Int J Theor Phys (2008) 47: 2353–2362
DOI 10.1007/s10773-008-9669-2

Generalized Multiparty Quantum Single-Qutrit-State Sharing

Jun Liu · Yi-Min Liu · Zhan-Jun Zhang

Received: 21 November 2007 / Accepted: 21 January 2008 / Published online: 25 January 2008

Abstract We present a three-party quantum single-qutrit-state sharing scheme with a non-maximally entangled three-qutrit state as the quantum channel. In the scheme, the sender's secret quantum information (i.e., the single-qutrit state) is split in such a way that it can be probabilistically reconstructed through introducing an auxiliary qutrit and performing appropriate operations provided that the receivers both collaborate together. We work out the success probability and reveal the relation between the probability and the parameters characterizing the quantum channel. After this, we then briefly introduce the generalization of the three-party scheme to a more-party one.

Keywords Generalized quantum state sharing · Non-maximally entangled state · Bell-state measurement · Single-qutrit projective measurement

Quantum information is an ingenious application of quantum mechanics within the field of information. So far, it has attracted a lot of attentions [1–5]. After Bennett and Brassard's pioneering work [6] published in 1984, almost all the branches of quantum communication have been developed quickly, such as quantum key distribution (QKD) [6–14], quantum secure direct communication (QSDC) [15–17], quantum teleportation [3, 4], quantum secret sharing (QSS) [18–48], and so on.

As a novel and quite different quantum cryptographic protocol, QSS is recently pursued by some groups [19–48] after Hillery, Bůzek, and Berthiaume (HBB) [18] proposed

J. Liu · Z.-J. Zhang (✉)
Key Laboratory of Optoelectronic Information Acquisition & Manipulation of Ministry of Education of China, School of Physics & Material Science, Anhui University, Hefei 230039, China
e-mail: zjzhang@ahu.edu.cn

Y.-M. Liu
Department of Physics, Shaoguan University, Shaoguan 512005, China

Z.-J. Zhang
Department of Physics and Center for Quantum Information Science, National Cheng Kung University, Tainan 70101, Taiwan

their original idea in 1999. QSS is likely to play a key role in both transmitting of a classical information and protecting a secret quantum information, such as in secure operations of distributed quantum computation, sharing difficult-to-construct ancillary states and joint sharing of quantum money [20, 29, 30]. To date, QSS has progressed quickly and becomes one of the most important applications of quantum information.

QSS concentrates mainly on two kinds of research works, one only deals with the QSS of classical information (i.e., bits), another deals with the QSS of quantum information, where the secret is an arbitrary unknown quantum state. Until 2004, the latter case was first clearly termed by Lance et al. [39] as the quantum state sharing (QSTS). Till now, various kinds of QSTS schemes have been proposed. For instance, the original QSTS protocol was put forward by HBB in 1999 by using a three-particle or a four-particle Greenberger-Horne-Zeilinger (GHZ) state for securely sharing an arbitrary unknown single-qubit state [18]. Soon after, Cleve et al. [35] investigated a more general quantum (k,n) threshold QSTS scheme. Bandyopadhyay [36] proposed a QSTS scheme by using optimal methods in 2000, and Hsu [37] proposed a further QSTS scheme based on Grover's algorithm in 2003. Recently, Li et al. [38] proposed a QSTS scheme for sharing an unknown single-qubit state with a multipartite joint measurement. Some QSTS schemes were implemented in cavity QED [42]. Zhang et al. [43] proposed a multiparty QSTS of an arbitrary unknown single-qubit state via photon pairs. Lance et al. [39, 44] proposed a continuous-variable QSTS scheme via quantum disentanglement. Deng et al. [45, 46] proposed two QSTS schemes for sharing an arbitrary two-qubit state based on entanglement swapping. Li et al. [47] proposed an efficient symmetric multiparty QSTS scheme of an arbitrary m-qubit state with m GHZ states. Wang et al. [48] proposed a three-party single-qutrit state sharing scheme by using a generalized GHZ state as the quantum channel. Notice that, for these schemes though the quantum channels may be different seemingly, they are all maximally entangled states in common.

In 2006, Gordon and Rigolin [49] first proposed two new *single-qubit* state sharing protocols by using non-maximally entangled states as the quantum channel. Soon later, Wang et al. [50] presented a scheme for probabilistically implementing quantum state sharing of an arbitrary *two-qubit* state by utilizing two non-maximally entangled three-qubit states as the quantum channel. In this paper we will propose a multi-party QSTS protocol for probabilistically sharing a *single-qutrit* state by using a non-maximally entangled three-qutrit state as the quantum channel.

For convenience, first we will introduce the three-party protocol. Suppose Alice is the initial owner of the secret quantum information (i.e., the single-qutrit state). She wants to let her two agents (say, Bob and Charlie) to share her secret quantum information in such a way that if and only if both agents collaborate together they can obtain it. This goal can be achieved by our following three-party QSTS scheme with 6 steps.

(1) The secret quantum information Alice wants to let Bob and Charlie share is the state in her qutrit 1, i.e.,

$$|P\rangle_1 = \alpha|0\rangle_1 + \beta|1\rangle_1 + \gamma|2\rangle_1, \tag{1}$$

where α, β and γ are complex and satisfy $|\alpha|^2 + |\beta|^2 + |\gamma|^2 = 1$. Moreover, Alice owns another qutrit (say, the qutrit 2), Bob the qutrit 3 and Charlie the qutrit 4. The three qutrits 2, 3 and 4 are in a non-maximally entangled state

$$|\psi\rangle_{234} = a|000\rangle_{234} + b|111\rangle_{234} + c|222\rangle_{234}, \tag{2}$$

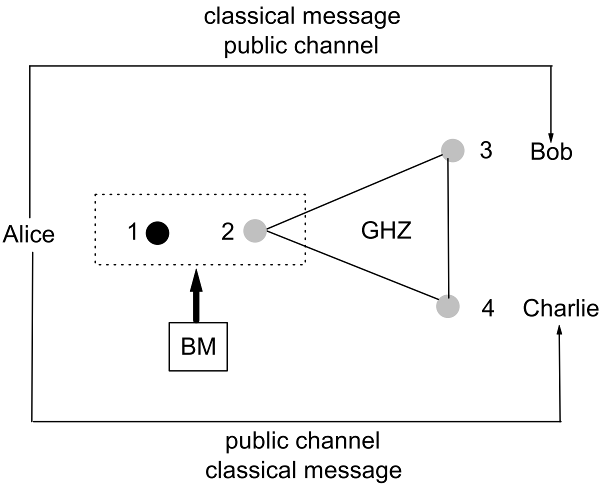


Fig. 1 Alice makes a generalized Bell-state measurement (BM) on qutrit pair (1, 2) and informs Bob and Charlie of the result. See steps (1)–(3) for details

where a, b and c are real, $|a|^2+|b|^2+|c|^2=1$, $|a|>|b|>|c|$. In this case, the combined state of the four qutrits is

$$|\Phi\rangle_{1234}=|P\rangle_1\otimes|\psi\rangle_{234}. \tag{3}$$

(2) To let the two agents share her secret quantum information, Alice first performs a generalized Bell-state measurement on her qutrit pair (1, 2) (see Fig. 1). After Alice's measurement, the system's state collapses to one of the following nine possible results:

$$|\Psi_{00}\rangle_{12}\langle\Psi_{00}|\Phi\rangle=\frac{1}{\sqrt{3}}|\Psi_{00}\rangle_{12}(a\alpha|00\rangle_{34}+b\beta|11\rangle_{34}+c\gamma|22\rangle_{34}), \tag{4}$$

$$|\Psi_{01}\rangle_{12}\langle\Psi_{01}|\Phi\rangle=\frac{1}{\sqrt{3}}|\Psi_{01}\rangle_{12}(b\alpha|11\rangle_{34}+c\beta|22\rangle_{34}+a\gamma|00\rangle_{34}), \tag{5}$$

$$|\Psi_{02}\rangle_{12}\langle\Psi_{02}|\Phi\rangle=\frac{1}{\sqrt{3}}|\Psi_{02}\rangle_{12}(c\alpha|22\rangle_{34}+a\beta|00\rangle_{34}+b\gamma|11\rangle_{34}), \tag{6}$$

$$|\Psi_{10}\rangle_{12}\langle\Psi_{10}|\Phi\rangle=\frac{1}{\sqrt{3}}|\Psi_{10}\rangle_{12}(a\alpha|00\rangle_{34}+e^{-2\pi i/3}b\beta|11\rangle_{34}+e^{-4\pi i/3}c\gamma|22\rangle_{34}), \tag{7}$$

$$|\Psi_{11}\rangle_{12}\langle\Psi_{11}|\Phi\rangle=\frac{1}{\sqrt{3}}|\Psi_{11}\rangle_{12}(b\alpha|11\rangle_{34}+e^{-2\pi i/3}c\beta|22\rangle_{34}+e^{-4\pi i/3}a\gamma|00\rangle_{34}), \tag{8}$$

$$|\Psi_{12}\rangle_{12}\langle\Psi_{12}|\Phi\rangle=\frac{1}{\sqrt{3}}|\Psi_{12}\rangle_{12}(c\alpha|22\rangle_{34}+e^{-2\pi i/3}a\beta|00\rangle_{34}+e^{-4\pi i/3}b\gamma|11\rangle_{34}), \tag{9}$$

$$|\Psi_{20}\rangle_{12}\langle\Psi_{20}|\Phi\rangle=\frac{1}{\sqrt{3}}|\Psi_{20}\rangle_{12}(a\alpha|00\rangle_{34}+e^{-4\pi i/3}b\beta|11\rangle_{34}+e^{-8\pi i/3}c\gamma|22\rangle_{34}), \tag{10}$$

$$|\Psi_{21}\rangle_{12}\langle\Psi_{21}|\Phi\rangle=\frac{1}{\sqrt{3}}|\Psi_{21}\rangle_{12}(b\alpha|11\rangle_{34}+e^{-4\pi i/3}c\beta|22\rangle_{34}+e^{-8\pi i/3}a\gamma|00\rangle_{34}), \tag{11}$$

$$|\Psi_{22}\rangle_{12}\langle\Psi_{22}|\Phi\rangle=\frac{1}{\sqrt{3}}|\Psi_{22}\rangle_{12}(c\alpha|22\rangle_{34}+e^{-4\pi i/3}a\beta|00\rangle_{34}+e^{-8\pi i/3}b\gamma|11\rangle_{34}), \tag{12}$$

where

$$|\Psi_{nm}\rangle = \sum_{j=0}^{2} e^{2\pi ijn/3}|j\rangle \otimes |(j+m) \bmod 3\rangle/\sqrt{3}, \quad n \in \{0,1,2\},\ m \in \{0,1,2\}. \tag{13}$$

(3) Alice publicly announces her measurement result. Although each outcome dose not occur with equal probability (because (4)–(12) are unnormalize, we can not consider the probability of each outcome occurs is 1/9 equally), the subsequent is similar. For convenience, only one case is taken as an example hereafter. Without loss of generality, suppose Alice's measurement result is $|\Psi_{00}\rangle_{12}$. After normalization, we can get $|\Psi_{00}\rangle_{12}$ occurs with the probability $\rho_1 = [(a\alpha)^2 + (b\beta)^2 + (c\gamma)^2]/3$. In this case, the qutrits 3 and 4 collapse to the entangled state

$$|K\rangle_{34} = \frac{1}{\sqrt{3}}(a\alpha|00\rangle_{34} + b\beta|11\rangle_{34} + c\gamma|22\rangle_{34}). \tag{14}$$

This state can be rewritten as

$$\begin{aligned}|K\rangle_{34} &= \frac{1}{\sqrt{3}}(a\alpha|00\rangle_{34} + b\beta|11\rangle_{34} + c\gamma|22\rangle_{34})\\ &= \frac{1}{\sqrt{3}}\Bigg[\frac{1}{\sqrt{3}}|\xi_0\rangle_3(a\alpha|0\rangle_4 + b\beta|1\rangle_4 + c\gamma|2\rangle_4)\\ &\quad + \frac{1}{\sqrt{3}}|\xi_1\rangle_3(a\alpha|0\rangle_4 + e^{-2\pi i/3}b\beta|1\rangle_4 + e^{-4\pi i/3}c\gamma|2\rangle_4)\\ &\quad + \frac{1}{\sqrt{3}}|\xi_2\rangle_3(a\alpha|0\rangle_4 + e^{-4\pi i/3}b\beta|1\rangle_4 + e^{-2\pi i/3}c\gamma|2\rangle_4)\Bigg],\end{aligned} \tag{15}$$

where

$$\begin{aligned}|\xi_0\rangle &= \frac{1}{\sqrt{3}}(|0\rangle + |1\rangle + |2\rangle),\\ |\xi_1\rangle &= \frac{1}{\sqrt{3}}(|0\rangle + e^{2\pi i/3}|1\rangle + e^{4\pi i/3}|2\rangle),\\ |\xi_2\rangle &= \frac{1}{\sqrt{3}}(|0\rangle + e^{4\pi i/3}|1\rangle + e^{2\pi i/3}|2\rangle).\end{aligned} \tag{16}$$

The three states $\{|\xi_t\rangle, t = 0,1,2\}$ are related to the computation basis vectors $\{|0\rangle, |1\rangle, |2\rangle\}$, and form a complete orthogonal basis set of a single-qutrit Hilbert space.

(4) Bob measures his qutrit in the orthogonal bases $B_s = \{|\xi_0\rangle, |\xi_1\rangle, |\xi_2\rangle\}$ and informs Charlie of the result (see Fig. 2). This measurement is a single-qutrit projective measurement. Obviously, there are three possible cases. *Case 1:* If Bob's measurement result is $|\xi_0\rangle_3$, the qutrit 4 is projected onto $|G_1\rangle_4 = a\alpha|0\rangle_4 + b\beta|1\rangle_4 + c\gamma|2\rangle_4$, Charlie first applies a unitary operation $U_0 = I$ on qutrit 4, then the scheme goes to step (5). *Case 2:* If Bob's measurement result is $|\xi_1\rangle_3$, the qutrit 4 is projected onto $|G_2\rangle_4 = a\alpha|0\rangle_4 + e^{-2\pi i/3}b\beta|1\rangle_4 + e^{-4\pi i/3}c\gamma|2\rangle_4$, Charlie first performs a unitary operation $U_1 = \sum_{j=0}^{2} e^{2\pi ij/3}|j\rangle\langle j|$ on qutrit 4 to turn $|G_2\rangle_4$ to $|G_1\rangle_4$, then the scheme goes to step (5). *Case 3:* If Bob's measurement result is $|\xi_2\rangle_3$, the qutrit 4 is projected onto $|G_3\rangle_4 = a\alpha|0\rangle_4 + e^{-4\pi i/3}b\beta|1\rangle_4 + e^{-2\pi i/3}c\gamma|2\rangle_4$, Charlie first carries out a unitary operation $U_2 = \sum_{j=0}^{2} e^{4\pi ij/3}|j\rangle\langle j|$ on qutrit 4 to change $|G_3\rangle_4$ to $|G_1\rangle_4$,

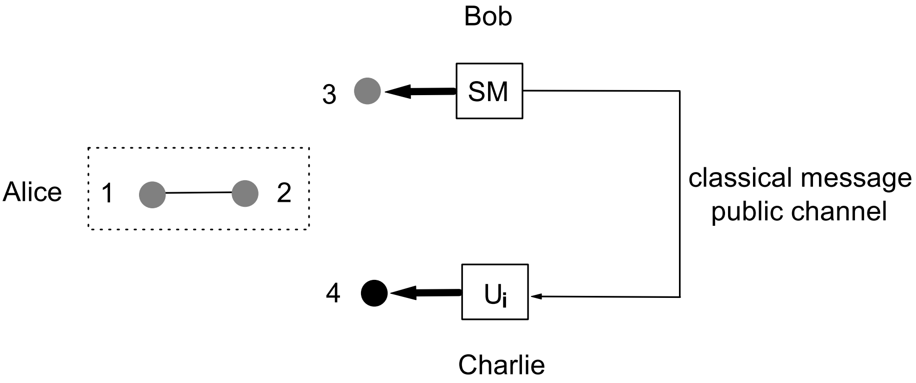
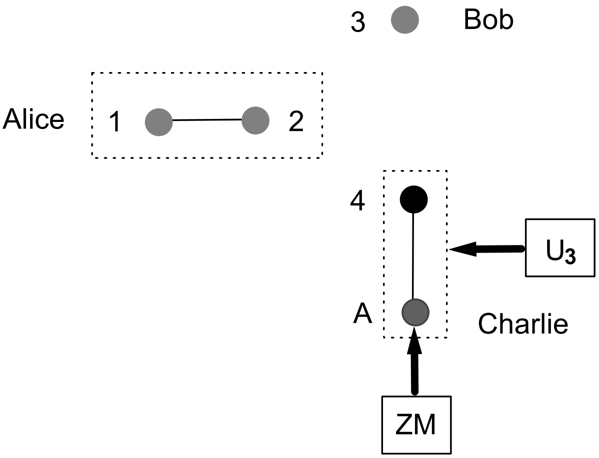


Fig. 2 Bob performs a single-qutrit projective measurement (SM) on qutrit 3 and tells Charlie his result, then Charlie applies a proper unitary operation U_i $(i = 0, 1, 2)$ on qutrit 4. See step (4) for details

Fig. 3 Charlie introduces an auxiliary qutrit A and first performs a collective unitary operation U_3 on qutrits 4 and A, then he makes a Z-measurement (ZM) on qutrit A to reconstruct the original state. See steps (5)–(6) for details



then the scheme goes to step (5). Note that Bob obtains $|\xi_t\rangle$ $(t = 0, 1, 2)$ with the probability $\rho_2 = 1/3$.

(5) Charlie introduces an auxiliary single-qutrit A in the initial state $|0\rangle_A$ and performs another collective unitary operation U_3 on particles 4 and A (see Fig. 3). Under the basis $\{|00\rangle_{4A}, |10\rangle_{4A}, |20\rangle_{4A}, |01\rangle_{4A}, |11\rangle_{4A}, |21\rangle_{4A}, |02\rangle_{4A}, |12\rangle_{4A}, |22\rangle_{4A}\}$, the collective unitary operation U_3 may take the form as the following 9×9 matrices

$$U_3 = \begin{pmatrix} A_1 & A_2 & 0 \\ A_2 & -A_1 & 0 \\ 0 & 0 & I \end{pmatrix}, \tag{17}$$

where I is the 3×3 identity matrix, A_i $(i = 1, 2)$ is the 3×3 diagonal matrix and may be described as

$$A_1 = \text{diag}\left(\frac{c}{a}, \frac{c}{b}, 1\right), \tag{18}$$

$$A_2 = \mathrm{diag}\left(\sqrt{1-\frac{c^2}{a^2}}, \sqrt{1-\frac{c^2}{b^2}}, 0\right). \tag{19}$$

After Charlie's collective unitary operation U_3, the state of the qutrits 4 and A is transformed into

$$\begin{aligned} &U_3\frac{1}{3}(a\alpha|0\rangle_4 + b\beta|1\rangle_4 + c\gamma|2\rangle_4)|0\rangle_A \\ &\quad = \frac{1}{3}[c(\alpha|0\rangle_4 + \beta|1\rangle_4 + \gamma|2\rangle_4)|0\rangle_A + (\sqrt{a^2-c^2}\alpha|0\rangle_4 + \sqrt{b^2-c^2}\beta|1\rangle_4)|1\rangle_A]. \end{aligned} \tag{20}$$

(6) Charlie measures the qutrit A in the bases $B_z = \{|0\rangle, |1\rangle, |2\rangle\}$. If his measurement result is $|0\rangle_A$, Charlie knows he has already successfully reconstructed the original state $|P\rangle_1$ on his qutrit 4. Otherwise, the scheme is aborted. From (20), after normalization we can calculate the probability of Charlie measures $|0\rangle_A$ is $\rho_3 = |c|^2/[(a\alpha)^2 + (b\beta)^2 + (c\gamma)^2]$. From the above analyses, one can see that the success probability Charlie reconstructs the original state is $\rho_t = \rho_1 \times \rho_2 \times \rho_3 = |c|^2/9$.

Similarly, in *Case 2* or *Case 3* of the step (4), when Bob's measurement result is $|\xi_1\rangle_3$ or $|\xi_2\rangle_3$, Charlie also can recover the initial state $|P\rangle_1$ under Bob's help with the success probability $|c|^2/9$. Hence the success probability Charlie reconstructs the original state is $(|c|^2/9) \times 3 = |c|^2/3$ in the case that Alice's generalized Bell-state measurement result is $|\Psi_{00}\rangle_{12}$. Obviously one can see that the probability of successful sharing the single-qutrit state is only determined by the parameter $|c|$, i.e., the smallest one among $|a|$, $|b|$ and $|c|$.

As mentioned before, there are 9 possible results (see (4)–(12) in the step (2)) when Alice performs generalized Bell-state measurement on her qutrit pair $(1,2)$. We have taken one of them as an example and extensively analyzed it. Now let us make some explanations about the other 8 possible results (cf., Table 1) in brief. When Alice's measurement result is $|\Psi_{10}\rangle_{12}$ ($|\Psi_{20}\rangle_{12}$), Bob first performs the operation $U = \sum_{j=0}^{2} e^{2\pi ij/3}|j\rangle\langle j|$ ($U = \sum_{j=0}^{2} e^{4\pi ij/3}|j\rangle\langle j|$) on his qutrit 3 to change $a\alpha|00\rangle_{34} + e^{-2\pi i/3}b\beta|11\rangle_{34} + e^{-4\pi i/3}c\gamma|22\rangle_{34}$ ($a\alpha|00\rangle_{34} + e^{-4\pi i/3}b\beta|11\rangle_{34} + e^{-8\pi i/3}c\gamma|22\rangle_{34}$) to $a\alpha|00\rangle_{34} + b\beta|11\rangle_{34} + c\gamma|22\rangle_{34}$, then the subsequent is the same to the outcome $|\Psi_{00}\rangle_{12}$. When Alice's measurement result is $|\Psi_{01}\rangle_{12}$ ($|\Psi_{02}\rangle_{12}$), Bob and Charlie first perform the operation $U = |0\rangle\langle 1| + |1\rangle\langle 2| + |2\rangle\langle 0|$ ($U = |0\rangle\langle 2| + |1\rangle\langle 0| + |2\rangle\langle 1|$) on their respective qutrit to turn $b\alpha|11\rangle_{34} + c\beta|22\rangle_{34} + a\gamma|00\rangle_{34}$

Table 1 The first and third columns give Alice's and Bob's respective measurement results, $|G\rangle_4$ is the state of qutrit 4 after Bob's single-qutrit measurement, U_i $(i = 0, 1, 2)$ is Charlie's unitary operation on qutrit 4. For simplicity, we define $\varepsilon = (a\alpha)^2 + (b\beta)^2 + (c\gamma)^2$, $\zeta = (b\alpha)^2 + (c\beta)^2 + (a\gamma)^2$, and $\eta = (c\alpha)^2 + (a\beta)^2 + (b\gamma)^2$. See text for more details

BM	ρ_1	SM	ρ_2	$\|G\rangle_4$	U_i	ρ_3	ρ_t
$\|\Psi_{i0}\rangle_{12}$	$\varepsilon/3$	$\|\xi_0\rangle_3$	$1/3$	$a\alpha\|0\rangle_4 + b\beta\|1\rangle_4 + c\gamma\|2\rangle_4$	U_0	$\|c\|^2/\varepsilon$	$\|c\|^2/9$
$\|\Psi_{i0}\rangle_{12}$	$\varepsilon/3$	$\|\xi_1\rangle_3$	$1/3$	$a\alpha\|0\rangle_4 + e^{-2\pi i/3}b\beta\|1\rangle_4 + e^{-4\pi i/3}c\gamma\|2\rangle_4$	U_1	$\|c\|^2/\varepsilon$	$\|c\|^2/9$
$\|\Psi_{i0}\rangle_{12}$	$\varepsilon/3$	$\|\xi_2\rangle_3$	$1/3$	$a\alpha\|0\rangle_4 + e^{-4\pi i/3}b\beta\|1\rangle_4 + e^{-2\pi i/3}c\gamma\|2\rangle_4$	U_2	$\|c\|^2/\varepsilon$	$\|c\|^2/9$
$\|\Psi_{i1}\rangle_{12}$	$\zeta/3$	$\|\xi_0\rangle_3$	$1/3$	$b\alpha\|0\rangle_4 + c\beta\|1\rangle_4 + a\gamma\|2\rangle_4$	U_0	$\|c\|^2/\zeta$	$\|c\|^2/9$
$\|\Psi_{i1}\rangle_{12}$	$\zeta/3$	$\|\xi_1\rangle_3$	$1/3$	$b\alpha\|0\rangle_4 + e^{-2\pi i/3}c\beta\|1\rangle_4 + e^{-4\pi i/3}a\gamma\|2\rangle_4$	U_1	$\|c\|^2/\zeta$	$\|c\|^2/9$
$\|\Psi_{i1}\rangle_{12}$	$\zeta/3$	$\|\xi_2\rangle_3$	$1/3$	$b\alpha\|0\rangle_4 + e^{-4\pi i/3}c\beta\|1\rangle_4 + e^{-2\pi i/3}a\gamma\|2\rangle_4$	U_2	$\|c\|^2/\zeta$	$\|c\|^2/9$
$\|\Psi_{i2}\rangle_{12}$	$\eta/3$	$\|\xi_0\rangle_3$	$1/3$	$c\alpha\|0\rangle_4 + a\beta\|1\rangle_4 + b\gamma\|2\rangle_4$	U_0	$\|c\|^2/\eta$	$\|c\|^2/9$
$\|\Psi_{i2}\rangle_{12}$	$\eta/3$	$\|\xi_1\rangle_3$	$1/3$	$c\alpha\|0\rangle_4 + e^{-2\pi i/3}a\beta\|1\rangle_4 + e^{-4\pi i/3}b\gamma\|2\rangle_4$	U_1	$\|c\|^2/\eta$	$\|c\|^2/9$
$\|\Psi_{i2}\rangle_{12}$	$\eta/3$	$\|\xi_2\rangle_3$	$1/3$	$c\alpha\|0\rangle_4 + e^{-4\pi i/3}a\beta\|1\rangle_4 + e^{-2\pi i/3}b\gamma\|2\rangle_4$	U_2	$\|c\|^2/\eta$	$\|c\|^2/9$

$(c\alpha|22\rangle_{34}+a\beta|00\rangle_{34}+b\gamma|11\rangle_{34})$ to $b\alpha|00\rangle_{34}+c\beta|11\rangle_{34}+a\gamma|22\rangle_{34}$ $(c\alpha|00\rangle_{34}+a\beta|11\rangle_{34}+b\gamma|22\rangle_{34})$, then the subsequent is similar to the outcome $|\Psi_{00}\rangle_{12}$. From Table 1, one can see clearly that, for Alice's each possible result, the success probability Charlie reconstructs the original state is $(|c|^2/9)\times 3=|c|^2/3$. That is to say, Charlie always can obtain the original state with the probability $|c|^2/3$, no matter what Alice's Bell-state measurement result is. Hence, for our three-party generalized QSTS scheme the total success probability is $(|c|^2/3)\times 9=3|c|^2$. Note that, if the quantum channel consists of a maximally entangled three-qutrit state, that is, the coefficient c is $1/\sqrt{3}$, the total success probability for our scheme is 1. In this case, the present generalized QSTS scheme is reduced to the usual standard QSTS scheme.

So far, we have demonstrated the generalized scheme of three-party sharing an arbitrary unknown single-qutrit state and worked out the success probability. Now we begin to concisely analyze the scheme security against eavesdropping and cheating. In a quantum scheme, all those legal parties should be authenticated in advance. Usually, authentication is taken as separated topic [51]. After authentication, all the legal parties are called as insiders. In contrast, the illegal parties are called as outsiders. In our scheme, we have assumed that the quantum channel among the three insiders is initially in the state described in the (2). This means that the precondition is that the three parties have already securely shared the quantum channel. As for the non-maximally entangled state characterizing the quantum channel, it may originates from the initial maximally entangled state due to decoherence or environment noise during the qutrit storage. In this case, the outsider's eavesdropping can be eliminated for our scheme. As for as the insiders are concerned, although each can pass the authentication to show its legality, she/he may be dishonest. In this case, in our scheme, we should also consider the case of insider's cheating. Fortunately, in our scheme, it is Alice who can assign either her agent Bob or agent Charlie to reconstruct the quantum information. If Bob or Charlie is dishonest and try to cheat the other insider such that he can get the quantum information solely, when Alice publishes some quantum information for comparison check, then the cheating can be revealed. Therefore, in our scheme, the insider's cheating can also be prevented. In short, our scheme is secure against eavesdropping and cheating.

Now let us generalize the three-party single-qutrit-state sharing scheme to the more-party case. Suppose there are $N+1$ legitimate parties. Alice is the quantum information sender. By the way, the quantum information is still given by (1). The other N parties are Alice's agents, named as Bob (1st agent), Charlie (2nd agent), ..., Zach (Nth agent), respectively. All the legitimate parties have successfully shared a non-maximally entangled $(N+1)-$qutrit state in prior

$$|\psi'\rangle_{23\ldots(N+2)}=a|00\ldots0\rangle_{23\ldots(N+2)}+b|11\ldots1\rangle_{23\ldots(N+2)}+c|22\ldots2\rangle_{23\ldots(N+2)}, \tag{21}$$

where a, b and c are defined as above. Qutrit 1 and 2 belong to Alice, and qutrits $3,4,\ldots,$ $(N+2)$ to Bob, Charlie, ..., Zach, respectively. The combined state of $(N+2)$ particles is

$$|\Phi'\rangle_{123\ldots(N+2)}=|P\rangle_1\otimes|\psi'\rangle_{23\ldots(N+2)}. \tag{22}$$

Similarly, in order to split her quantum information into N parts for her N agents, Alice first performs a generalized Bell-state measurement on her qutrit pair $(1,2)$. After her measurement, the system's state evolves to one of the following nine possible results:

$$|\Psi_{00}\rangle_{12}\langle\Psi_{00}|\Phi'\rangle = \frac{1}{\sqrt{3}}|\Psi_{00}\rangle_{12}(a\alpha|00\ldots0\rangle_{34\ldots(N+2)} + b\beta|11\ldots1\rangle_{34\ldots(N+2)} + c\gamma|22\ldots2\rangle_{34\ldots(N+2)}), \tag{23}$$

$$|\Psi_{01}\rangle_{12}\langle\Psi_{01}|\Phi'\rangle = \frac{1}{\sqrt{3}}|\Psi_{01}\rangle_{12}(b\alpha|11\ldots1\rangle_{34\ldots(N+2)} + c\beta|22\ldots2\rangle_{34\ldots(N+2)} + a\gamma|00\ldots0\rangle_{34\ldots(N+2)}), \tag{24}$$

$$|\Psi_{02}\rangle_{12}\langle\Psi_{02}|\Phi'\rangle = \frac{1}{\sqrt{3}}|\Psi_{02}\rangle_{12}(c\alpha|22\ldots2\rangle_{34\ldots(N+2)} + a\beta|00\ldots0\rangle_{34\ldots(N+2)} + b\gamma|11\ldots1\rangle_{34\ldots(N+2)}), \tag{25}$$

$$|\Psi_{10}\rangle_{12}\langle\Psi_{10}|\Phi'\rangle = \frac{1}{\sqrt{3}}|\Psi_{10}\rangle_{12}(a\alpha|00\ldots0\rangle_{34\ldots(N+2)} + e^{-2\pi i/3}b\beta|11\ldots1\rangle_{34\ldots(N+2)} + e^{-4\pi i/3}c\gamma|22\ldots2\rangle_{34\ldots(N+2)}), \tag{26}$$

$$|\Psi_{11}\rangle_{12}\langle\Psi_{11}|\Phi'\rangle = \frac{1}{\sqrt{3}}|\Psi_{11}\rangle_{12}(b\alpha|11\ldots1\rangle_{34\ldots(N+2)} + e^{-2\pi i/3}c\beta|22\ldots2\rangle_{34\ldots(N+2)} + e^{-4\pi i/3}a\gamma|00\ldots0\rangle_{34\ldots(N+2)}), \tag{27}$$

$$|\Psi_{12}\rangle_{12}\langle\Psi_{12}|\Phi'\rangle = \frac{1}{\sqrt{3}}|\Psi_{12}\rangle_{12}(c\alpha|22\ldots2\rangle_{34\ldots(N+2)} + e^{-2\pi i/3}a\beta|00\ldots0\rangle_{34\ldots(N+2)} + e^{-4\pi i/3}b\gamma|11\ldots1\rangle_{34\ldots(N+2)}), \tag{28}$$

$$|\Psi_{20}\rangle_{12}\langle\Psi_{20}|\Phi'\rangle = \frac{1}{\sqrt{3}}|\Psi_{20}\rangle_{12}(a\alpha|00\ldots0\rangle_{34\ldots(N+2)} + e^{-4\pi i/3}b\beta|11\ldots1\rangle_{34\ldots(N+2)} + e^{-8\pi i/3}c\gamma|22\ldots2\rangle_{34\ldots(N+2)}), \tag{29}$$

$$|\Psi_{21}\rangle_{12}\langle\Psi_{21}|\Phi'\rangle = \frac{1}{\sqrt{3}}|\Psi_{21}\rangle_{12}(b\alpha|11\ldots1\rangle_{34\ldots(N+2)} + e^{-4\pi i/3}c\beta|22\ldots2\rangle_{34\ldots(N+2)} + e^{-8\pi i/3}a\gamma|00\ldots0\rangle_{34\ldots(N+2)}), \tag{30}$$

$$|\Psi_{22}\rangle_{12}\langle\Psi_{22}|\Phi'\rangle = \frac{1}{\sqrt{3}}|\Psi_{22}\rangle_{12}(c\alpha|22\ldots2\rangle_{34\ldots(N+2)} + e^{-4\pi i/3}a\beta|00\ldots0\rangle_{34\ldots(N+2)} + e^{-8\pi i/3}b\gamma|11\ldots1\rangle_{34\ldots(N+2)}). \tag{31}$$

Similar to the three-party case, we only take into account one case as an example hereafter. Without loss of generality, suppose Alice's measurement result is $|\Psi_{00}\rangle_{12}$. In this case, the state of the qutrits $3, 4, \ldots, (N+2)$ collapse to the state

$$|K'\rangle_{34\ldots(N+2)} = \frac{1}{\sqrt{3}}(a\alpha|00\ldots0\rangle_{34\ldots(N+2)} + b\beta|11\ldots1\rangle_{34\ldots(N+2)} + c\gamma|22\ldots2\rangle_{34\ldots(N+2)}). \tag{32}$$

This state can be reexpressed as

$$|K'\rangle_{34\ldots(N+2)} = \frac{1}{\sqrt{3}}(a\alpha|00\ldots0\rangle_{34\ldots(N+2)} + b\beta|11\ldots1\rangle_{34\ldots(N+2)} + c\gamma|22\ldots2\rangle_{34\ldots(N+2)})$$

$$= \left(\frac{1}{\sqrt{3}}\right)^N \sum_{l_1=0}^{2}\sum_{l_2=0}^{2}\cdots\sum_{l_{m-1}=0}^{2}\sum_{l_{m+1}=0}^{2}\cdots\sum_{l_N=0}^{2}[|\xi_{l_1}\rangle_3|\xi_{l_2}\rangle_4\cdots|\xi_{l_{m-1}}\rangle_{m+1} \times (a\alpha|0\rangle_{m+2} + e^{-2\pi iL/3}b\beta|1\rangle_{m+2} + e^{-4\pi iL/3}c\gamma|2\rangle_{m+2})|\xi_{l_{m+1}}\rangle_{m+3}\cdots|\xi_{l_N}\rangle_{N+2}], \quad (33)$$

where

$$L = \sum_{i=1}^{m-1} l_i + \sum_{j=m+1}^{N} l_j. \quad (34)$$

Due to symmetry, Alice can assign any one of the N agents to reconstruct her unknown state. Without loss of generality, we assume Alice assigns the mth agent to reconstruct her original state. Alice publishes the measurement result $|\Psi_{00}\rangle_{12}$ via a classical channel, then she asks the other $N-1$ agents to make a single-qutrit projective measurement on their own qutrit in the orthogonal bases B_s respectively. After these, the qutrit in the mth agent's possession is projected onto $|G'\rangle_{m+2} = a\alpha|0\rangle_{m+2} + e^{-2\pi iL/3}b\beta|1\rangle_{m+2} + e^{-4\pi iL/3}c\gamma|2\rangle_{m+2}$. If all the other agents collaborate with the assigned agent, he/she can turn the state $|G'\rangle_{m+2}$ to $|G\rangle_{m+2}$ by performing the unitary operation $U_4 = \sum_{j=0}^{2} e^{2\pi ijL/3}|j\rangle\langle j|$, where $|G\rangle_{m+2} = a\alpha|0\rangle_{m+2} + b\beta|1\rangle_{m+2} + c\gamma|2\rangle_{m+2}$. Next he/she introduces an auxiliary single-qutrit A in the initial state $|0\rangle_A$ and performs certain appropriate collective unitary operation on particles $(m+2)$ and A. At last, he/she can probabilistically reconstruct the original state by measuring the qutrit A in the bases B_z. Obviously one can see, since the probability is only determined by the small coefficients of generalized GHZ state, the success probability in the multiparty scheme is also $3|c|^2$. The security of the multiparty quantum single-qutrit state sharing scheme is the same as the three-party case, here we do not repeat any more.

To summarize, in this paper we have proposed a QSTS scheme for probabilistically sharing an arbitrary unknown single-qutrit state by taking a non-maximally generalized GHZ state as the quantum channel. The state sender Alice needs to perform a generalized Bell-state measurement on her qutrit pair and then publishes her measurement result through a classical channel. Due to the symmetry, Alice can assign anyone of the agents to recover the original state. After Alice's assignment, the other agents are required to perform single-qutrit projective measurement on their respective qutrit. Then in terms of Alice's classical message, the designed agent can probabilistically reconstruct the original state by performing certain appropriate unitary operations only and only if all the other agents collaborate with him/her. In addition, we have also worked out the success probability of the scheme is $3|c|^2$ and found the probability is only determined by the small one among the absolute values of the coefficients characterizing the quantum channel.

Acknowledgements Supported by the program for New Century Excellent Talents all the University of China under Grant No. NCET-06-0554, the National Natural Science Foundation of China under Grant Nos. 60677001 and 10747146, the science-technology fund of Anhui province for outstanding youth under Grant. No. 06042087, the key fund of the ministry of education of China under Grant No. 206063, the Natural Science Foundation of Guangdong Province under Grant Nos. 06300345 and 7007806, and Natural Science Foundation of Hubel Province under Grant No. 2006ABA354.

References

1. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press, Cambridge (2000)

2. Long, G.L., Xiao, L.: Phys. Rev. A **69**, 052303 (2004)
3. Bennett, C.H., Brassard, G., Crpeau, C., Jozsa, R., Peres, A., Wootters, W.K.: Phys. Rev. Lett. **70**, 1895 (1993)
4. Bouwmeester, D., Pan, J.W., Mattle, K., Eibl, M., Weinfurter, H., Zeilinger, A.: Nature **390**, 575 (1997)
5. Bennett, C.H., Wiesner, S.J.: Phys. Rev. Lett. **69**, 2881 (1992)
6. Bennett, C.H., Brassard, G.: In: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India. IEEE, New York (1984), pp. 175–179
7. Gisin, N., Ribordy, G., Tittel, W., Zbinden, H.: Rev. Mod. Phys. **74**, 145 (2002)
8. Cabello, A.: Phys. Rev. Lett. **85**, 5635 (2000)
9. Xue, P., Li, C.F., Guo, G.C.: Phys. Rev. A **65**, 022317 (2002)
10. Ekert, A.K.: Phys. Rev. Lett. **67**, 661 (1991)
11. Bennett, C.H., Brassard, G., Mermin, N.D.: Phys. Rev. Lett. **68**, 557 (1992)
12. Deng, F.G., Long, G.L.: Phys. Rev. A **68**, 042315 (2003)
13. Deng, F.G., Long, G.L.: Phys. Rev. A **70**, 012311 (2004)
14. Lo, H.K., Chau, H.F., Ardehali, M.: J. Cryptol. **18**, 133 (2005)
15. Deng, F.G., Long, G.L., Liu, X.S.: Phys. Rev. A **68**, 042317 (2003)
16. Deng, F.G., Long, G.L.: Phys. Rev. A **69**, 052319 (2004)
17. Wang, C., et al.: Phys. Rev. A **71**, 044305 (2005)
18. Hillery, M., Buzek, V., Berthiaume, A.: Phys. Rev. A **59**, 1829 (1999)
19. Karlsson, A., Koashi, M., Imoto, N.: Phys. Rev. A **59**, 162 (1999)
20. Gottesman, D.: Phys. Rev. A **61**, 042311 (2000)
21. Tittel, W., Zbinden, H., Gisin, N.: Phys. Rev. A **63**, 042301 (2001)
22. Karimipour, V., Bahraminasab, A., Bagherinezhad, S.: Phys. Rev. A **65**, 042320 (2002)
23. Chau, H.F.: Phys. Rev. A **66**, 060302 (2002)
24. Bagherinezhad, S., Karimipour, V.: Phys. Rev. A **67**, 044302 (2003)
25. Guo, G.P., Guo, G.C.: Phys. Lett. A **310**, 247 (2003)
26. Xiao, L., Long, G.L., Deng, F.G., Pan, J.W.: Phys. Rev. A **69**, 052307 (2004)
27. Singh, S.K.: Phys. Rev. A **71**, 012328 (2005)
28. Hsu, L.Y., Li, C.M.: Phys. Rev. A **71**, 022321 (2005)
29. Zhang, Z.J., et al.: Phys. Lett. A **342**, 60 (2005)
30. Zhang, Z.J., et al.: Phys. Lett. A **361**, 24 (2007)
31. Zhang, Z.J., et al.: Phys. Rev. A **71**, 044301 (2005)
32. Zhang, Z.J., et al.: Phys. Rev. A **72**, 022303 (2005)
33. Zhang, Z.J., et al.: Chin. Phys. Lett. **22**, 1588 (2005)
34. Zhang, Z.J., et al.: Opt. Commun. **269**, 418 (2007)
35. Cleve, R., Gottesman, D., Lo, H.K.: Phys. Rev. Lett. **83**, 648 (1999)
36. Bandyopadhyay, S.: Phys. Rev. A **62**, 012308 (2000)
37. Hsu, L.Y.: Phys. Rev. A **68**, 022306 (2003)
38. Li, Y.M., Zhang, K.S., Peng, K.C.: Phys. Lett. A **324**, 420 (2004)
39. Lance, A.M., Symul, T., Bowen, W.P., Sanders, B.C., Lam, P.K.: Phys. Rev. Lett. **92**, 177903 (2004)
40. Deng, F.G., et al.: Phys. Lett. A **337**, 329 (2005)
41. Deng, F.G., Li, X.H., Zhou, H.Y., Zhang, Z.J.: Phys. Rev. A **72**, 044302 (2005)
42. Zhang, Z.J.: Opt. Commun. **261**, 199 (2006)
43. Zhang, Z.J., et al.: Eur. Phys. J. D **33**, 133 (2005)
44. Lance, A.M., et al.: Phys. Rev. A **71**, 033814 (2005)
45. Deng, F.G., et al.: Phys. Rev. A **72**, 044301 (2005)
46. Deng, F.G., Li, X.H., Li, C.Y., Zhou, P., Zhou, H.Y.: e-print quant-ph/ 0509029
47. Li, X.H., et al.: J. Phys. B **39**, 1975 (2006)
48. Wang, Z.Y., Yuan, H., Shi, S.H., Zhang, Z.J.: Eur. Phys. J. D, **41**, 371 (2007)
49. Gordon, G., Rigolin, G.: Phys. Rev. A **73**, 062316 (2006)
50. Wang, Z.Y., Liu, Y.M., Wang, D., Zhang, Z.J.: Opt. Commun. **276**, 322 (2007)
51. Zeng, G., Zhang, W.: Phys. Rev. A **61**, 022303 (2000)