Article

Chinese Science Bulletin

Quantum Information

April 2012 Vol.57 No.10: 1089–1094
doi: 10.1007/s11434-012-5008-3

An efficient scheme for multi-party quantum state sharing via non-maximally entangled states

JIANG Min[1*], HUANG Xu[1], ZHOU LiuLei[1], ZHOU YiMing[2] & ZENG Jia[3]

[1] *School of Electronics & Information Engineering, Soochow University, Suzhou 215006, China;*
[2] *Beijing Institute of Space Science and Technology Information, Beijing 100086, China;*
[3] *The 208th Institute of the Second Research Academy, CASIC, Beijing 100854, China*

Received November 22, 2011; accepted December 30, 2011

We present a new scheme for investigating the usefulness of non-maximally entangled states for multi-party quantum state sharing in a simple and elegant manner. In our scheme, the sender, Alice shares n various probabilistic channels composed of non-maximally entangled states with n agents in a network. Our protocol involves only Bell-basis measurements, single qubit measurements, and a two-qubit unitary transformation operated by free optional agents. Our scheme is a more convenient realization because no other multipartite joint measurements are needed. Furthermore, in our scheme various probabilistic channels lessen the requirement for quantum channels, which makes it more practical for physical implementation.

quantum state sharing, probabilistic channel, multi-particle state, two-particle entangled state

Citation: Jiang M, Huang X, Zhou L L, et al. An efficient scheme for multi-party quantum state sharing via non-maximally entangled states. Chin Sci Bull, 2012, 57: 1089–1094, doi: 10.1007/s11434-012-5008-3

Quantum secret sharing (QSS) is a method for creating a private key and dividing it between parties. It has potential applications ranging from quantum secure communication, quantum key distribution, and joint sharing of quantum money [1–6]. This research area covers classical secret sharing and quantum information sharing among multiple participants. The latter case was named "quantum state sharing" (QSTS) by Lance et al. [7]. The basic idea of QSTS in the multi-party case is that some information in a secret quantum state of a multi-qubit possessed by one person is distributed between that person, whom we call "Alice", and multiple remote recipients. This is done in such a way that it can be jointly reconstructed and shared only if all participants collaborate. In some sense, QSTS is equivalent to quantum-controlled teleportation. However, during the process of quantum teleportation, an unknown quantum state is transferred to a distant location without revealing any information about the state in the course of the transformation. For a general QSTS protocol, that information is not so restricted. The shared quantum states can be known or unknown in advance to the initial holder. In most QSTS protocols [8–19], entanglement is the main phenomenon used to share quantum information. So far, various entangled states have been extensively used in QSTS protocols, such as Bell states [7–11], GHZ states [12–15], W states [16,17], cluster states [18–20], and Brown states [21–23]. Recently, Gao et al. [24] presented a scheme for quantum state sharing between a multi-party and a multi-party with three conjugate bases. In recent techniques, Einstein-Podolsky-Rosen (EPR) pairs are ideally entangled resources for quantum state sharing [13,14]. For example, Wang et al. [15] and Shi et al. [11,25,26] have presented several multi-party QSTS schemes for sharing an arbitrary two-qubit state using Bell states as quantum resources. Very recently, several asymmetric schemes for five-party and multi-party quantum state sharing with maximally entangled states of two particles and three particles have been proposed [27–30].

When applied to a real communication scenario, due to

*Corresponding author (email: jiangmin03@gmail.com)

inevitable environmental effects, any initially maximally entangled states may easily evolve into non-maximally entangled states or mixed states. There have been some results related to the probabilistic teleportation of two-particle and multi-particle states [31–37] with non-maximally entangled states as the teleportation channels. A similar circumstance occurs for quantum state sharing in a network. To implement state sharing via probabilistic channels, it is often necessary to perform a high-dimensional operation, which is difficult to implement using current quantum information processing technology. It is not realistic that each terminal node in the quantum network be equipped with powerful information processing capabilities and precious auxiliary qubit resources [38,39]. Such potential obstacles stimulated the search for alternative schemes which would eliminate the need for high-dimensional operations. In this paper, we developed a systematic approach that used only two qubit gates to address the above problems.

1 Multi-party quantum state sharing of one qubit state in a multi-qubit system via probabilistic channels

Without loss of generality, we assume that the unknown state to be teleported in Alice's position can be expressed in the following form:

$$|\varphi\rangle_{T_1T_2\cdots T_n}=\left(\sum\alpha_{\{i\}}|\{i\}\rangle_{T_1T_2\cdots T_{n-1}}\right)|0\rangle_{T_n}+\left(\sum\beta_{\{i\}}|\{i\}\rangle_{T_1T_2\cdots T_{n-1}}\right)|1\rangle_{T_n}. \quad (1)$$

To share the above state, Alice first prepares n non-maximally entangled states as the quantum channel with n agents in a network:

$$|\phi\rangle_{A_iB_i}=\left(a_i|00\rangle_{A_iB_i}+b_i|11\rangle_{A_iB_i}\right), \quad (2)$$

where A_i and B_i are the two particles in the state $|\phi\rangle_{A_iB_i}$, and a_i and b_i are complex numbers that satisfy the normalized condition:

$$|a_i|^2+|b_i|^2=1\left(|a_i|<|b_i|\right). \quad (3)$$

Each agent Bob$_i$ (i=1, 2,…n) possesses one particle A_i (i=1, 2,…n) and Alice possesses particles B_i (i=1, 2,…n) as shown in Figure 1. The state of the whole system can be described, without being normalized, as

$$|\varphi\rangle_{T_1T_2\cdots T_nA_1B_1A_2B_2\cdots A_nB_n}=\left(\left(\sum\alpha_{\{i\}}|\{i\}\rangle_{T_1T_2\cdots T_{n-1}}\right)|0\rangle_{T_n}+\left(\sum\beta_{\{i\}}|\{i\}\rangle_{T_1T_2\cdots T_{n-1}}\right)|1\rangle_{T_n}\right)\otimes\prod_{i=1}^{n}\left(a_i|00\rangle_{A_iB_i}+b_i|11\rangle_{A_iB_i}\right), \quad (4)$$

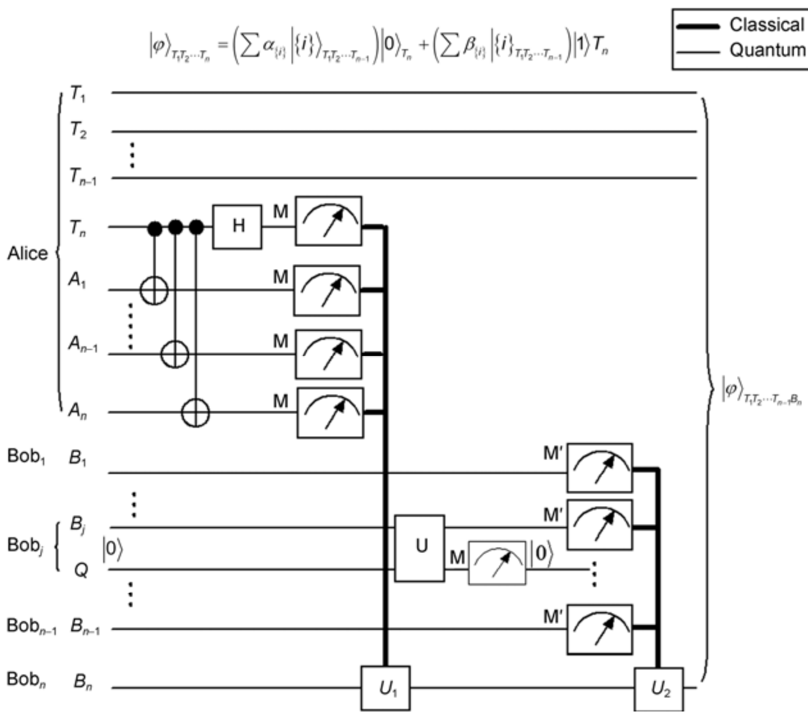

Figure 1 The principle of multi-party QSTS of an arbitrary one-qubit state in a multi-qubit system. M(M′) denotes the single-particle measurement based on $\{|0\rangle,|1\rangle\}$($\{|+x\rangle,|-x\rangle\}$).

which can be rewritten in the following form:

$$\begin{aligned}&|\varphi\rangle_{T_1T_2\cdots T_n A_1B_1A_2B_2\cdots A_nB_n}=\left(\sum\alpha_{\{i\}}|\{i\}\rangle_{T_1T_2\cdots T_{n-1}}\right)\\&\otimes\left(\sum_{k_n=a_n}^{b_n}k_1k_2\cdots k_n|1\{x_1\}\{x_2\}\cdots\{x_n\}\rangle_{T_nA_1B_1A_2B_2\cdots A_nB_n}\right)\\&+\left(\sum\beta_{\{i\}}|\{i\}\rangle_{T_1T_2\cdots T_{n-1}}\right)\\&\otimes\left(\sum_{k_1=a_1}^{b_1}\sum_{k_2=a_2}^{b_2}\cdots\sum_{k_n=a_n}^{b_n}k_1k_2\cdots k_n|1\{x_1\}\{x_2\}\cdots\{x_n\}\rangle_{T_nA_1B_1A_2B_2\cdots A_nB_n}\right),\end{aligned}\tag{5}$$

where if k_i=a_i, then $\{x_i\}$ represents sequence "00". Otherwise, k_i=b_i, and $\{x_i\}$ represents sequence "11".

Then, Alice can transfer her unknown state to the qubits controlled by all the agents. To be precise, Alice should send particles T_n and A_i (i=1, 2,…n) through CNOT gates, where particle T_n is the control particle and particle A_i is the target particle. The state of the whole system can be described as (without being normalized)

$$\begin{aligned}&|\varphi\rangle_{T_1T_2\cdots T_n A_1B_1A_2B_2\cdots A_nB_n}=\left(\sum\alpha_{\{i\}}|\{i\}\rangle_{T_1T_2\cdots T_{n-1}}\right)\\&\otimes\left(\sum_{k_1=a_1}^{b_1}\sum_{k_2=a_2}^{b_2}\cdots\sum_{k_n=a_n}^{b_n}k_1k_2\cdots k_n|0\{x_1\}\{x_2\}\cdots\{x_n\}\rangle_{T_nA_1B_1A_2B_2\cdots A_nB_n}\right)\\&+\left(\sum\beta_{\{i\}}|\{i\}\rangle_{T_1T_2\cdots T_{n-1}}\right)\\&\otimes\left(\sum_{k_1=a_1}^{b_1}\sum_{k_2=a_2}^{b_2}\cdots\sum_{k_n=a_n}^{b_n}k_1k_2\cdots k_n|1\{x'_1\}\{x'_2\}\cdots\{x'_n\}\rangle_{T_nA_1B_1A_2B_2\cdots A_nB_n}\right).\end{aligned}\tag{5}$$

Subsequently, Alice first performs a Hadamard transformation onto particle T_n. Hence, the state of the whole system can be represented as (without being normalized)

$$\begin{aligned}&|\varphi\rangle_{T_1T_2\cdots T_n A_1B_1A_2B_2\cdots A_nB_n}=\left(\sum\alpha_{\{i\}}|\{i\}\rangle_{T_1T_2\cdots T_{n-1}}\right)\\&\otimes\left(\sum_{k_1=a_1}^{b_1}\sum_{k_2=a_2}^{b_2}\cdots\sum_{k_n=a_n}^{b_n}k_1k_2\cdots k_n|0\{x_1\}\{x_2\}\cdots\{x_n\}\rangle_{T_nA_1B_1A_2B_2\cdots A_nB_n}\right)\\&+\left(\sum\alpha_{\{i\}}|\{i\}\rangle_{T_1T_2\cdots T_{n-1}}\right)\\&\otimes\left(\sum_{k_1=a_1}^{b_1}\sum_{k_2=a_2}^{b_2}\cdots\sum_{k_n=a_n}^{b_n}k_1k_2\cdots k_n|1\{x_1\}\{x_2\}\cdots\{x_n\}\rangle_{T_nA_1B_1A_2B_2\cdots A_nB_n}\right)\\&+\left(\sum\beta_{\{i\}}|\{i\}\rangle_{T_1T_2\cdots T_{n-1}}\right)\\&\otimes\left(\sum_{k_1=a_1}^{b_1}\sum_{k_2=a_2}^{b_2}\cdots\sum_{k_n=a_n}^{b_n}k_1k_2\cdots k_n|0\{x'_1\}\{x'_2\}\cdots\{x'_n\}\rangle_{T_nA_1B_1A_2B_2\cdots A_nB_n}\right)\\&-\left(\sum\beta_{\{i\}}|\{i\}\rangle_{T_1T_2\cdots T_{n-1}}\right)\\&\otimes\left(\sum_{k_1=a_1}^{b_1}\sum_{k_2=a_2}^{b_2}\cdots\sum_{k_n=a_n}^{b_n}k_1k_2\cdots k_n|1\{x'_1\}\{x'_2\}\cdots\{x'_n\}\rangle_{T_nA_1B_1A_2B_2\cdots A_nB_n}\right).\end{aligned}\tag{6}$$

The first term remains the same as it was in eq. (5). In the second term,

$$\begin{aligned}&\left(\sum\beta_{\{i\}}|\{i\}\rangle_{T_1T_2\cdots T_{n-1}}\right)\\&\otimes\left(\sum_{k_1=a_1}^{b_1}\sum_{k_2=a_2}^{b_2}\cdots\sum_{k_n=a_n}^{b_n}k_1k_2\cdots k_n|1\{x'_1\}\{x'_2\}\cdots\{x'_n\}\rangle_{T_nA_1B_1A_2B_2\cdots A_nB_n}\right),\end{aligned}$$

if k_i=a_i, then $\{x'_i\}$ represents "10". Otherwise, k_i=b_i, and $\{x_i\}$ represents "01". Thus, it can be regrouped in the following form:

$$\begin{aligned}&|\varphi\rangle_{T_1T_2\cdots T_n A_1B_1A_2B_2\cdots A_nB_n}\\&=|0\rangle_{T_n}\left(\sum_{p_1,p_2,\cdots p_n=0}^{p_1,p_2,\cdots p_n=1}|p_1p_2\cdots p_n\rangle_{A_1A_2\cdots A_n}\right.\\&\quad\otimes\left(k_{p_1}k_{p_2}\cdots k_{p_n}\left(\sum\alpha_{\{i\}}|\{i\}\rangle_{T_1T_2\cdots T_{n-1}}\right)\otimes|p_1p_2\cdots p_n\rangle_{B_1B_2\cdots B_n}\right.\\&\quad\left.\left.+\left(\bar{k}_{p_1}\bar{k}_{p_2}\cdots\bar{k}_{p_n}\left(\sum\beta_{\{i\}}|\{i\}\rangle_{T_1T_2\cdots T_{n-1}}\right)|\bar{p}_1\bar{p}_2\cdots\bar{p}_n\rangle_{B_1B_2\cdots B_n}\right)\right)\right)\\&\quad+|1\rangle_{T_n}\left(\sum_{p_1,p_2,\cdots p_n=0}^{p_1,p_2,\cdots p_n=1}|p_1p_2\cdots p_n\rangle_{A_1A_2\cdots A_n}\right.\\&\quad\otimes\left(k_{p_1}k_{p_2}\cdots k_{p_n}\left(\sum\alpha_{\{i\}}|\{i\}\rangle_{T_1T_2\cdots T_{n-1}}\right)\otimes\left(|p_1p_2\cdots p_n\rangle_{B_1B_2\cdots B_n}\right.\right.\\&\quad\left.\left.\left.-\left(\bar{k}_{p_1}\bar{k}_{p_2}\cdots\bar{k}_{p_n}\left(\sum\beta_{\{i\}}|\{i\}\rangle_{T_1T_2\cdots T_{n-1}}\right)|\bar{p}_1\bar{p}_2\cdots\bar{p}_n\rangle_{B_1B_2\cdots B_n}\right)\right)\right)\right),\end{aligned}\tag{7}$$

where if p_i=0, then $k_{p_i}=a_i$, $\bar{k}_{p_i}=b_i$. Otherwise $k_{p_i}=b_i$, $\bar{k}_{p_i}=a_i$.

Next, Alice performs a single-particle measurement M on her particles T_n and A_i (i=1, 2,…n) with the basis $\{|0\rangle,|1\rangle\}$. If the outcome obtained by Alice is $|0p_1p_2\cdots p_n\rangle_{T_nA_1A_2\cdots A_n}$ or $|1p_1p_2\cdots p_n\rangle_{T_nA_1A_2\cdots A_n}$, the collapsed state of the subsystem composed of the retained particles T_n and B_i (i=1, 2,…n) can be written as (without being normalized)

$$\begin{aligned}&|\varphi\rangle_{T_1T_2\cdots T_{n-1}B_1B_2\cdots B_n}\\&=k_{p_1}k_{p_2}\cdots k_{p_n}\left(\sum\alpha_{\{i\}}|\{i\}\rangle_{T_1T_2\cdots T_{n-1}}\right)|p_1p_2\cdots p_n\rangle_{B_1B_2\cdots B_n}\\&\quad+\bar{k}_{p_1}\bar{k}_{p_2}\cdots\bar{k}_{p_n}\left(\sum\beta_{\{i\}}|\{i\}\rangle_{T_1T_2\cdots T_{n-1}}\right)|\bar{p}_1\bar{p}_2\cdots\bar{p}_n\rangle_{B_1B_2\cdots B_n},\end{aligned}\tag{8}$$

or

$$\begin{aligned}&|\varphi\rangle_{T_1T_2\cdots T_{n-1}B_1B_2\cdots B_n}\\&=k_{p_1}k_{p_2}\cdots k_{p_n}\left(\sum\alpha_{\{i\}}|\{i\}\rangle_{T_1T_2\cdots T_{n-1}}\right)|p_1p_2\cdots p_n\rangle_{B_1B_2\cdots B_n}\\&\quad-\bar{k}_{p_1}\bar{k}_{p_2}\cdots\bar{k}_{p_n}\left(\sum\beta_{\{i\}}|\{i\}\rangle_{T_1T_2\cdots T_{n-1}}\right)|\bar{p}_1\bar{p}_2\cdots\bar{p}_n\rangle_{B_1B_2\cdots B_n}.\end{aligned}\tag{9}$$

Depending on the measurement outcome of Alice,

$\left|0p_1p_2\cdots p_n\right\rangle_{T_nA_1A_2\cdots A_n}$ or $\left|1p_1p_2\cdots p_n\right\rangle_{T_nA_1A_2\cdots A_n}$, Bob$_n$ performs the following unitary operation:

$$U_1 = U_{p_1}^{B_1}\otimes U_{p_2}^{B_2}\cdots\otimes U_{p_2}^{B_{n-1}}\otimes U_{p_n}^{B_n}, \qquad (10)$$

or

$$U_1 = U_{p_1}^{B_1}\otimes U_{p_2}^{B_2}\cdots\otimes U_{p_{n-1}}^{B_{n-1}}\otimes\left(Z_{p_n}^{B_n}\otimes U_{p_n}^{B_n}\right), \qquad (11)$$

where $Z_{p_i}^{B_i}\ (i=1,2,\cdots n)$ represents a phase-flip operation $\sigma_z = \left|0\right\rangle\left\langle 0\right| - \left|1\right\rangle\left\langle 1\right|$. If p_k=1 (k=1, 2…n), then $U_{p_k}^{B_k}$ is a NOT operation and $\sigma_x = \left|0\right\rangle\left\langle 1\right| + \left|1\right\rangle\left\langle 0\right|$. Otherwise, if p_k=0 (k=1, 2…n), $U_{p_k}^{B_k}$ represents an identity gate. Therefore the collapsed state of the subsystem composed of the retaining particles can be written as (without being normalized)

$$\begin{aligned}&\left|\varphi\right\rangle_{T_1T_2\cdots T_{n-1}B_1B_2\cdots B_n}\\ &= k_{p_1}k_{p_2}\cdots k_{p_n}\left(\sum\alpha_{\{i\}}\left|\{i\}\right\rangle_{T_1T_2\cdots T_{n-1}}\right)\left|00\cdots 0\right\rangle_{B_1B_2\cdots B_n}\\ &\quad+\bar{k}_{p_1}\bar{k}_{p_2}\cdots\bar{k}_{p_n}\left(\sum\beta_{\{i\}}\left|\{i\}\right\rangle_{T_1T_2\cdots T_{n-1}}\right)\left|11\cdots 1\right\rangle_{B_1B_2\cdots B_n}.\end{aligned} \qquad (12)$$

From eq. (13) we can see that the quantum information of the unknown state $\left|\varphi\right\rangle_{T_1T_2\cdots T_n}$ has been transferred into the subsystem composed of the n particles B_i (i=1, 2,…n) which are privately kept by Bob$_i$ (i=1, 2,…n), and they can cooperate to extract the original information with a certain probability.

Then, if some agent Bob$_j$ wishes to initiate the two-qubit unitary operation, he must introduce an auxiliary two-state particle Q with its initial state $\left|0\right\rangle_Q$ and make another unitary transformation U on particles B_j and Q under the basis { $\left|00\right\rangle_{B_jQ}$, $\left|01\right\rangle_{B_jQ}$, $\left|10\right\rangle_{B_jQ}$, $\left|11\right\rangle_{B_jQ}$ }. If $\left|k_{p_1}k_{p_2}\cdots k_{p_n}\right| < \left|\bar{k}_{p_1}\bar{k}_{p_2}\cdots\bar{k}_{p_n}\right|$, the unitary operation U may take the following 4×4 matrix:

$$U=\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&\dfrac{k_{p_1}k_{p_2}\cdots k_{p_n}}{\bar{k}_{p_1}\bar{k}_{p_2}\cdots\bar{k}_{p_n}}&\sqrt{1-\dfrac{\left(k_{p_1}k_{p_2}\cdots k_{p_n}\right)^2}{\left(\bar{k}_{p_1}\bar{k}_{p_2}\cdots\bar{k}_{p_n}\right)^2}}\\0&0&-\sqrt{1-\dfrac{\left(k_{p_1}k_{p_2}\cdots k_{p_n}\right)^2}{\left(\bar{k}_{p_1}\bar{k}_{p_2}\cdots\bar{k}_{p_n}\right)^2}}&\dfrac{k_{p_1}k_{p_2}\cdots k_{p_n}}{\bar{k}_{p_1}\bar{k}_{p_2}\cdots\bar{k}_{p_n}}\end{bmatrix}, \qquad (13)$$

under which the state of the collapsed system becomes

$$\begin{aligned}&U\otimes\left|\varphi\right\rangle_{T_1T_2\cdots T_{n-1}B_1B_2\cdots B_nQ}\\ &= k_{p_1}k_{p_2}\cdots k_{p_n}\left(\left(\left(\sum\alpha_{\{i\}}\left|\{i\}\right\rangle_{P_1P_2\cdots P_{n-1}}\right)\left|00\cdots 0\right\rangle_{B_1B_2\cdots B_n}\right.\right.\\ &\quad\left.\left.+\left(\sum\beta_{\{i\}}\left|\{i\}\right\rangle_{P_1P_2\cdots P_{n-1}}\right)\left|11\cdots 1\right\rangle_{B_1B_2\cdots B_n}\right)\left|0\right\rangle_Q\right)\\ &\quad+\sqrt{\left(\bar{k}_{p_1}\bar{k}_{p_2}\cdots\bar{k}_{p_n}\right)^2-\left(k_{p_1}k_{p_2}\cdots k_{p_n}\right)^2}\\ &\quad\times\left(\sum\beta_{\{i\}}\left|\{i\}\right\rangle_{P_1P_2\cdots P_{n-1}}\right)\left|00\cdots 0\right\rangle_{B_1B_2\cdots B_n}\left|1\right\rangle_Q.\end{aligned} \qquad (14)$$

Subsequently, Bob$_j$ measures the state of auxiliary particle Q under the basis { $\left|0\right\rangle,\left|1\right\rangle$ }. If the measurement result is $\left|0\right\rangle_Q$, the resulting state will be of the following form:

$$\begin{aligned}\left|\varphi\right\rangle_{T_1T_2\cdots T_{n-1}B_1B_2\cdots B_n} &= \left(\sum\alpha_{\{i\}}\left|\{i\}\right\rangle_{T_1T_2\cdots T_{n-1}}\right)\left|00\cdots 0\right\rangle_{B_1B_2\cdots B_n}\\ &\quad+\left(\sum\beta_{\{i\}}\left|\{i\}\right\rangle_{T_1T_2\cdots T_{n-1}}\right)\left|11\cdots 1\right\rangle_{B_1B_2\cdots B_n}.\end{aligned} \qquad (15)$$

Finally, if all Bob$_i$ agree to help Bob$_n$ obtain the original state, each Bob$_i$ (i=1, 2,…n−1) must perform a single particle measurement on his particle B_i with the basis $(\{1/\sqrt{2}(\left|0\right\rangle+\left|1\right\rangle), 1/\sqrt{2}(\left|0\right\rangle-\left|1\right\rangle)\})$. They then must inform Bob$_n$ of the measurement outcomes via the classical channel. Bob$_n$ can recover the original unknown state $\left|\varphi\right\rangle_{T_1T_2\cdots T_n}$ by applying a local unitary operation U_2 on his particle B_n according to the measurement results of Alice and all Bob$_i$. That is, if the number of $\left|-x\right\rangle$ in all of Bob$_i$'s measurement outcomes are odd (even), Bob$_n$ should perform the $\sigma_z(\sigma_x)$ gate onto his particle B_n. The final state composed of particle T_i (i=1, 2,…n−1) and B_n is

$$\begin{aligned}&\left|\varphi\right\rangle_{T_1T_2\cdots T_{n-1}B_n}\\ &=\left(\sum\alpha_{\{i\}}\left|\{i\}\right\rangle_{T_1T_2\cdots T_{n-1}}\right)\left|0\right\rangle_{B_n}+\left(\sum\beta_{\{i\}}\left|\{i\}\right\rangle_{T_1T_2\cdots T_{n-1}}\right)\left|1\right\rangle_{B_n}.\end{aligned} \qquad (16)$$

According to eqs. (1) and (17), the particle T_n held by the receiver Bob$_n$ dominates the same position as the particle held by the sender which means that now Alice and Bob$_n$ jointly share the original initial state $\left|\varphi\right\rangle_{T_1T_2\cdots T_n}$.

As a consequence, the unknown quantum state of multiple particles can be shared one by one with a certain probability of accuracy when the non-maximally entangled channels are set between involved agents.

The probability to obtain the state (13) is

$$g_1 = \left|\sum\left|\alpha_{\{i\}}\right|^2\prod_{i=1}^{n}k_i\right|^2+\left|\sum\left|\beta_{\{i\}}\right|^2\prod_{i=1}^{n}\bar{k}_i\right|^2. \qquad (17)$$

The total probability then can be calculated as

$$g=\sum_{\{p_1,p_2,\dots p_n=0\}}^{\{p_1,p_2,\dots p_n=1\}}\min\left(\left|\sum\left|\alpha_{\{i\}}\right|^2\prod_{i=1}^{n}k_i\right|^2+\left|\sum\left|\beta_{\{i\}}\right|^2\prod_{i=1}^{n}\bar{k}_i\right|^2\cdot\frac{2\left|\sum\left|\alpha_{\{i\}}\right|^2\prod_{i=1}^{n}k_i\right|,2\left|\sum\left|\beta_{\{i\}}\right|^2\prod_{i=1}^{n}\bar{k}_i\right|^2}{\left|\sum\left|\alpha_{\{i\}}\right|^2\prod_{i=1}^{n}k_i\right|^2+\left|\sum\left|\beta_{\{i\}}\right|^2\prod_{i=1}^{n}\bar{k}_i\right|^2}\right)\geqslant 2^n\prod_{i=1}^{2^n}\left|\alpha_i\right|^2. \tag{18}$$

In fact, if all $|a_i|=|b_i|=1/\sqrt{2}$, the success probability approaches 1 and the auxiliary particle is not needed, which is consistent with the existing scheme [25]. This analysis is consistent with the scheme proposed in [25] where the sender Alice first shares n EPR pairs in Bell states with n agents to implement multi-party quantum state sharing of an arbitrary two-qubit state. Our scheme can further analyze and interpret the correctness of their scheme. In their work [25], an arbitrary two-qubit state composed of particle x and y is written as

$$|\phi\rangle_{xy}=\left(a|00\rangle+b|01\rangle+c|10\rangle+d|11\rangle\right)_{xy}. \tag{19}$$

It can be rewritten as the following two forms:

$$|\phi\rangle_{xy}=\left(a|0\rangle+c|1\rangle\right)_x|0\rangle_y+\left(b|0\rangle+d|1\rangle\right)_x|1\rangle_y, \tag{20}$$

or

$$|\phi\rangle_{xy}=\left(a|0\rangle+b|1\rangle\right)_y|0\rangle_x+\left(c|0\rangle+d|1\rangle\right)_y|1\rangle_x. \tag{21}$$

In this way, one Bell pair can implement the state transfer of particle $x(y)$ between the sender and some designated receiver. The remaining Bell pairs play the role of controlling the channels.

Another point to be noted here is that because a high dimensional unitary operation is usually difficult to implement, it is impractical to equip each terminal node with high dimensional operation capability. Therefore, in our scheme, limited by the capability of each node, we can freely choose which Bob$_j$ can implement two-qubit gates among all the involved nodes to adjust the probabilistic channel. That will greatly reduce the implementation complexity of other agents in a network and bring more convenience to the physical realization of our scheme.

2 Discussion and summary

In previous schemes [11–24,30,31], the shared quantum state via different maximally entangled states can, in principle, be recovered if all participants agree to collaborate. Similar to most existing QSTS schemes, our scheme also presents a control and probabilistic teleportation protocol. As discussed in references [1–9], the security of this QSTS scheme still depends on the process of setting up quantum channels. However, in the case of other schemes, due to inevitable environmental effects, an initially maximally entangled channel shared between the agents involved may easily evolve into various non-maximally entangled channels. For this reason, our scheme utilizes various probabilistic channels composed of non-maximal entangled states instead of standard Bell pair or GHZ states, bringing it closer to a practical communication scenario. Finally, the probability for successful state sharing is calculated.

It should be noted again that when the sender shares different channels with involving agents, any agent who is equipped with the capability of a two qubit operation can help the receiver adopt an appropriate unitary-reduction strategy [27–31] to restore the initial state. Therefore, terminal users will not need to worry about the availability of auxiliary qubits, multi qubit gates or other issues, bypassing the high-dimensional operation problem, which facilitates better physical realization.

In summary, we investigated the usefulness of non-maximally entangled states for simpler and more elegant multi-party quantum state sharing. No multipartite joint measurements are required in our scheme, making it a much more reasonable and acceptable physical design of a quantum teleportation network. We hope that our presented scheme can open up a new road to investigating quantum state sharing in real communication scenarios composed of non-maximally entangled Bell states.

This work was supported by the National Natural Science Foundation of China (61104002, 60904034 and 61071214), the Natural Science Foundation of Jiangsu Province (BK2011283 and BK2011377) and Natural Science Foundation of the Jiangsu Higher Education Institutions of China (10KJB510024).

1 Hillery M, Buzek V, Berthiaume A. Quantum secret sharing. Phys Rev A, 1999, 59: 1829–1834
2 Cleve R, Gottesman D, Lo H K. How to share a quantum secret. Phys Rev Lett, 1999, 83: 648–651
3 Deng F G, Long G L, Liu X S. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. Phys Rev A, 2003, 68: 042317
4 Deng F G, Long G L. Secure direct communication with a quantum one-time pad. Phys Rev A, 2004, 69: 052319
5 Xiao L, Long G L, Deng F G, et al. Efficient multiparty quantum-secret-sharing schemes. Phys Rev A, 2004, 69: 052307
6 Wang C, Deng F G, Long G L. Multi-step quantum secure direct communication using multi-particle Green-Horne-Zeilinger state. Opt Commun, 2005, 253: 15–20
7 Lance A M, Symul T, Bowen W P, et al. Tripartite quantum state sharing. Phys Rev Lett, 2004, 92: 177903
8 Deng F G, Li C Y, Li Y S, et al. Symmetric multiparty-controlled teleportation of an arbitrary two-particle entanglement. Phys Rev A, 2005, 72: 022338
9 Deng F G, Li X H, Li C Y, et al. Multiparty quantum-state sharing of an arbitrary two-particle state with Einstein-Podolsky-Rosen pairs. Phys Rev A, 2005, 72: 044301

10 Zhang J F, Long G L, Zhang W, et al. Simulation of Heisenberg XY-interactions and realization of a perfect state transfer in spin chains using liquid nuclear magnetic resonance. Phys Rev A, 2005, 72: 012331

11 Shi R H, Huang L S, Yang W, et al. Quantum secret sharing between multiparty and multiparty with Bell states and Bell measurements. Sci China Phys Mech Astron, 2010, 53: 2238–2244

12 Hou K, Liu G H, Zhang X Y, et al. An efficient scheme for five-party quantum state sharing of an arbitrary m-qubit state using multi qubit cluster states. Quant Inf Proc, 2011, 10: 463–473

13 Li X H, Zhou P, Li C Y, et al. Efficient symmetric multiparty quantum state sharing of an arbitrary m-qubit state. J Phys B, 2006, 39: 1975–1984

14 Man Z X, Xia Y J, An N B. Quantum state sharing of an arbitrary multi-qubit state using non maximally entangled GHZ states. Eur Phys J D, 2007, 42: 333–340

15 Wang C, Zhang Y, Jin G S. Generalized quantum state sharing of the arbitrary two particles state. Sci China Phys Mech Astron, 2010, 53: 2064–2068

16 Zheng S B. Splitting quantum information via W states. Phys Rev A, 2006, 74: 054303

17 Cao Z L, Song W. Teleportation of a two-particle entangled state via W class states. Physica A, 2005, 347: 177–183

18 Muralidharan S, Panigrahi P K. Quantum-information splitting using multipartite cluster states. Phys Rev A, 2008, 78: 062333

19 Xia Y, Song J, Song H S. Quantum state sharing using linear optical elements. Opt Commun, 2008, 281: 4946

20 Muralidharan S, Panigrahi P K. Splitting of quantum information using N-qubit linear cluster states. Opt Commun, 2011, 28: 1082–1085

21 Muralidharan S, Panigrahi P K. Perfect teleportation, quantum-state sharing, and superdense coding through a genuinely entangled five-qubit state. Phys Rev A, 2008, 77: 032321

22 Choudhury S, Muralidharan S, Panigrahi P K. Quantum teleportation and state sharing using a genuinely entangled six-qubit state. J Phys A: Math Theor, 2009, 42: 115303

23 Hou K, Li Y B, Shi S H. Quantum state sharing with a genuinely entangled five-qubit state and Bell-state measurements. Opt Commun, 2010, 283: 1961–1965

24 Gao T, Yan F L, Li Y C. Quantum secret sharing between m-party and n-party with six states. Sci China Ser G: Phys Mech Astron, 2009, 52: 1191–1202

25 Shi R H, Huang L S, Yang W, et al. Multi-party quantum state sharing of an arbitrary two-qubit state with Bell states. Quant Inf Proc, 2011, 10: 231–239

26 Shi R H, Huang L S, Yang W, et al. Asymmetric five-party quantum state sharing of an arbitrary m-qubit state. Eur Phys J D, 2010, 57: 287–291

27 Hou K, Liu G H, Zhang X Y, et al. An efficient scheme for five-party quantum state sharing of an arbitrary m-qubit state using multiqubit cluster states. Quant Inf Proc, 2011, 10: 463–473

28 Yuan H, Liu Y M, Zhang W, et al. Optimizing resource consumption, operation complexity and efficiency in quantum state sharing. J Phys B At Mol Opt Phys, 2008, 41: 145506

29 Yang C P, Chu S I, Han S Y. Efficient many-party controlled teleportation of multiqubit quantum information via entanglement. Phys Rev A, 2004, 70: 022329

30 Shi R H, Huang L S, Yang W, et al. Efficient multi-party quantum state sharing of an arbitrary two-qubit state. Opt Commun, 2010, 283: 2762–2766

31 Zhang Z J. Controlled teleportation of an arbitrary n-qubit information using quantum secret sharing of classical message. Phys Lett A, 2006, 352: 55–58

32 Jiang M, Li H, Zhang Z K, et al. Faithful teleportation of multi-particle states involving multi spatially remote agents via probabilistic channels. Physica A, 2011, 390: 760–768

33 Gao T, Wang Z X, Yan F L. Quantum logic network for probabilistic teleportation of two-particle state of general form. Chin Phys Lett, 2003, 20: 2094

34 Gao T, Yan F L, Wang Z X. Quantum logic networks for probabilistic teleportation of many particle state of general form. Quant Inf Comput, 2004, 4: 186–195

35 Liu D M, Wang Y W, Jiang X M, et al. A criterion for quantum teleportation of an arbitrary N-particle state via a 2N-particle quantum channel. Chin Phys B, 2010, 19: 020307

36 Nie Y Y, Li Y H, Liu J C, et al. Quantum information splitting of an arbitrary three-qubit state by using two four-qubit cluster states. Quant Inf Proc, 2011, 10: 297–305

37 Jiang M, Li H, Zhang Z K, et al. Faithful teleportation via multi-particle quantum states in a network with many agents. Quant Inf Proc, 2012, 11: 23–40

38 Yang C P. A new protocol for constructing nonlocal n-qubit controlled-U gates. Phys Lett A, 2008, 372: 2782–2786

39 Dong D Y, Petersen I R. Sliding mode control of quantum systems. New J Phys, 2009, 11: 105033