eigenvectors as follows:

$$|0\rangle\,, \quad |1\rangle\,, \quad |2\rangle\,, \cdots, \quad |d-1\rangle\,. \tag{22}$$

So, the d eigenvectors of the X_d-MB can also be described as follows:

$$\begin{aligned}
|0\rangle_x &= \frac{1}{\sqrt{d}}(|0\rangle + |1\rangle + \ \cdots \ + |d-1\rangle),\\
|1\rangle_x &= \frac{1}{\sqrt{\mathrm{d}}}|0\rangle + \mathrm{e}^{\frac{2\pi\mathrm{i}}{d}}\,|1\rangle + \cdots + \mathrm{e}^{\frac{2(d-1)\pi\mathrm{i}}{d}}\,|d-1\rangle),\\
|2\rangle_x &= \frac{1}{\sqrt{\mathrm{d}}}(|0\rangle + \mathrm{e}^{\frac{4\pi\mathrm{i}}{d}}\,|1\rangle + \cdots + \mathrm{e}^{\frac{4(d-1)\pi\mathrm{i}}{d}}\,|d-1\rangle),\\
&\cdots\\
|d-1\rangle_x &= \frac{1}{\sqrt{d}}(|0\rangle + \mathrm{e}^{\frac{2(d-1)\pi\mathrm{i}}{d}}\,|1\rangle + \cdots + \mathrm{e}^{\frac{(d-1)^2\pi\mathrm{i}}{d}}\,|d-1\rangle),
\end{aligned} \tag{23}$$

and the operation

$$H_d = \begin{bmatrix} 1 & 1 & 1 & \cdots \\ 1 & \mathrm{e}^{\frac{2\pi\mathrm{i}}{\mathrm{d}}} & \mathrm{e}^{\frac{4\pi\mathrm{i}}{\mathrm{d}}} & \cdots \\ 1 & \mathrm{e}^{\frac{4\pi\mathrm{i}}{d}} & \mathrm{e}^{\frac{8\pi\mathrm{i}}{d}} & \cdots \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \mathrm{e}^{\frac{2(d-1)\pi\mathrm{i}}{d}} & \mathrm{e}^{\frac{4(d-1)\pi\mathrm{i}}{d}} & \cdots \end{bmatrix} /\sqrt{d} \tag{24}$$

can realize the transformation between the Z_d-MB and the X_d-MB.

4. High-dimensional multiparty quantum secret sharing scheme with EPR pairs

Moreover, we can also generalize the above scheme to a n-party ($n \geq 4$) scheme. That is to say, if Alice wants to distribute her private key into $(n-1)$ receivers, i.e. Bob, Charlie, Dick, ..., and Zach, then, similar to the three-party scheme, the d-dimension multiparty scheme can be described as follows:

1) Bob prepares an EPR pair in the Bell state $|\Psi_{00}^d\rangle_{HT}$. Then he keeps the particle H and sends the other one T to Charlie.

2) After receiving the particle T, Charlie randomly chooses the message mode or check mode with the probabilities p_{bc} or $(1-p_{\mathrm{bc}})$. If Charlie's choice is check mode, then he performs the same security checking as the step (2) in Section 2; otherwise he randomly chooses one of the above unitary operators U_{nm}^d, noted as U_C, and two operations $\{I, H_d\}$ to encode and encrypt the particle T. After doing these, he sends the particle T to Dick.

3) Dick receives the particle T. He also randomly chooses the message mode or check mode with probability p_{cd} or $(1-p_{\mathrm{cd}})$. If the choice is check mode, he should use the same checking process as mentioned above to check the existent of the eavesdropping or the dishonest man; otherwise, he randomly chooses a unitary operators from U_{nm}^d, noted as U_{D}, and two operations $\{I, H_d\}$ to encode and encrypt the particle T. After doing these, he sends the particle T to the next receiver.

4) After receiving the particle T, the next receiver performs the same operations as Dick does, ... Deduced from this, the procedure continues until the last receiver Zach also finishes similar encoding process and sends the particle T to Alice.

5) After Alice has received the particle T, she can also choose the message mode or check mode with probability p_{za} or $(1-p_{\mathrm{za}})$. If Alice chooses the check mode, then the checking method is the same as that of Alice in section 2. If Alice chooses the message mode, then she randomly chooses one of the above unitary operators U_{nm}^d to encrypt the particle T and sends it to Zach.

6) After receiving this particle, Zach decrypts the particle T with the operation I or $H_d^\dagger$ same as that encrypted by him, and then requires Bob to send the particle H to her after he operates it with one of the d^2 local unitary operations, say U_{B}. After doing these, Zach performs a Bell measurement on those two par-

ticles and publishes the outcome.

7) Zach asks other $n-2$ participants (except Alice but including Bob) to cooperate with him, exchanging their results with each other. According to these results, they can deduce which local unitary operation is chosen by Alice and then get the information of the key.

All the above steps will be repeated N turns, and the security analysis is the same as that in the three-party case. Then through cooperation, all participants can obtain the information of Alice's operation respectively; otherwise, none of them can get anything.

In our scheme, only one particle need to be transmitted in each turn of the transmission process. So long as the security of the particle's transmission is guaranteed, then the whole QSS scheme will be secure. The details of how to guarantee the transmission security of one particle can be found in Refs.[25,26,37]. In our scheme, the method for the particle transmission and security check is the same as that in Refs.[25,26,37], so our scheme is also secure.

Moreover, in the schemes we have discussed above, we transmit one EPR pair after another. So, all participants, except Bob, do not need to store particle. They just need to store some intermediate results, such as some contrastive results. As a result, the storage space is greatly saved.

Another advantage of our scheme is that the code capacity on one qubit enhances greatly because the unitary operators which operate on the particle are randomly chosen from the d^2 unitary operators U_{nm}^d by each participant. Thereby, the utilization ratio as well as the transmission efficiency of particle are also improved.

5. Summary

To summarize, in this paper we have proposed a quantum secret sharing scheme by using EPR pairs and local unitary operators based on Zhang-Li-Man MQSS protocol, and then generalize this scheme to high dimension multiparty scheme. Our scheme has the advantage of not only having higher capacity, but also saving storage space. The security of our scheme is guaranteed.

References

[1] Blakley G R 1979 *in Proceedings of the American Federation of Information Processing* 1979 *National Computer Conference* (American Federation of Information Processing, Arlington, VA) 313

[2] Shamir A 1979 *Commun. ACM* **22** 612

[3] Hillery M, Bužek V and Berthiaume A 1999 *Phys. Rev.* A **59** 1829

[4] Karlsson A, Koashi M and Imoto N 1999 *Phys. Rev.* A **59** 162

[5] Gottesman D 2000 *Phys. Rev.* A **61** 042311

[6] Smith A 2000 quant-ph/0001087
Bandyopadhyay S 2000 *Phys. Rev.* A **62** 012308

[7] Nascimento A C A, Mueller-Quade J and Imai H 2001 *Phys. Rev.* A **64** 042311

[8] Cabello A 2001 quant-ph 0009025
Yang C P and Gea-Banacloche J 2001 *J. Opt. B: Quantum Semiclass. Opt.* **3** 407

[9] Karimipour V, Bahraminasab A and Bagherinezhad S 2002 *Phys. Rev.* A **65** 042320

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

[11] Tyc T and Sanders B C 2002 *Phys. Rev.* A **65** 042310

[12] Guo G P and Guo G C 2003 *Phys. Lett.* A **310** 247

[13] Lance A M, Symul T, Bowen W P, Tyc T, Sanders B C and Lam P K 2003 *New J. Phys.* **5** 4

[14] Tyc T, Rowe D J and Sanders B C 2003 *J. Phys.* A*: Math. Gen.* **36** 7625

[15] Sen A, Sen U and Zukowski M 2003 *Phys. Rev.* A **68** 032309

[16] Xiao L, Long G L, Deng F G and Pan J W 2004 *Phys. Rev.* A **69** 052307
Deng F G, Zhou H Y and Long G L 2005 *Phys. Lett.* A **337** 329
Deng F G, Long G L and Zhou H Y 2005 *Phys. Lett.* A **340** 43

[17] Zhang Y Q, Jin X R and Zhang S 2005 *Phys. Lett.* A **341** 380

[18] Yan F L and Gao T 2005 *Phys. Rev.* A **72** 012304

[19] Wang J, Zhang Q and Tang C J 2005 quant-ph 0510212

[20] Chen Z H and Lin X M 2005 *Chin. Phys.* **14** 1821

[21] Yang Y G, Wen Q Y and Zhu F C 2006 *Chin. Phys. Sin.* **55** 3255 (in Chinese)

[22] Cleve R, Gottesman D and Lo H K 1999 *Phys. Rev. Lett.* **83** 648

[23] Li Y M, Zhang K S and Peng K C 2004 *Phys. Lett.* A **324** 420

[24] Deng F G, Li X H, Li C Y, Zhou P and Zhou H Y 2005 *Phys. Rev.* A **72** 044301
Deng F G, Li C Y, Li Y S, Zhou H Y and Wang Y 2005 *Phys. Rev.* A **72** 022338

[25] Zhang Z J, Li Y and Man Z X 2005 *Phys. Rev.* A **71** 044301

[26] Deng F G and Long G L 2004 *Phys. Rev.* A **69** 052319
Deng F G and Long G L 2004 *Phys. Rev.* A **70** 012311

[27] Deng F G, Li X H, Zhou H Y and Zhang Z J 2005 *Phys. Rev.* A **72** 044302

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

[29] Bennett C H, DiVincenzo D P, Smolin J A and Wootters W K 1996 *Phys. Rev.* A **54** 3824
[30] Deutsch D, Ekert A, Jozsa R, Macchiavello C, Popescu S and Sanpera A 1996 *Phys. Rev. Lett.* **77** 2818
[31] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557
[32] Inamori H, Ralan L and Vedral V 2001 *J. Phys.* A **34** 6913
[33] Waks E, Zeevi A and Yamamoto Y 2002 *Phys. Rev.* A **65** 052310
[34] Deng F G, Li X H, Li C Y, Zhou P and Zhou H Y 2006 quant-ph 0602160
[35] Preskill J http://www.theory.caltech.edu/ preskill 229
[36] Bostrom K and Felbinger T 2002 *Phys. Rev. Lett.* **89** 187902
[37] Deng F G, Long G L and Liu X S 2003 *Phys. Rev.* A **68** 042317
[38] Wójcik A 2003 *Phys. Rev. Lett.* **90** 157901
[39] Degiovanni I P, Berchera I R, Castelletto S, Rastello M L, Bovino F A, Colla A M and Castagnoli G 2004 *Phys. Rev.* A **69** 032310
[40] Wójcik A 2005 *Phys. Rev.* A **71** 016301
[41] Degiovanni I P, Berchera I R, Castelletto S, Rastello M L, Bovino F A, Colla A M and Castagnoli G 2005 *Phys. Rev.* A **71** 016302
[42] Lucamarini M and Mancini S 2005 *Phys. Rev. Lett.* **94** 140501
[43] Fuchs C A, Gisin N, Griffiths R B, Niu C S and Peres A 1997 *Phys. Rev.* A **56** 1163
[44] Gisin N and Griffiths R B 1999 *Phys. Rev.* A **60** 2764
[45] Sen(De) A, Sen U and Żukowski M 2003 *Phys. Rev.* A **68** 032309
[46] Scarani V and Gisin N 2001 *Phys. Rev. Lett.* **87** 117901
[47] Cai Q Y and Li B W 2004 *Phys. Rev.* A **69** 054301
[48] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)
[49] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
[50] Bennett C H and Brassard G 1984 *Proc. IEEE Int.Conf. on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York) 175
[51] Bennett C H, Brassard G, Crépeau C, Jozsa R, Peres A and Wootters W K 1993 *Phys. Rev. Lett.* **70** 1895
[52] Zeng B, Liu X S, Li Y S and Long G L 2002 *Commun. Theor. Phys.* **38** 537
[53] Liu X S, Long G L, Tong D M and Li F 2002 *Phys. Rev.* A **65** 022304
[54] Wang C, Deng F G, Li Y S, Liu X S and Long G L 2005 *Phys. Rev.* A **71** 044305
[55] Wang C, Deng F G and Long G L 2005 *Opt. Commun.* **253** 15
[56] Bechmann-Pasquinucci H and Peres A 2000 *Phys. Rev. Lett.* **85** 3313