Eur. Phys. J. D **33**, 133–136 (2005)
DOI: 10.1140/epjd/e2005-00029-5

THE EUROPEAN
PHYSICAL JOURNAL D

Multiparty secret sharing of quantum information using and identifying Bell states

Z.J. Zhang[1,2,a], J. Yang[1], Z.X. Man[2], and Y. Li[3]

[1] School of Physics & Material Science, Anhui University, Hefei 230039, P.R. China
[2] Wuhan Institute of Physics and Mathematics, Chinese Academy of Sciences, Wuhan 430071, P.R. China
[3] Department of Physics, Huazhong Normal University, Wuhan 430079, P.R. China

Received 1st November 2004
Published online 1st March 2005 – © EDP Sciences, Società Italiana di Fisica, Springer-Verlag 2005

Abstract. In this paper, only Bell states are employed and needed to be identified to realize the multiparty secret sharing of quantum information, where the secret is an arbitrary unknown quantum state in a qubit. In our multiparty quantum information secret sharing (QISS) scheme, no subset of all the quantum information receivers is sufficient to reconstruct the unknown state in a qubit but the entire is. The present multiparty QISS scheme is more feasible with present-day technique.

PACS. 03.67.Pp Quantum error correction and other methods for protection against decoherence – 03.65.Db Functional analytical methods – 42.65.Lm Parametric down conversion and production of entangled photons

The quantum secret sharing (QSS) is likely to play a key role in protecting secret quantum information, e.g., in secure operations of distributed quantum computation, sharing difficult-to-construct ancilla states and joint sharing of quantum money, and so on. Hence, after the pioneering QSS work proposed by using three-particle and four-particle GHZ states [1], this kind of works on QSS attracted a great deal of attentions in both theoretical and experimental aspects [2–14]. In all these works, the secret which is sent by a sender and shared by multi-receivers can be classified into two types, i.e., the classical messages (bits) or the quantum information (where the secret is an arbitrary unknown quantum state in the sender's qubit). The essence of a multiparty secret sharing of a quantum information is that no subset of all the quantum information receivers can reconstruct the unknown state in a qubit but the entire collaborates, i.e., only with all other receivers' helps, one receiver can reconstruct the unknown state in a qubit. To achieve multiparty secret sharing of a quantum information, in those existing works [1,2,5,10,14], multi-particle GHZ states are widely used and the identification of the multi-particle GHZ states is necessary. Only very recently, Li, Zhang and Peng [13] have proposed a multiparty quantum information secret sharing (QISS) scheme by employing only Bell states. However, in their scheme, the identification of a multi-particle GHZ state is also necessary. It is generally admitted that, to the present-day technique, an identification of a Bell state [15] is much easier that an identification of a multi-particle GHZ state. Hence, in this paper, we will propose a multi-party QISS scheme by using and identifying only Bell state.

Before giving our multiparty QISS scheme, let us briefly review quantum entanglement swapping, for it will be used and will play a very important role in our scheme. It is well-known that quantum entanglement swapping [16–19] can entangle two quantum systems which do not interact with each other. Let $|0\rangle$ and $|1\rangle$ be the different degrees of a qubit, respectively. Then the four Bell states, $\phi^{\pm} = (|00\rangle \pm |11\rangle)/\sqrt{2}$ and $\psi^{\pm} = (|01\rangle \pm |10\rangle)/\sqrt{2}$, are maximally entangled states in the two-qubit Hilbert space. If the initial states are two qubit pairs each in a Bell state, then after the quantum entanglement swapping the possible output states are another two qubit pairs in Bell states. The possibility is 1/4. The corresponding relations between the initial Bell states and the possible output Bell states after the quantum entanglement swapping are summarized in Table 1. Note that, one very important feature which will be used later is that, provided that one initial Bell state and the two Bell state outcomes after the quantum entanglement swapping are known, one can immediately know the other initial Bell state.

Let us turn to our multiparty QISS scheme. Suppose that there are n parties. Alice is the sender of a quantum information, where the secret is an arbitrary unknown state $|F\rangle = \alpha|0\rangle_u + \beta|1\rangle_u$. Bob, Charlie, Dick, ..., Zech are

[a] e-mail: zhangzj@wipm.ac.cn

Table 1. The corresponding relations between the two initial Bell states (TIBSs) and the two possible output Bell states (TPOBSs) after the quantum entanglement swapping.

TIBSs	TPOBSs	TPOBSs	TPOBSs	TPOBSs
$\{\phi^+_{12}, \phi^+_{34}\}$ $(\{\phi^-_{12}, \phi^-_{34}\}, \{\psi^+_{12}, \psi^+_{34}\}, \{\psi^-_{12}, \psi^-_{34}\})$	$\{\phi^+_{13}, \phi^+_{24}\}$	$\{\phi^-_{13}, \phi^-_{24}\}$	$\{\psi^+_{13}, \psi^+_{24}\}$	$\{\psi^-_{13}, \psi^-_{24}\}$
$\{\phi^-_{12}, \phi^+_{34}\}$ $(\{\phi^+_{12}, \phi^-_{34}\}, \{\psi^-_{12}, \psi^+_{34}\}, \{\psi^+_{12}, \psi^-_{34}\})$	$\{\phi^+_{13}, \phi^-_{24}\}$	$\{\phi^-_{13}, \phi^+_{24}\}$	$\{\psi^+_{13}, \psi^-_{24}\}$	$\{\psi^-_{13}, \psi^+_{24}\}$
$\{\psi^+_{12}, \phi^+_{34}\}$ $(\{\psi^-_{12}, \phi^-_{34}\}, \{\phi^+_{12}, \psi^+_{34}\}, \{\phi^-_{12}, \psi^-_{34}\})$	$\{\phi^+_{13}, \psi^+_{24}\}$	$\{\phi^-_{13}, \psi^-_{24}\}$	$\{\psi^+_{13}, \phi^+_{24}\}$	$\{\psi^-_{13}, \phi^-_{24}\}$
$\{\psi^-_{12}, \phi^+_{34}\}$ $(\{\psi^+_{12}, \phi^-_{34}\}, \{\phi^-_{12}, \psi^+_{34}\}, \{\phi^+_{12}, \psi^-_{34}\})$	$\{\phi^+_{13}, \psi^-_{24}\}$	$\{\phi^-_{13}, \psi^+_{24}\}$	$\{\psi^+_{13}, \phi^-_{24}\}$	$\{\psi^-_{13}, \phi^+_{24}\}$

the first, second, third, ..., $(n-1)$th quantum information receivers, respectively. Alice wants to let Bob, Charlie, Dick, ..., Zech to securely share her quantum information, in other words, any subset of the $(n-1)$ receivers can not reconstruct the unknown quantum state in a qubit but the entire collaborates. By the way, since the entanglement is employed in our schemes, whether the transmission of a photon of an entangled pair in a quantum channel is attacked can be easily detected by the generally used two-measuring-basis method [20], that is, the security of the photon transmission can be assured. Our n-party scheme contains the following steps.

(1) Each party prepares a photon pair in a Bell state. Besides the entangled photon pair Alice has one more photon (named u hereafter) in the unknown state $|F\rangle = \alpha|0\rangle_u + \beta|1\rangle_u$. Now the state of the whole system is $\mathcal{B}_{b_1b_2}|u\rangle\mathcal{A}_{a_1a_2}\mathcal{C}_{c_1c_2}\mathcal{D}_{d_1d_2}...\mathcal{Z}_{z_1z_2}$, where each of the calligraphic alphabets stands for an arbitrary Bell state (same hereafter), x_i $(x = b, a, c, d, ..., z; i = 1, 2)$ is the label of the photon in Bob's (Alice's, Charlie's, Dick's, ..., Zech's) photon pair.

(2) Bob sends to Alice the photon b_2, Alice sends to Charlie the photon a_2, Charlie sends to Dick the photon c_2, and so on. The $(n-1)$th receiver Zech sends to Alice but not to Bob the photon z_2.

(3) Alice performs a Bell-state measurement on the photons b_2 and u in her lab. This is an identification of a Bell state in the present scheme instead of the identification of the multi-particle GHZ state in other schemes [1,2,5,10,13,14]. Now the state of the whole system is one of the following states with possibility 1/4, $(U_j|F\rangle_{b_1})\mathcal{H}^j_{ub_2}\mathcal{A}_{a_1a_2}\mathcal{C}_{c_1c_2}\mathcal{D}_{d_1d_2}...\mathcal{Z}_{z_1z_2}, (j = 1, 4)$, where the unitary operator $U_j (j = 1, 4)$ are determined by the initial Bell state $\mathcal{B}_{b_1b_2}$ according to the elaborated quantum teleportation theory first presented by Bennett et al. [25].

(4) According to her Bell-state measurement outcome $\mathcal{H}^j_{ub_2} (j = 1, 4)$, Alice performs the corresponding unitary operation U_j on either the photon a_1 or the photon z_2, say, on the photon a_1, then the state of the whole system now becomes $(U_j|F\rangle_{b_1})\mathcal{H}^j_{ub_2}\mathcal{A}'_{a_1a_2}\mathcal{C}_{c_1c_2}\mathcal{D}_{d_1d_2}...\mathcal{Z}_{z_1z_2}$, where $\mathcal{A}'_{a_1a_2} = U_j\mathcal{A}_{a_1a_2}$. After her unitary operation, she performs a Bell-state measurement on the two photons a_1 and z_2, then the state of the whole system becomes $(U_j|F\rangle_{b_1})\mathcal{H}^j_{ub_2}\mathcal{M}_{a_1z_2}\mathcal{C}_{c_1c_2}\mathcal{D}_{d_1d_2}...\mathcal{N}^{cz}_{a_2z_1}$, where $\mathcal{M}^a_{a_1z_2}$ is Alice's Bell-state measurement outcome and $\mathcal{N}^{cz}_{a_2z_1}$ denotes that the photon a_2 in Charlie's lab is entangled with the photon z_1 in Zech's lab after Alice's measurement. Alice announces her measurement outcome $\mathcal{M}^a_{a_1z_2}$ and the state $\mathcal{A}_{a_1a_2}$ of her initially prepared photon pair.

(5) After knowing Alice's public announcements, Charlie, Dick, ..., Zech perform in turn Bell-state measurements on the photon pairs in their respective lab, then the state of the whole system evolves as follows,

$$\begin{aligned}&(U_j|F\rangle_{b_1})\mathcal{H}^j_{ub_2}\mathcal{M}^a_{a_1z_2}\mathcal{C}_{c_1c_2}\mathcal{D}_{d_1d_2}...\mathcal{N}^{cz}_{a_2z_1} \rightarrow\\ &\quad(U_j|F\rangle_{b_1})\mathcal{H}^j_{ub_2}\mathcal{M}^a_{a_1z_2}\mathcal{Q}^c_{a_2c_1}\mathcal{D}_{d_1d_2}...\mathcal{R}^{dz}_{c_2z_1} \rightarrow\\ &\quad(U_j|F\rangle_{b_1})\mathcal{H}^j_{ub_2}\mathcal{M}^a_{a_1z_2}\mathcal{Q}^c_{a_2c_1}\mathcal{S}^d_{c_2d_1}...\mathcal{T}^{dz}_{d_2z_1} \rightarrow ... \rightarrow\\ &\qquad(U_j|F\rangle_{b_1})\mathcal{H}^j_{ub_2}\mathcal{M}^a_{a_1z_2}\mathcal{Q}^c_{a_2c_1}\mathcal{S}^d_{c_2d_1}...\mathcal{W}^z_{y_2z_1}.\end{aligned}$$

(6) If all quantum information receivers except for Bob collaborate, they can deduce in a recursive way what the unitary operator U_j is. Further, if they collaborate with Bob, they can designate Bob to perform the specific unitary operation U_j on his qubit b_1. In this case, the unknown state $|F\rangle$ now is successfully reconstructed in Bob's photon b_1. All these mean that only all the quantum information receivers' collaborate can the unknown state $|F\rangle$ be reconstructed in Bob's photon b_1. Otherwise, the reconstruction fails.

So far we have presented a n-party $(n \geq 3)$ QISS scheme. To more easily understand the present multiparty QISS scheme, let us show a specific example of a 5-party QISS scheme.

(F1) Without loss of the generality, one can suppose that the Bell state in the photon pair prepared by Bob (Alice, Charlie, Dick, Ellen) is $\phi^+_{b_1b_2}$ $(\phi^+_{a_1a_2}, \phi^-_{c_1c_2}, \psi^+_{d_1d_2}, \psi^-_{e_1e_2})$. Alice is the quantum information sender and has one more photon u in an unknown state $|F\rangle = \alpha|0\rangle_u + \beta|1\rangle_u$. Other persons are the quantum information receivers.

(F2) Bob (Alice, Charlie, Dick, Ellen) sends Alice (Charlie, Dick, Ellen, Alice) the photon b_2 (a_2, c_2, d_2, e_2). Note that Ellen sends the photon e_2 to Alice but not to Bob.

(F3) Alice performs a Bell-state measurement on the photons b_2 and u in her lab. Since the following equation holds,

$$\begin{aligned}
&|F\rangle_u \phi^+_{b_1b_2}(\alpha|0\rangle_u+\beta|1\rangle_u)\phi^+_{b_1b_2}\\
&\quad=(\alpha|0\rangle_u+\beta|1\rangle_u)\frac{1}{\sqrt{2}}(|0\rangle_{b_1}|0\rangle_{b_2}+|1\rangle_{b_1}|1\rangle_{b_2}\\
&\quad=\frac{1}{2}\phi^+_{ub_2}(\alpha|0\rangle_{b_1}+\beta|1\rangle_{b_1})+\frac{1}{2}\psi^+_{ub_2}(\alpha|1\rangle_{b_1}+\beta|0\rangle_{b_1})\\
&\qquad+\frac{1}{2}\phi^-_{ub_2}(\alpha|0\rangle_{b_1}-\beta|1\rangle_{b_1})+\frac{1}{2}\psi^-_{ub_2}((\alpha|1\rangle_{b_1}-\beta|0\rangle_{b_1})\\
&\quad=\frac{1}{2}\phi^+_{ub_2}(U_1|F\rangle_{b_1})+\frac{1}{2}\psi^+_{ub_2}(U_2|F\rangle_{b_1})\\
&\qquad+\frac{1}{2}\phi^-_{ub_2}(U_3|F\rangle_{b_1})+\frac{1}{2}\psi^-_{ub_2}(U_4|F\rangle_{b_1}), \qquad (1)
\end{aligned}$$

where $U_1=|0\rangle\langle 0|+|1\rangle\langle 1|$, $U_2=|0\rangle\langle 1|+|1\rangle\langle 0|$, $U_3=|0\rangle\langle 0|-|1\rangle\langle 1|$ and $U_4=|0\rangle\langle 1|-|1\rangle\langle 0|$, Alice's measurement outcome should be a Bell state, say, $\psi^+_{ub_2}$.

(F4) According to her measurement outcome in (F3), Alice performs the unitary operation U_2 on the photon a_1, then the state of the system now becomes $\psi^+_{ub_2}(U_2|F\rangle_{b_1})(U_2\phi^+_{a_1a_2})\phi^-_{c_1c_2}\psi^+_{d_1d_2}\psi^-_{e_1e_2} = \psi^+_{ub_2}(U_2|F\rangle_{b_1})\psi^+_{a_1a_2}\phi^-_{c_1c_2}\psi^+_{d_1d_2}\psi^-_{e_1e_2}$. After Alice's unitary operation, Alice performs another Bell-state measurement on the photons a_1 and e_2 in her lab and then publicly announces the Bell state $\phi^+_{a_1a_2}$ of her initially prepared photon pair and her second measurement outcome, say, $\psi^-_{a_1e_2}$. Then the state of the whole system now becomes $\psi^+_{ub_2}(U_2|F\rangle_{b_1})\psi^-_{a_1e_2}\phi^-_{c_1c_2}\psi^+_{d_1d_2}\psi^+_{a_2e_1}$ according to the Table 1 about the quantum entanglement swapping.

(F5) After knowing Alice's public announcements, Charlie performs a Bell-state measurement on the two photons a_2 and c_1 in his lab. Since the outcome should be one of the four Bell states, without loss of the generality, we suppose it is $\phi^-_{a_2c_1}$. Then the state of the whole system evolves to $\psi^+_{ub_2}(U_2|F\rangle_{b_1})\psi^-_{a_1e_2}\phi^-_{a_2c_1}\psi^+_{d_1d_2}\psi^+_{c_2e_1}$. After Charlie's measurement, Dick and Ellen perform the Bell-state measurements on the photons in their labs, respectively. Since the initial states are $\psi^+_{d_1d_2}$ and $\psi^+_{c_2e_1}$, according to Table 1, their measurement outcomes after the quantum entanglement swapping should be one of the four Bell state groups, i.e., $\{\phi^+_{c_2d_1},\ \phi^+_{d_2e_1}\}$ or $\{\phi^-_{c_2d_1},\ \phi^-_{d_2e_1}\}$ or $\{\psi^+_{c_2d_1},\ \psi^+_{d_2e_1}\}$ or $\{\psi^-_{c_2d_1},\ \psi^-_{d_2e_1}\}$. Also without loss of the generality, we suppose they are the first group, then the state of the whole system becomes $\psi^+_{ub_2}(U_2|F\rangle_{b_1})\psi^-_{a_1e_2}\phi^-_{a_2c_1}\phi^+_{c_2d_1}\phi^+_{d_2e_1}$.

(F6) If Charlie, Dick and Ellen collaborate, they can work out the unitary operation U_2 Alice has performed on the photon a_2 in a recursive way. This is completely a reverse process of (F5) and (F4). Therefore, if they collaborate with Bob further, they can designate Bob to perform the unitary operation U_2 on his qubit b_1. In this case, the unknown state $|F\rangle$ has been successfully reconstructed in the photon b_1. This is realized by all the quantum information receivers' collaboration. If any one does not collaborate, the reconstruction fails.

Now let us do some discussions. First, since the present multiparty QISS scheme is based on EPR pairs, so the proof of the security is the same in essence as those in references [20–24]. It is also unconditionally secure. Secondly, our multiparty SSQI scheme ($n \geq 3$) is almost the same as the secure teleportation of an arbitrary quantum state in a qubit, except one point. In the secure quantum teleportation, Alice's announcement of the Bell-state measurement outcome is a necessary step. In the present scheme, instead of her public announcement, Alice distributes her Bell-state measurement outcome to all the quantum information receivers except for Bob. Hence, all the parties except for Bob has essentially formed a group of a quantum secret sharing of classical messages, that is, all the receivers except Bob share securely Alice's measurement outcome if they collaborate. In fact, before Alice distributes his secret messages to All the receivers except for Bob, this group can and should detect whether the quantum channel is attacked by Eve by using the so-called two-measuring-basis method as well as the message authentification method used generally. As for a serious case that there is an insider who may be on one or more receivers and will collaborate with Bob to get Alice's secret messages and thereby they can break away from other receivers's control, their attacks can also be detected by Alice and other receivers in terms of the two-measuring-basis method just and Alice's final message authentification. Further, if they collaborate with Bob, then all $n-1$ receivers can reconstruct the unknown state in Bob's qubit by designating Bob to perform an appropriate unitary operation. The third, in the present paper, only Bell states are used and needed to be identified. It is generally admitted that the preparation and identification of Bell states are much easier than those of multi-particle GHZ states, which are necessary in other schemes [1,2,5,10,13,14]. Hence, the present multiparty SSQI scheme is more feasible with present-day technique [16]. By the way, we also note that, a feasible realization of complete Bell-state analyzer with present-day technique is still far to come.

To summarize, in this paper by using and identifying only Bell states we have proposed a multiparty SSQI scheme. It is unconditionally secure and more feasible with present-day technique.

We are grateful to Professor Baiwen Li for his encouragement. This work is supported by the National Natural Science Foundation of China under Grant No. 10304022.

References

1. M. Hillery, V. Buzk, A. Berthiaume, Phys. Rev. A **59**, 1829 (1999)
2. R. Cleve, D. Gottesman, H.K. Lo, Phys. Rev. Lett. **83**, 648 (1999)
3. A. Karlsson, M. Koashi, N. Imoto, Phys. Rev. A **59**, 162 (1999)
4. D. Gottesman, Phys. Rev. A **61**, 042311 (2000)
5. S. Bandyopadhyay, Phys. Rev. A **62**, 012308 (2000)
6. W. Tittel, H. Zbinden, N. Gisin, Phys. Rev. A **63**, 042301 (2001)

7. V. Karimipour, A. Bahraminasab, Phys. Rev. A **65**, 042320 (2002)
8. H.F. Chau, Phys. Rev. A **66**, 060302 (2002)
9. S. Bagherinezhad, V. Karimipour, Phys. Rev. A **67**, 044302 (2003)
10. L.Y. Hsu, Phys. Rev. A **68**, 022306 (2003)
11. G.P. Guo, G.C. Guo, Phys. Lett. A **310**, 247 (2003)
12. L. Xiao, G.L. Long, F.G. Deng, J.W. Pan, Phys. Rev. A **69**, 052307 (2004)
13. Y.M. Li, K.S. Zhang, K.C. Peng, Phys. Lett. A **324**, 420 (2004)
14. A.M. Lance, T. Symul, W.P. Bowen, B.C. Sanders, P.K. Lam, Phys. Rev. Lett. **92**, 177903 (2004)
15. Y.H. Kim, S.P. Kulik, Y. Shih, Phys. Rev. Lett. **86**, 1370 (2001)
16. M. Zukowski, A. Zeilinger, M.A. Horne, A.K. Ekert, Phys. Rev. Lett. **71**, 4287 (1993)
17. S. Bose, V. Vedral, P.L. Knight, Phys. Rev. A **57**, 822 (1998)
18. L. Hardy, D. Song, Phys. Rev. A **62**, 052315 (2000)
19. J.W. Pan, M. Daniell, S. Gasparoni, G. Weihs, A. Zeilinger, Phys. Rev. Lett. **86**, 4435 (2001)
20. F.G. Deng, G.L. Long, X.S. Liu, Phys. Rev. A **68**, 042317 (2003)
21. C.H. Bennett, G. Brassard, N.D. Mermin, Phys. Rev. Lett. **68**, 557 (1992)
22. H. Inamori, L. Rallan, V. Verdral, J. Phys. A **34**, 6913 (2001)
23. G.L. Long, X.S. Liu, Phys. Rev. A **65**, 032302 (2002)
24. E. Waks, A. Zeevi, Y. Yamamoto, Phys. Rev. A **65**, 052310 (2002)
25. C.H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, W.K. Wotters, Phys. Rev. Lett. **70**, 1895 (1993)