Efficient symmetric multiparty quantum state sharing of an arbitrary $m$-qubit state

Xi-Han Li$^{1,2}$, Ping Zhou$^{1,2}$, Chun-Yan Li$^{1,2}$, Hong-Yu Zhou$^{1,2,3}$ and Fu-Guo Deng$^{1,2,3}$

$^1$ Key Laboratory of Beam Technology and Material Modification of Ministry of Education, Beijing Normal University, Beijing 100875, People’s Republic of China
$^2$ Institute of Low Energy Nuclear Physics, and Department of Material Science and Engineering, Beijing Normal University, Beijing 100875, People’s Republic of China
$^3$ Beijing Radiation Center, Beijing 100875, People’s Republic of China

E-mail: fgdeng@bnu.edu.cn

Received 24 November 2005, in final form 3 March 2006
Published 5 April 2006
Online at stacks.iop.org/JPhysB/39/1975

Abstract

We present a scheme for symmetric multiparty quantum state sharing of an arbitrary $m$-qubit state with $m$ Greenberger–Horne–Zeilinger states following some ideas from the controlled teleportation (2005 Phys. Rev. A 72 02338). The sender Alice performs $m$ Bell-state measurements on her $2m$ particles and the controllers need only take some single-photon product measurements on their photons independently, not multipartite entanglement measurements, which makes this scheme more convenient than the latter. Also it does not require the parties to perform a controlled-NOT gate on the photons for reconstructing the unknown $m$-qubit state and it is an optimal one as its efficiency for qubits approaches 100% in principle.

1. Introduction

Suppose the president of a bank, say Alice, wants to send some secret message $M_A$ to her agents, Bob and Charlie, who are at a remote place for her business. She doubts that one of the two persons may be dishonest and he or she will destroy the business with the message independently. Alice believes that the honest one will keep the dishonest one from doing any damage if they both appear in the process of dealing with the business. In this way, the message cannot be transmitted to the agents directly. In classical secret sharing [1], Alice splits $M_A$ into two pieces, $M_B$ and $M_C$, and sends them to Bob and Charlie, respectively. When they act in concert, they can recover the message $M_A = M_B \oplus M_C$; otherwise, they can obtain nothing about the message. The classical signal is in one of the eigenvectors of a measuring basis (MB), say $\sigma_z$, and it can be copied fully and freely [2]. It is impossible for the parties to communicate in an unconditionally secure way if they only resort to classical
communication [3]. When quantum mechanics enters the field of information, the story is changed [3, 4].

Quantum secret sharing (QSS) is the generalization of classical secret sharing into a quantum scenario. Most existing QSS schemes are focused on creating a private key among several parties or splitting a classical secret. For example, an original QSS scheme [5] was proposed by Hillery, Bužek and Berthiaume (HBB) in 1999 by using three-particle and four-particle entangled Greenberger–Horne–Zeilinger (GHZ) states for distributing a private key among some agents and sharing classical information. In HBB scheme the three parties, Alice, Bob and Charlie, choose randomly two measuring bases (MBs), \( \sigma_x \) and \( \sigma_y \), to measure their particles independently. The probability that the quantum resource can be used for carrying the useful information is 50%. That is, their results are correlated and will be kept for creating a key when they all choose the MB \( \sigma_x \) or one chooses \( \sigma_x \) and the others choose \( \sigma_y \), which takes place with the probability 50%. They removed the ideas in the controlled teleportation [6] to split a classical secret among the agents. Subsequently, Karlsson, Koashi and Imoto proposed another QSS protocol for those two goals with multi-particle entangled states and entanglement swapping [7]. Its intrinsic efficiency for qubits \( \eta_q \) [8], the ratio of the number of theoretical valid transmitted qubits to the number of transmitted qubits is about 50% as half of the instances will be abandoned [9]. Now, there are some theoretic schemes for sharing and splitting a classical message [5, 7, 9–22]. The experiment demonstration of QSS was also studied by some groups [23, 24].

Recently, a novel concept, quantum state sharing (QSTS) was proposed and actively pursued by some groups [24–27]. It is the extension of QSS for sharing an unknown state among several agents by resorting to the multipartite entanglements. Cleve, Gottesman and Lo [25] introduced a way for a \((k, n)\) threshold QSTS scheme which can be used to split a secret quantum state related to a classical secret message [27]. Li et al [26] proposed a scheme for sharing an unknown single qubit with some Einstein–Podolsky–Rosen (EPR) pairs and a multi-particle joint measurement. In 2004, Lance et al studied QSTS with a continuous variable [24]. Deng et al [27] introduced a scheme for splitting an arbitrary two-qubit state with EPR pairs and GHZ-state measurements. Also, some controlled teleportation schemes were discussed in [6, 28, 29]. The unknown state can be teleported to the sender with the control of some controllers. In fact, almost all those controlled teleportation schemes can be used for QSTS with or without a little modification. For example, in [29], QSTS for an arbitrary two-qubit state can be implemented with the symmetric controlled teleportation scheme [29] without any modification. In essence, a secure QSTS scheme can also be used for controlled teleportation by the means that some agents act as the controllers in the latter.

In this paper, we will present a scheme for QSTS of an arbitrary \( m \)-particle state following some ideas in [29]. It will be shown that the agents need only to perform a product measurement \( \sigma_1 x \otimes \sigma_2 x \otimes \cdots \otimes \sigma_m x \) on their particles, not multipartite entanglement measurements, which makes this scheme more convenient than [29]. Moreover, it requires the agents only to perform some local unitary operations on the photons retained for recovering the unknown state, not a two-qubit joint operation, such as controlled-NOT operation.

2. QSTS of an arbitrary \( M \)-qubit state

2.1. QSTS of an arbitrary two-qubit state with two agents

For simplicity, we first present a way for the symmetric quantum state sharing of an arbitrary two-qubit state with two three-particle GHZ states. That is, there are two agents, Bob and Charlie. We assume that the parties share a sequence of multipartite entangled states securely.
Quantum information is an unknown arbitrary two-qubit state in a noise channel. The basic idea of this QSTS scheme can be described as follows. Suppose that the quantum information is an unknown arbitrary two-qubit state

\[ |\Phi\rangle_{xy} = a|00\rangle_{xy} + b|01\rangle_{xy} + c|10\rangle_{xy} + d|11\rangle_{xy}, \]

where \(|0\rangle\) and \(|1\rangle\) are the two eigenvectors of the MB \(\sigma_z\) (for example, the polarization of the single photon along the \(z\)-direction), and

\[ |a|^2 + |b|^2 + |c|^2 + |d|^2 = 1. \]

Alice prepares two three-particle GHZ states

\[ |\Psi\rangle_{a_1a_2a_3} = |\Psi\rangle_{b_1b_2b_3} = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle). \]

When Alice performs the Bell-state measurement on the photons \(x\) and \(a_1\), they are randomly in one of the four Bell states

\[ |\phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle |0\rangle |1\rangle), \]

\[ |\psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle |0\rangle |1\rangle). \]

So does the quantum system comprising the photons \(y\) and \(b_1\).

As an example for demonstrating the principle of this QSTS scheme, we assume that the outcomes obtained by Alice are \(|\phi^+\rangle_{xa_1}\) and \(|\phi^+\rangle_{yb_1}\). Then the retained four photons are in the state \(|\Psi\rangle_r\). Here

\[ |\Psi\rangle_r = a|00\rangle_{a_2b_2}|00\rangle_{a_3b_3} + b|01\rangle_{a_2b_3}|01\rangle_{a_3b_2} + c|10\rangle_{a_2b_3}|10\rangle_{a_3b_2} + d|11\rangle_{a_2b_2}|11\rangle_{a_3b_3}. \]

If Bob performs the product measurement \(\sigma_x \otimes \sigma_y\) on the photons \(a_2\) and \(b_2\), the state \(|\Psi\rangle_r\) can be written as

\[ |\Psi\rangle_r = \frac{1}{2} \left[ |a_2\rangle + |b_2\rangle (a|00\rangle_{a_2b_2} + b|01\rangle_{a_2b_2} + c|10\rangle_{a_2b_2} + d|11\rangle_{a_2b_2}) \right. \]

\[ + |a_2\rangle - |b_2\rangle (a|00\rangle_{a_2b_2} - b|01\rangle_{a_2b_2} + c|10\rangle_{a_2b_2} - d|11\rangle_{a_2b_2}) \]

\[ + |a_2\rangle + |b_2\rangle (a|00\rangle_{a_2b_2} + b|01\rangle_{a_2b_2} - c|10\rangle_{a_2b_2} - d|11\rangle_{a_2b_2}) \]

\[ + |a_2\rangle - |b_2\rangle (a|00\rangle_{a_2b_2} - b|01\rangle_{a_2b_2} - c|10\rangle_{a_2b_2} + d|11\rangle_{a_2b_2}). \]
parity of the Bell-basis measurement and the single-particle measurement \( v \) value entanglement measurements, which makes this QSTS scheme more convenient than that in cooperate. Moreover, the agents need only two single-photon measurements, not multipartite theory.

Different from \([29]\), it is unnecessary for Alice to take a Hadamard operation on each photon in the GHZ state in this QSTS scheme. Also, the agents need not take the operations needed to reconstruct the original state \( |\phi\rangle \) as the bit value of the Bell state, i.e.,

\[
U_0 = |0\rangle \langle 0| + |1\rangle \langle 1|, \quad U_1 = |0\rangle \langle 0| - |1\rangle \langle 1|.
\]

For the other case, the relation between the measurement results and the final state and the operations needed to reconstruct the original state \( |\Phi\rangle_{xy} \) is shown in Table 1. Similar to \([29]\), we define \( V \) as the bit value of the Bell state, i.e., \( V_{\{\phi^+\}} = 0, V_{\{\phi^-\}} = 1 \). That is, the bit value \( V = 0 \) if the states of the two particles are parallel, otherwise \( V = 1 \). \( P \) denotes the parity of the Bell-basis measurement and the single-particle measurement \( \sigma_x \), i.e.,

\[
P_{\{\phi^+\}} \equiv \pm, \quad P_{\{\phi^-\}} \equiv \pm, \quad P_{\{|k\rangle\}} \equiv \pm.
\]

and

\[
U_2 = |1\rangle \langle 0| + |0\rangle \langle 1|, \quad U_3 = |0\rangle \langle 1| - |1\rangle \langle 0|.
\]

Table 1. The relation between the local unitary operations and the results \( R_{sa_1}, R_{sb_1}, R_{sa_2}, \) and \( R_{sb_2} \). \( \Phi_{sa_2b_2} \) is the state of the two particles held in the hands of Charlie after all the measurements are done by Alice and Bob; \( U_C \) are the local unitary operations with which Charlie can reconstruct the unknown state \( |\Phi\rangle_{xy} \).

\[
\begin{array}{|c|c|c|c|c|c|}
\hline
V_{sa_1} & V_{sb_1} & P_{sa_1} \otimes P_{sa_2} & P_{sb_1} \otimes P_{sb_2} & \Phi_{sa_2b_2} & U_C \\
\hline
0 & 0 & + & + & a(00) + b(01) + c(10) + d(11) & U_0 \otimes U_0 \\
0 & 0 & + & - & a(00) - b(01) + c(10) - d(11) & U_0 \otimes U_1 \\
0 & 0 & - & + & a(00) + b(01) - c(10) - d(11) & U_1 \otimes U_0 \\
0 & 0 & - & - & a(00) - b(01) - c(10) - d(11) & U_1 \otimes U_1 \\
0 & 1 & + & + & a(01) + b(00) + c(11) + d(10) & U_0 \otimes U_2 \\
0 & 1 & + & - & a(01) - b(00) + c(11) - d(10) & U_0 \otimes U_3 \\
0 & 1 & - & + & a(01) + b(00) - c(11) - d(10) & U_1 \otimes U_2 \\
0 & 1 & - & - & a(01) - b(00) - c(11) + d(10) & U_1 \otimes U_3 \\
1 & 0 & + & + & a(10) + b(11) + c(00) + d(01) & U_2 \otimes U_0 \\
1 & 0 & + & - & a(10) - b(11) + c(00) - d(01) & U_2 \otimes U_1 \\
1 & 0 & - & + & a(10) + b(11) - c(00) - d(01) & U_3 \otimes U_0 \\
1 & 0 & - & - & a(10) - b(11) - c(00) + d(01) & U_3 \otimes U_1 \\
1 & 1 & + & + & a(11) + b(10) + c(01) + d(00) & U_2 \otimes U_2 \\
1 & 1 & + & - & a(11) - b(10) + c(01) - d(00) & U_2 \otimes U_3 \\
1 & 1 & - & + & a(11) + b(10) - c(01) - d(00) & U_3 \otimes U_2 \\
1 & 1 & - & - & a(11) - b(10) - c(01) + d(00) & U_3 \otimes U_3 \\
\hline
\end{array}
\]
### 2.2. QSTS of an arbitrary two-qubit state with \( n + 1 \) agents

It is straightforward to generalize this QSTS scheme to the case with \( n + 1 \) agents, similar to [29]. For this multiparty QSTS, Alice will prepare two \((n + 2)\)-photon GHZ states and share them with the \( n + 1 \) agents securely first. Then the composite state of the system is

\[
|\Psi_S\rangle \equiv |\Phi_{xy}\rangle \otimes |\Psi_{a_1}\rangle \otimes |\Psi_{a_2}\rangle \\
= (a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle)_{xy} \\
\otimes \frac{1}{\sqrt{2}} \left( \prod_{i=1}^{n+2} |0\rangle_{a_i} + \prod_{i=1}^{n+2} |1\rangle_{a_i} \right) \\
\otimes \frac{1}{\sqrt{2}} \left( \prod_{i=1}^{n+2} |0\rangle_{b_i} + \prod_{i=1}^{n+2} |1\rangle_{b_i} \right) .
\]

(12)

After Alice takes the Bell-state measurements on the particles \( x \) and \( a_1 \), and \( y \) and \( b_1 \), respectively, the state of the subsystem (without being normalized) becomes

\[
|\Psi_{\text{sub}}\rangle = \alpha \prod_{i=2}^{n+2} |0\rangle_{a_i} \prod_{i=2}^{n+2} |0\rangle_{b_i} + \beta \prod_{i=2}^{n+2} |0\rangle_{a_i} \prod_{i=2}^{n+2} |1\rangle_{b_i} + \gamma \prod_{i=2}^{n+2} |1\rangle_{a_i} \prod_{i=2}^{n+2} |0\rangle_{b_i} + \delta \prod_{i=2}^{n+2} |1\rangle_{a_i} \prod_{i=2}^{n+2} |1\rangle_{b_i} .
\]

(13)

The relation between the parameters \( \alpha, \beta, \gamma, \delta \) and the results \( R_{xa_1} \) and \( R_{yb_1} \) is shown in Table 2.

When the agents want to reconstruct the original state \( |\Phi_{xy}\rangle \), \( n \) agents perform the single-photon product measurement \( \sigma_z \otimes \sigma_z \) on their photons independently. Let us assume that the agents who measure the photons are Bob \( i \) \((i = 2, 3, \ldots, n + 1)\) and the one who does not measure his photons is Charlie. That is, the Bob \( i \) act as the controllers for recovering the unknown state. The measurements done by them can be expressed by the formula \( M \),

\[
M \equiv [(|+\rangle x)^{n-1}(|-\rangle x)^{\parallel}]_b \otimes [(|+\rangle x)^{n-2}(|-\rangle x)^{\parallel}]_b .
\]

(14)
Here \([(+(x)^{n-q}(-x)^{q})]_a\) is the measurement operation related to the state of \(a_i\), and \([(+(x)^{n-q}(-x)^{q})]_b\) is related to \(b_i\). \(t\) and \(q\) are the numbers of the controllers who obtain the result \((-x)\) when they measure the particle \(a_i\) and \(b_i\), respectively. After the measurements done by Alice and the \(n\) controllers, the final state \(\Phi_{a_{n+2}b_{n+2}}\) can be gained by means of performing the operation \(M\) on the state \(\Psi_{\text{sub}}\),

\[
\Phi_{a_{n+2}b_{n+2}} = M \left( \prod_{i=2}^{n+2} a_i \prod_{i=2}^{n+2} (0)_{b_i} + \beta \prod_{i=2}^{n+2} (0)_{a_i} \prod_{i=2}^{n+2} (1)_{b_i} \right)
+ \gamma \prod_{i=2}^{n+2} (1)_{a_i} \prod_{i=2}^{n+2} (0)_{b_i} + \delta \prod_{i=2}^{n+2} (1)_{a_i} \prod_{i=2}^{n+2} (1)_{b_i} \right)
= \alpha |0\rangle_{a_{n+2}} |0\rangle_{b_{n+2}} + (-1)^t \beta |0\rangle_{a_{n+2}} |1\rangle_{b_{n+2}}
+ (-1)^q \gamma |1\rangle_{a_{n+2}} |0\rangle_{b_{n+2}} + (-1)^{t+q} \delta |1\rangle_{a_{n+2}} |1\rangle_{b_{n+2}}.
\]

(15)

We define

\[
P_1 = P_{x_{a_i}} \otimes \prod_{i=2}^{n+1} P_{a_i}, \quad P_2 = P_{y_{b_i}} \otimes \prod_{i=2}^{n+1} P_{b_i},
\]

(16)

where \(P_{x_{a_i}}\) and \(P_{y_{b_i}}\) are the results of Bell-basis measurements done by Alice, and \(P_{a_i}\) and \(P_{b_i}\) are the results of single-particle measurements done by the \(n\) controllers, respectively.

The relation between the results of the measurements and the local operations with which Charlie reconstructs the original state when he cooperates with Bob \(j\) is the same as that in table 1 with a little modification. That is, \(P_{x_{a_i}} \otimes P_{a_i}, P_{y_{b_i}} \otimes P_{b_i}\) and \(\Phi_{a_{n+2}b_{n+2}}\) are replaced by \(P_1, P_2\) and \(\Phi_{a_{n+2}b_{n+2}}\), respectively.

Same as the case with two agents, this multiparty QSTS does not require the agents to do Bell-state measurements on their photons. Whether the number of the controllers is odd or even, the last agent Charlie need only take two local unitary operations on the two photons for reconstructing the unknown two-qubit state.

2.3. QSTS of an arbitrary \(m\)-qubit state with \(n + 1\) agents

An \(m\)-qubit state can be described as

\[
|\Phi\rangle = \sum_{i_1, x_2, \ldots, x_m} a_{i_1 x_2 \ldots x_m} |i_1 x_2 \ldots x_m\rangle,
\]

(17)

where \(i, j, \ldots, k \in \{0, 1\}\), and \(x_1, x_2, \ldots, x_m\) are the \(m\) particles in the unknown state. For sharing this \(m\)-qubit state, Alice will prepare \(m\) \((n + 2)\)-photon GHZ states and share them with the \(n + 1\) agents, say Bob \(j\) \((j = 1, 2, \ldots, n)\) and Charlie. Then the state of the composite quantum system can be written as

\[
|\Psi\rangle \equiv \left( \sum_{i_1, x_2, \ldots, x_m} a_{i_1 x_2 \ldots x_m} |i_1 x_2 \ldots x_m\rangle \right)
\otimes \prod_{i=1}^{m} \left[ \frac{1}{\sqrt{2}} \left( \prod_{j=0}^{n+1} |0\rangle_{b_{j_i}} + \sum_{j=0}^{n+1} |1\rangle_{b_{j_i}} \right) \right],
\]

(18)

where the particles \(b_{j_1}\) \((i = 1, 2, \ldots, m)\) are held in the hands of Bob \(j_1\) \((j = 1, 2, \ldots, n)\), \(b_{j_0}\) are the particles of Alice, and \(b_{(n+1)}\) are controlled by Charlie. Similar to [34], after the Bell-state measurements on the particles \(x_i\) and \(b_{j_0}\) done by Alice \((i = 1, 2, \ldots, m)\), the
unknown $m$-qubit state will be transferred to the quantum system composed of the photons kept by the agents. Each of Bob$_j$ performs the product measurement $\sigma_i^1 \otimes \sigma_i^2 \otimes \cdots \otimes \sigma_i^m$ on his $m$ photons $b_{ij}$ ($i = 1, 2, \ldots, m$), then the state of the photons kept by Charlie becomes $(U_{-i}^{-1} \otimes \cdots \otimes U_{-i}^{-1} \otimes \cdots \otimes U_{-m}^{-1})|\Phi\rangle_u$. Here $U_{-i}^{-1} \otimes U_{-i}' = I$, and the relation between the results of the measurements and the local unitary operations $U_i'$ is shown in table 3. The notation $V_i$ is the bit value of the Bell-state measurement on the particles $x_i$ and $b_{i0}$, and $P_i$ is defined as

$$P_i = P_{x, b_{i0}} \otimes \prod_{k=1}^{n} P_{b_{kj}}.$$  

That is, if $V_i = 0$ and $P_i = +$, Charlie performs the unitary operation $U_0$ on the $i$th photon for reconstructing the unknown state $|\Phi\rangle_u$.

3. Discussion and summary

In fact, every one of the multiparty quantum state sharing schemes can be used for multiparty-controlled teleportation by the means that some of the agents act as the controllers. That is, this multiparty QSTS scheme can also be used for completing the task in [29] efficiently. For sharing of multipartite entanglement, the parties should resort to either multipartite entanglement quantum resources acting as the quantum channel or multipartite entanglement measurements. At present, both of them are not easy to be implemented [35–37]. With the development of technology, they may be feasible in the future. Compared with the scheme in [27], this multiparty QSTS scheme is more feasible when the unknown quantum system is $m$-qubit one and the number of agents is $n$ ($m, n > 2$) as the sender Alice should perform two $(\frac{n+m}{2}+1)$-photon GHZ-state measurements in the former. Different from [29], each of the controllers needs only to take a product measurement $\sigma_i^1 \otimes \sigma_i^2 \otimes \cdots \otimes \sigma_i^m$ on his photons, no multipartite entanglement measurements, and the last agent can reconstruct the unknown $m$-qubit state with only $m$ local unitary operations, not CNOT gates, when he cooperates with the controllers, which makes this QSTS scheme more convenient than that in the former.

From table 3, one can see that the agent Charlie can reconstruct the original unknown state with the probability 100% in principle if he cooperates with all the other agents. However, he will only has the probability $\frac{1}{2^n}$ to get the correct result if one of the other agents does not agree to cooperate as Charlie has only half of the chance to choose the correct operation for each qubit according to the information published by Alice and the other $n-1$ agents. That is, this multiparty QSTS scheme is a $(n, n)$ threshold one, same as that in [7]. On the other hand, as almost all the quantum sources (except for the instances chosen for eavesdropping check) can be used to carry the quantum information if the agents act in concert, the intrinsic efficiency for qubits $\eta_q$ in this scheme approaches 100%, same as those in the schemes [28, 29, 34, 38–43] for quantum teleportation and controlled teleportation. Here [8]

$$\eta_q = \frac{q_u}{q_t},$$  

where $q_u$ is the number of the useful qubits in QSTS and $q_t$ is the number of transmitted qubits. In our scheme, for sharing $m$-qubit quantum information with $n+1$ agents $q_u = q_t = (n+1)m$. 

---

**Table 3.** The relation between the values of $V_i$, $P_i$ and the local unitary operation $U_i$.

| $V_i$ | $P_i$ | $U_i'$ | $U_0$ | $U_1$ | $U_2$ | $U_3$ |
|-------|-------|--------|-------|-------|-------|-------|
| 0     | 0     | 1      | 1     |       |       |       |
|       | +     | −      | +     | −     | −     | −     |
We exploited the definition of the intrinsic efficiency for qubits introduced by Cabello for quantum cryptography \[8\]. The total efficiency for this scheme can be calculated as follows,

\[
\eta_t = \frac{q_u}{q_t + b_t},
\]

(21)

where \( b_t \) is the number of the classical bits exchanged, \( b_t = 2m + nm = (n + 2)m \). That is,

\[
\eta_t = \frac{(n + 1)m}{(n + 1)m + (n + 2)m} = \frac{n + 1}{2n + 3},
\]

the maximal value for QSTS.

In summary, we present a multiparty QSTS scheme for sharing an arbitrary \( m \)-qubit state with \( m \) GHZ states, removing some ideas in the symmetric multiparty-controlled teleportation \[29\]. It is an optimal one with GHZ states used as a quantum channel for sharing an arbitrary \( m \)-qubit state as one of the parties needs only to perform two-photon Bell-state measurements and the others use single-photon product measurements. Moreover, its efficiency for qubits is 100\%, the maximal value as all the quantum resources are useful in theory, and each of the agents can act as the receiver. Simultaneously, this multiparty QSTS scheme can be used for controlled teleportation efficiently.

Acknowledgments

This work is supported by the National Natural Science Foundation of China under grant nos 10447106, 10435020, 10254002, A0325401 and 10374010, and Beijing Education Committee under grant no XK100270454.

References

[1] Blakley G R 1979 Proc. American Federation of Information Processing 1979 National Computer Conference (Arlington, VA: American Federation of Information Processing) p 313
[2] Shamir A 1979 Commun. ACM 22 612
[3] Nielsen M A and Chuang I L 2000 Quantum Computation and Quantum Information (Cambridge: Cambridge University Press)
[4] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 Rev. Mod. Phys. 74 145
[5] Hillery M, Bužek V and Berthiaume A 1999 Phys. Rev. A 59 1829
[6] Karlsson A and Bourennane M 1998 Phys. Rev. A 58 4394
[7] Karlsson A, Koashi M and Imoto N 1999 Phys. Rev. A 59 162
[8] Cabello A 2000 Phys. Rev. Lett. 85 5635
[9] Deng F G, Zhou H Y and Long G L 2005 Phys. Lett. A 337 329
[10] Gottesman D 2000 Phys. Rev. A 61 012308
[11] Nascimento A C A, Mueller-Quade J and Imai H 2001 Phys. Rev. A 64 042311
[12] Yang C P and Gea-Banacloche J 2001 J. Opt. B: Quantum Semiclass. Opt. 3 407
[13] Bagherinezhad S and Karimipour V 2003 Phys. Rev. A 67 044302
[14] Tyc T and Sanders B C 2002 Phys. Rev. A 65 042310
[15] Xiao L, Long G L, Deng F G and Pan J W 2004 Phys. Rev. A 69 052307
[16] Deng F G, Long G L and Zhou H Y 2005 Phys. Lett. A 340 43
[17] Guo G P and Guo G C 2003 Phys. Lett. A 310 247
[18] Zhang Z J 2005 Phys. Lett. A 342 60
[19] Bandyopadhyay S 2000 Phys. Rev. A 62 012308
[20] Karimipour V, Bahraminasab A and Bagherinezhad S 2002 Phys. Rev. A 65 042320
Efficient symmetric multiparty quantum state sharing of an arbitrary $m$-qubit state

[21] Zhang Z J, Li Y and Man Z X 2005 Phys. Rev. A 71 044301
Deng F G et al 2005 Phys. Rev. A 72 044302

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

[23] Tittel W, Zbinden H and Gisin N 2001 Phys. Rev. A 63 042301

[24] Lance A M, Symul T, Bowen W P, Sanders B C and Lam P K 2004 Phys. Rev. Lett. 92 177903
Lance A M, Symul T, Bowen W P, Sanders B C, Tyc T, Ralph T C and Lam P K 2005 Phys. Rev. A 71 033814

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

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

[27] Yang C P, Chu S I and Han S Y 2004 Phys. Rev. A 70 022329

[28] Deng F G, Li C Y, Li Y S, Zhou H Y and Wang Y 2005 Phys. Rev. A 72 022338

[29] Deng F G, Long G L and Liu X S 2003 Phys. Rev. A 68 042317

[30] Deng F G and Long G L 2004 Phys. Rev. A 69 052319

[31] Deng F G et al 2005 Phys. Rev. A 71 044305

[32] Deutsch D, Ekert A, Jozsa R, Macchiavello C, Popescu S and Sanpera A 1996 Phys. Rev. Lett. 77 2818

[33] Merao M, Pleno M B, Popescu S, Vedral V and Knight P L 1998 Phys. Rev. A 57 R4075

[34] Yang C P and Guo G C 2000 Chin. Phys. Lett. 17 162

[35] Pigeon G and Long G L 2003 Phys. Rev. A 71 032303

[36] Deng F G 2005 Phys. Rev. A 72 036301

[37] Bouwmeester D, Pan J W, Daniell M, Weinfurter H and Zeilinger A 1999 Phys. Rev. Lett. 82 1345

[38] Pan J W, Daniell M, Gasparoni S, Weihs G and Zeilinger A 2001 Phys. Rev. Lett. 86 4435

[39] Zhao Z, Chen Y A, Zhang A N, Yang T, Briegel H J and Pan J W 2004 Nature 430 54

[40] Bennett C H, Brassard G, Crépeau C, Jozsa R, Peres A and Wootters W K 1993 Phys. Rev. Lett. 70 1895

[41] Gorbachev V N and Trubilko A I 1999 Preprint quant-ph/9906110

[42] Marinatto L and Weber T 2000 Found. Phys. Lett. 13 119

[43] Shi B S, Jiang Y K and Guo G C 2000 Phys. Lett. A 268 161

[44] Lu H and Guo G C 2000 Phys. Lett. A 276 209

[45] Yan F L, Tan H G and Yang L G 2002 Commun. Theor. Phys. 37 649