Vol 17 No 2, February 2008
1674-1056/2008/17(02)/0624-04

Chinese Physics B

© 2008 Chin. Phys. Soc.
and IOP Publishing Ltd

Quantum state sharing of an arbitrary qudit state by using nonmaximally generalized GHZ state

Tao Ying-Juan(陶应娟)[a)†], Tian Dong-Ping(田东平)[b)],
Hu Ming-Liang(胡明亮)[a)], and Qin Meng(秦 猛)[a)]

[a)] *School of Science, Xi'an Jiaotong University, Xi'an* 710049, *China*

[b)] *Xi'an Institute of Post and Telecommunication, Xi'an* 710061, *China*

(Received 25 May 2007; revised manuscript received 28 June 2007)

We present a scheme for quantum state sharing of an arbitrary qudit state by using nonmaximally entangled generalized Greenberger–Horne–Zeilinger (GHZ) states as the quantum channel and generalized Bell-basis states as the joint measurement basis. We show that the probability of successful sharing an unknown qudit state depends on the joint measurements chosen by Alice. We also give an expression for the maximally probability of this scheme.

Keywords: quantum state sharing, qudit state, partially entangled channels
PACC: 4250, 0367

1. Introduction

The basic idea of secret sharing is that a secret key transmitted by a sender is shared between two or more recipients in such a way that the key can be reconstructed only if all recipients collaborate with each other. Quantum secret sharing (QSS) is the generalization of classical secret sharing into quantum scenario, i.e., QSS is used to complete the task of classical secret sharing with the principles of quantum mechanics. Since Hillery *et al*[1] presented the first QSS scheme by using a three-qubit or a four-qubit Greenberger–Horne–Zeilinger (GHZ) state for securely sharing an arbitrary unknown single-qubit state in 1999, QSS has been intensively investigated.[2−22]

Different from classical secret sharing, QSS has two main goals: one deals with the QSS of classical messages;[2−7,18−21] another deals with the QSS of quantum information,[1,8−17,22] where the secret is an arbitrary unknown quantum state. The former is usually referred as quantum secret sharing (QSS); the latter as quantum state sharing (QSTS), which was first clearly termed by Lance *et al* in 2004.[10] Recently, Li *et al* [13] proposed an efficient symmetric multiparty QSTS scheme of an arbitrary m-qubit state with m GHZ states, and Zhang *et al* [14] proposed a three-party QSTS scheme for an unknown single-qutrit state.

In the above protocols, the quantum channels used to teleport the qubits are noiseless maximally entangled state. But in a realistic scenario noisy effects and decoherence decrease the entanglement of the channel. In this scenario, the quantum channels may be a non-maximally entangled state. So it is significative to investigate the QSS scheme of an arbitrary qudit state by using non-maximally entangled state as quantum channel. Very recently, Gordon and Rigolin[15] proposed two new QSTS protocols where the quantum channels are not maximally entangled states, Man *et al* [22] presented a quantum state sharing of an arbitrary multiqubit state using nonmaximally GHZ entangled states. Pati and Agrawal[23] presented a probability teleportation of a qudit. In this paper, we will propose a QSTS protocol for sharing an arbitrary unknown qudit state using nonmaximally entangled state as a quantum channel. Moreover, in essence, this QSTS scheme can also be used for symmetric controlled teleportation by means of some agents acting as the controllers in the latter.

This paper is organized as follows. In Section 2, a three-party QSTS scheme for sharing an arbitrary single-qudit state by using nonmaximally entangled GHZ state is presented and the scheme security is also analysed. In Section 3, the three-party QSTS scheme is generalized to a multiparty case for an arbitrary qudit state. Finally, summaries are given in Section 4.

†E-mail: taoyingjuan@stu.xjtu.edu.n

2. Three-party quantum state sharing of an arbitrary single-qudit state

We first consider the three-party QSTS scheme for sharing an arbitrary single-qudit state in this section for clarity. Suppose that Alice wants to transmit an arbitrary single-qudit state $|\phi\rangle$ to two remote agents Bob and Charlie in such a way that only one of them can faithfully reconstruct the original state with the help of the other agent, where $|\phi\rangle$ has the form

$$|\phi\rangle_1 = \sum_{i=0}^{d-1} \alpha_i |i\rangle_1, \tag{1}$$

with the unknown complex coefficient α_i and $\sum_{i=0}^{d-1} |\alpha_i|^2 = 1$. Let Alice share with Bob and Charlie a nonmaximally entangled generalized GHZ (GGHZ) state in advance as a quantum channel,

$$|\Psi\rangle_{\rm ABC} = D \sum_{j=0}^{d-1} d_j |jjj\rangle_{\rm ABC}, \tag{2}$$

where d_j is complex coefficient and $D = 1/\sqrt{\sum_{j=0}^{d-1} |d_j|^2}$ is the normalization constant. Subsequently, the initial state of the system can be written as

$$\begin{aligned} |\Psi\rangle_s &= |\phi\rangle_1 \otimes |\Psi\rangle_{\rm ABC} \\ &= D \sum_{i=0}^{d-1} \alpha_i |i\rangle_1 \\ &\quad \otimes \sum_{j=0}^{d-1} d_j |jjj\rangle_{\rm ABC}, \end{aligned} \tag{3}$$

where 1 and A label Alice's two qudits, B labels Bob's qudit and C labels Charlie's qudit. Let us introduce a set of generalized entangled Bell state as follows:

$$|\Phi^{xy}\rangle = D^{xy} \sum_{k=0}^{d-1} {\rm e}^{2\pi {\rm i} kx/d} d_k^{xy} |k\rangle \otimes |k \oplus y\rangle, \tag{4}$$

where $x,\ y \in \{0, 1, \cdots, d-1\}$, $D^{xy} = 1/\sqrt{\sum_{k=0}^{d-1} |d_k^{xy}|^2}$, which is the normalization constant, and $k \oplus y$ means the sum of k and y modulo d. The coefficients $\{d_k^{xy}\}$ should satisfy the following orthonormal condition

$$D^{x_1 y} D^{x_2 y} \sum_{k=0}^{d-1} d_k^{*x_1 y} d_k^{x_2 y} {\rm e}^{2\pi {\rm i} k(x_2 - x_1)} = \delta^{x_1 x_2}, \tag{5}$$

with the indices $x_1,\ x_2,\ y \in \{0, 1, \cdots, d-1\}$. Thus the state of the system can be rewritten as

$$\begin{aligned} |\Psi\rangle_{\rm s} &= |\phi\rangle_1 \otimes |\Psi\rangle_{\rm ABC} \\ &= D \sum_{xy} |\Phi^{xy}\rangle_{\rm 1A} D^{xy} \sum_{k=0}^{d-1} d_k^{*xy} d_{k\oplus y} \alpha_k \\ &\quad \times {\rm e}^{-2\pi {\rm i} kx/d} |k \oplus y\rangle_{\rm B} |k \oplus y\rangle_{\rm C}. \end{aligned} \tag{6}$$

Now Alice performs the generalized Bell-basis $\{|\Phi^{xy}\rangle\}$ measurement on her qudit pair $\{1, {\rm A}\}$, and then she can assign either Bob or Charlie to reconstruct the unknown state. Without loss of generality, suppose Bob is the assigned. The agent Charlie would collaborate with Bob by first performing a transformation on his particle C and then measuring it in the generalized computational basis $\{|0\rangle, |1\rangle, \cdots, |d-1\rangle\}$. The transformation performed by Charlie is defined as

$$F^{(d)} |j\rangle = \frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} {\rm e}^{2\pi {\rm i} lj/d} |l\rangle. \tag{7}$$

Then the state of qudits B and C becomes

$$|\Psi\rangle_{\rm BC} = \frac{1}{\sqrt{d}} D D^{xy} \sum_{l=0}^{d-1} \left(\sum_{k=0}^{d-1} {\rm e}^{2\pi {\rm i}((k\oplus y)l - kx)/d} d_k^{*xy} d_{k\oplus y} \alpha_k |k \oplus y\rangle_{\rm B} \right) |l\rangle_{\rm C} \tag{8}$$

for an outcome $|\Phi^{xy}\rangle_{\rm 1A}$. Charlie measures his particle C in the generalized computational basis $\{|0\rangle, |1\rangle, \cdots, |d-1\rangle\}$. If his result is $|l\rangle_{\rm C}$, then the state of Bob becomes

$$|\Psi\rangle_{\rm B} = \frac{1}{\sqrt{d}} D D^{xy} \sum_{k=0}^{d-1} {\rm e}^{2\pi {\rm i}((k\oplus y)l - kx)/d} d_k^{*xy} d_{k\oplus y} \alpha_k |k \oplus y\rangle_{\rm B}. \tag{9}$$

When Bob knows the results of the sender Alice and the agent Charlie, he can reconstruct the original state by performing a proper local transformation on his qudit. If the results are $|\Phi^{xy}\rangle_{\rm 1A}$ and $l_{\rm c}$, the corresponding local transformation U^{xyl} is

$$U^{xyl} = \sum_{k=0}^{d-1} {\rm e}^{2\pi {\rm i}(kx - (k\oplus y)l)/d} |k\rangle \langle k \oplus y|. \tag{10}$$

Then the state of his qudit becomes

$$U^{xyl} |\Psi\rangle_{\rm B} = \frac{1}{\sqrt{d}} D D^{xy} \sum_{k=0}^{d-1} d_k^{*xy} d_{k\oplus y} \alpha_k |k\rangle_{\rm B}. \tag{11}$$

From Eq.(11), we find that the measuring basis parameters $\{d_k^{xy}\}$ can be freely manipulated by Alice. By proper adjusting it, Alice can achieve a unity fidelity protocol with a certain probability. Obvi-

ously, the protocol will be successful with a probability $|DD^{xy}|^2$ for an outcome $|\Phi^{xy}\rangle$ if $\{d_k^{xy}\} = \left\{\frac{1}{d^*_{k\oplus y}}\right\}$; otherwise, the protocol will be failed. However, those parameters must also satisfy the orthonormality condition in Eq.(5). Combining the two conditions, we obtain

$$\sum\nolimits_{k=0}^{d-1} \frac{1}{|d_{k\oplus y}|^2} \frac{1}{\sum_{p=0}^{d-1}\left(\frac{1}{|d_{p\oplus y}|^2}\right)} \mathrm{e}^{2\pi \mathrm{i} k(x_2-x_1)} = \delta^{x_1 x_2}. \tag{12}$$

This equation shows that the two conditions can be satisfied simultaneously only when $x_1 = x_2$. That is to say, the measurement results, which can lead to successful protocol, are at most d out of the total d^2 possible results of Alice. So we can calculate explicitly the maximal probability of success in sharing an unknown single-qudit state

$$\begin{aligned} P_{\max} =& d|DD^{xy}|^2 \\ =& \frac{d}{\sum_{j=0}^{d-1}|d_j|^2 \sum_{k=0}^{d-1}\left(\frac{1}{|d_k|^2}\right)}. \end{aligned} \tag{13}$$

In other words, the successful probability is dependent on the Bell-basis measurement chosen by Alice. By adjusting the parameters $\{d_k^{xy}\}$, she can control the successful probability to gain one value of $\{0, |DD^{xy}|^2, 2|DD^{xy}|^2, \ldots, d|DD^{xy}|^2\}$. It is worth mentioning that the channel information is not necessary for both Bob and Charlie, and the protocol will correspond to the qubit (qutrit) case when d=2 (3).

The security checking of this protocol is very similar to the methods described in Refs.[1,10,14,15]. Let us consider two kinds of eavesdroppers or cheaters separately in the following.

1) Outsider eavesdropper or cheater: Suppose there is an eavesdropper who wants to gain the quantum information transmitted by Alice by entangling an ancilla with the quantum channel during the particles distribution process. In order to check whether there is an eavesdropper or not, Alice chooses a randomly single-qudit measurement basis to measure her GGHZ qudit, and Bob and Charlie use the same measurement as Alice to measure their respective qudits. Their measurement results should be strongly correlated. But if there exists an eavesdropper who wants to gain information about Alice's state, he (she) must invariably introduce errors. Thus, when the three parties publicly compare their results, the outside eavesdropper can be detected.

2) Inside eavesdropper or cheater: Suppose one of the two agents, Bob or Charlie, is dishonest, and he wants to solely recover Alice's quantum state or supply wrong information so that the other agent cannot obtain the right state. Only when Alice assigns him to reconstruct the state, he can avoid the security detection, otherwise, he can be disclosed.

3. Multi-party quantum state sharing of an arbitrary multi-qudit state

In this section, we will further generalize the above method to present the multi-party QSTS scheme for sharing an arbitrary m-qudit state. We omit the normalized factors in the following for simplicity. Suppose that the m-qudit state Alice wants to send is

$$\begin{aligned} |\phi\rangle_{1,2,\cdots,m} =& \sum\nolimits_{i_1=0}^{d-1}\sum\nolimits_{i_2=0}^{d-1}\cdots\sum\nolimits_{i_m=0}^{d\text{ - }1} \\ & \times \alpha_{i_1,i_2,\cdots,i_m}|i_1,i_2,\cdots,i_m\rangle. \end{aligned} \tag{14}$$

Alice prepares m generalized GHZ states as the quantum channel

$$\begin{aligned} |\Psi\rangle_{x_i,b_{i1},\cdots,b_{in}} =& D_i \sum\nolimits_{j_i=0}^{d-1} d_{j_i}|j_i,j_i,\cdots,j_i\rangle \\ & \text{with}\ \ i=1,2,\cdots,m. \end{aligned} \tag{15}$$

After Alice performing m generalized Bell-basis measurements on her particle pairs $\{(i,\ x_i)\}$ in the basis $\{|\Phi^{xy}\rangle\}$, the state of the subsystem becomes (for the outcomes $\{|\phi\rangle_{ix_i}^{x_i y_i}\}$)

$$\begin{aligned} |\Psi\rangle_{sub} =& {}_{1x_1}\langle\Phi_{x_1y_1}|\cdots{}_{mx_m}\langle\Phi_{x_my_m}||\phi\rangle_{1,2,\cdots,m}|\Psi\rangle_{x_1,b_{11},\cdots,b_{1n}}\cdots|\Psi\rangle_{x_m,b_{m1},\cdots,b_{mn}} \\ =& \prod\nolimits_{t=1}^{m} D_t D_t^{x_t y_t} \sum\nolimits_{k_t=0}^{d-1} \mathrm{e}^{-2\pi \mathrm{i} k_t x_t/d} d_{k_t}^{*x_t y_t} d_{k_t\oplus y_t} \alpha_{k_1,k_2,\cdots,k_m} \\ & \times |k_t\oplus y_t\rangle|k_t\oplus y_t\rangle\cdots|k_t\oplus y_t\rangle_{b_{t1},\cdots,b_{tn}}. \end{aligned} \tag{16}$$

Suppose Alice assigns the p-th agent to reconstruct the original state. All the other agents perform the $F^{(d)}$

transformations on their qudits respectively and then the state becomes

$$|\Psi\rangle_{sub} = \prod_{t=1}^{m} D_t D_t^{x_t y_t} \Bigg(\prod_{j=1}^{n} \sum_{l_{tj}=0}^{d-1} \Bigg(\sum_{k_t=0}^{d-1} \mathrm{e}^{2\pi \mathrm{i}((k_t \oplus y_t) l_t - k_t x_t)/d} \times d_{k_t}^{*x_t y_t} d_{k_t \oplus y_t} \alpha_{k_1,k_2,\cdots,k_m} |k_t \oplus y_t\rangle |l_{tj}\rangle \Bigg) \Bigg), \tag{17}$$

where $l_t = l_{t1} \oplus l_{t2} \oplus \cdots \oplus l_{tn}$, which represents the results of the j-th agent's particles. After each of the other agents performed the $F^{(d)}$ transformations and generalized computational measurements on his (her) qudits separately, the state of Bob becomes

$$\prod_{t=1}^{m} D_t D_t^{x_t y_t} \Bigg(\sum_{k_t=0}^{d-1} \mathrm{e}^{2\pi \mathrm{i}((k_t \oplus y_t) l_t - k_t x_t)/d} \times d_{k_t}^{*x_t y_t} d_{k_t \oplus y_t} \alpha_{k_1,k_2,\cdots,k_m} |k_t \oplus y_t\rangle \Bigg), \tag{18}$$

which is similar to the state in Eq.(9). So the local operations performed on qudit particles b_{p1}, $b_{p2} \cdots b_{pm}$ by the receiver are similar to that in the three-party case. The local operations performed on the t-th particle of the receiver is $U^{x_t y_t l_t}$ and

$$U^{x_t y_t l_t} = \sum_{k_t=0}^{d-1} \mathrm{e}^{2\pi \mathrm{i}(k_t x_t - (k_t \oplus y_t) l_t)/d} |k_t\rangle \langle k_t \oplus y_t|, \tag{19}$$

where $t = 1, 2, \cdots, m$. And similar to the three-party case, Alice can freely adjust the measurement basis parameters $\{d_{k_t}^{x_t y_t}\}$ to control the probability of the protocol, and the probability has the maximal value $\prod_{t=1}^{m} d^m |D^t D^{x_t y_t}|^2 = \prod_{t=1}^{m} \frac{d^m}{\sum_{j_t=0}^{d-1} |d_{j_t}|^2 \sum_{k_t=0}^{d-1} \left(\frac{1}{|d_{k_t}|^2} \right)}$ when $\{d_{k_t}^{x_t y_t}\} = \left\{ \frac{1}{d_{k_t \oplus y_t}^*} \right\}$.

The security of the multi-party qudit state sharing scheme is the same as the security of the three-party case. An eavesdropper can be detected by publicly comparing a subset of the quantum state.

4. Conclusions

We have presented a scheme for quantum state sharing of an arbitrary qudit state by using nonmaximally entangled generalized GHZ states as the quantum channel and the generalized Bell-basis as the joint measurement basis. For sharing an arbitrary qudit state, Alice should perform m generalized Bell-basis measurements on her particle pairs and assign any one of the agents to reconstruct the unknown quantum state. In order to help the receiver, the other agents should first perform $F^{(d)}$ transformations and then the generalized computational measurements on their particles separately. We have shown that the probability of successful sharing an unknown qudit state is dependent on the joint measurements which are adjusted by Alice, and also we have given an explicit expression for the maximal probability of this scheme.

References

[1] Hillery M, Bužek V and Berthiaume A 1999 *Phys. Rev.* A **59** 1829
[2] Karlsson A, Koashi M and Imoto N 1999 *Phys. Rev.* A **59** 162
[3] Gottesman D 2000 *Phys. Rev.* A **61** 042311
[4] Tittel W, Zbinden H and Gisin N 2001 *Phys. Rev.* A **63** 042301
[5] Karimipour V, Bahraminasab A and Bagherinezhad S 2002 *Phys. Rev.* A **65** 042320
[6] Zhang Z J, Li Y and Man Z X 2005 *Phys. Rev.* A **71** 044301
[7] Zhang Z J and Man Z X 2005 *Phys. Rev.* A **72** 022303
[8] Bandyopadhyay S 2000 *Phys. Rev.* A **62** 012308
[9] Li Y M, Zhang K S and Peng K C 2004 *Phys. Lett.* A **324** 420
[10] Lance A M, Symul T, Bowen W P, Sanders B C and Lam P K 2004 *Phys. Rev. Lett.* **92** 177903
[11] Deng F G *et al* 2005 *Phys. Rev.* A **72** 022338
[12] Deng F G, Li X H, Li C Y, Zhou P and Zhong H Y quant-ph/0509029
[13] Li X H, Zhou P, Li C Y, Zhou H Y and Deng F G quant-ph/0511223v2
[14] Wang Z Y and Zhang Z J quant-ph/0607187
[15] Gordon G and Rigolin G 2006 *Phys. Rev.* A **73** 062316
[16] Agrawal and Pati A K 2002 *Phys. Lett.* A **305** 12
[17] Huang Y C and Liu M 2005 *Acta Phys.Sin.* **54** 4517 (in Chinese)
[18] Chen P, Deng F G and Long G L 2006 *Chin. Phys.* **15** 2228
[19] Liu W T, Liang L M, Li C Z and Yuan J M 2006 *Chin. Phys. Lett.* **12** 3148
[20] Deng F G, Zhou P, Li X H, Li C Y and Zhou H Y 2006 *Chin. Phys. Lett.* **5** 1084
[21] Xue Z H, Yi Y M and Cao Z L 2006 *Chin. Phys.* **15** 1421
[22] Man Z X, Xia Y J and An N B 2007 *Eur. Phys. J.* D **42** 333
[23] Pati A K and Agrawal P quant-ph/0611115v1