Available online at www.sciencedirect.com
SCIENCE DIRECT®
Physics Letters A 324 (2004) 420–424
PHYSICS LETTERS A
www.elsevier.com/locate/pla

Multiparty secret sharing of quantum information based on entanglement swapping

Yongmin Li, Kuanshou Zhang *, Kunchi Peng

State Key Laboratory of Quantum Optics and Quantum Optics Devices, Institute of Opto-Electronics, Shanxi University, Taiyuan 030006, China

Received 20 February 2004; received in revised form 12 March 2004; accepted 17 March 2004

Communicated by P.R. Holland

Abstract

A protocol of multiparty secret sharing of quantum information based on entanglement swapping is analyzed. In this protocol, Bell states are needed in order to realize the quantum information secret sharing and it is convenient to realize the quantum secret sharing among the members of any subset of users.

PACS: 03.67.Dd; 03.65.Ud

Keywords: Quantum secret sharing; Entanglement swapping

1. Introduction

In classical secret sharing, a secret message can be distributed among N users in such a way that, only by combining their pieces of information can the N users recover the secret message. Recently this concept was generalized to the quantum scenario [1] by using three-particle and four-particle GHZ states and has attracted a great deal of attention in theoretical aspects [2–9], and also in experimental implementation [10]. In [2] Karlsson et al. considered quantum secret sharing using two-particle entanglement. In [3,6] Cleve and coworkers investigated a more general quantum (k, n) threshold scheme and they considered the connection between quantum secret sharing and quantum error-correction code [3]. The quantum version of secret sharing cannot only provide absolute security, but also likely 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 [6], etc.

Entanglement swapping means to entangle quantum systems that have never interacted before [11,12], which has found a number of applications in quantum information [12,13] such as constructing a quantum telephone exchange, speeding up the distribution of entanglement, correcting errors in Bell states, preparing entangled states of a higher number of particles, and secret sharing of classical information.

* Corresponding author.
E-mail address: kuanshou@sxu.edu.cn (K. Zhang).

0375-9601/$ – see front matter
doi:10.1016/j.physleta.2004.03.034

In this Letter, a specially chosen quantum (k, n) threshold secret sharing scheme with $k = n$ based on entanglement swapping is analyzed. The proposed protocol consumes Bell states, and the splitting of quantum information is realized by entanglement swapping, this makes our scheme differing from other known schemes. Also, it is convenient to fulfill the secret sharing among the members of any subset of users by employing entanglement swapping. Comparing with [2] in which Bell states were used for secret sharing of classical secret, our scheme utilizes Bell states for secret sharing of quantum information (an arbitrary two-dimensional quantum state).

The present Letter is organized as follows. In Section 2 we discuss the three-party secret sharing of quantum information based on entanglement swapping. In Section 3 the scheme of three-party secret sharing is generalized to the case of N-party, and the main advantages of this protocol is discussed. Finally, in Section 4 we summarize and conclude.

2. Three-party quantum information secret sharing

For simplicity we will only treat three-party system in this section. Three parties, say, Alice, Bob and Charlie. At first, Alice possesses five qubits: qubits 1, 2, 3, 4, and 5, where qubits 1 and 2, qubits 3 and 4 are prepared in one of the following Bell basis

$$\begin{aligned}\left|\Phi^{\pm}\right\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle \pm |11\rangle\right),\\ \left|\Psi^{\pm}\right\rangle &= \frac{1}{\sqrt{2}}\left(|01\rangle \pm |10\rangle\right).\end{aligned} \tag{1}$$

We assume qubits 1 and 2, qubits 3 and 4 are both in the state $|\Psi^{+}\rangle$, qubit 5 is an unknown qubit that Alice is supposed to sent to Bob and Charlie

$$|\phi\rangle = a|0\rangle + b|1\rangle. \tag{2}$$

Now the combined state of the five qubits is

$$\begin{aligned}|\psi_s\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle_{12} + |10\rangle_{12}\right) \otimes \frac{1}{\sqrt{2}}\left(|01\rangle_{34} + |10\rangle_{34}\right)\\ \otimes \left(a|0\rangle_5 + b|1\rangle_5\right).\end{aligned} \tag{3}$$

We observe that the state $|\psi_s\rangle$ can also be written as

$$\begin{aligned}|\psi_s\rangle = \frac{1}{2\sqrt{2}}\big\{&|\Phi_1\rangle \otimes \left(a|11\rangle_{24} + b|00\rangle_{24}\right)\\ &+ |\Phi_2\rangle \otimes \left(b|11\rangle_{24} + a|00\rangle_{24}\right)\\ &+ |\Phi_3\rangle \otimes \left(a|10\rangle_{24} + b|01\rangle_{24}\right)\\ &+ |\Phi_4\rangle \otimes \left(a|01\rangle_{24} + b|10\rangle_{24}\right)\\ &+ |\Phi_5\rangle \otimes \left(a|11\rangle_{24} - b|00\rangle_{24}\right)\\ &+ |\Phi_6\rangle \otimes \left(b|11\rangle_{24} - a|00\rangle_{24}\right)\\ &+ |\Phi_7\rangle \otimes \left(a|10\rangle_{24} - b|01\rangle_{24}\right)\\ &+ |\Phi_8\rangle \otimes \left(a|01\rangle_{24} - b|10\rangle_{24}\right)\big\},\end{aligned} \tag{4}$$

where the set $\{|\Phi_i\rangle\}$, $i = 1, 2, \ldots, 8$, forms a complete orthonormal basis of the combined Hilbert space of the three spin-1/2 particles (or two-level systems):

$$\begin{aligned}|\Phi_1\rangle &= \frac{1}{\sqrt{2}}\left(|000\rangle_{135} + |111\rangle_{135}\right),\\ |\Phi_2\rangle &= \frac{1}{\sqrt{2}}\left(|001\rangle_{135} + |110\rangle_{135}\right),\\ |\Phi_3\rangle &= \frac{1}{\sqrt{2}}\left(|010\rangle_{135} + |101\rangle_{135}\right),\\ |\Phi_4\rangle &= \frac{1}{\sqrt{2}}\left(|100\rangle_{135} + |011\rangle_{135}\right),\\ |\Phi_5\rangle &= \frac{1}{\sqrt{2}}\left(|000\rangle_{135} - |111\rangle_{135}\right),\\ |\Phi_6\rangle &= \frac{1}{\sqrt{2}}\left(|001\rangle_{135} - |110\rangle_{135}\right),\\ |\Phi_7\rangle &= \frac{1}{\sqrt{2}}\left(|010\rangle_{135} - |101\rangle_{135}\right),\\ |\Phi_8\rangle &= \frac{1}{\sqrt{2}}\left(|100\rangle_{135} - |011\rangle_{135}\right).\end{aligned} \tag{5}$$

Firstly, Alice sends qubits 2 and 4 to Bob and Charlie, respectively. After Alice verifies that Bob and Charlie both receive a qubit, then she performs a GHZ-basis measurement on her qubits 1, 3, and 5 (let the nature of the measurement be such that it projects qubits 1, 3, and 5 to the complete orthonormal basis described by Eq. (5)). From Eq. (4), the state of qubits 2 and 4 becomes a pure entangled state of two particles, due to the multi-particle entanglement swapping. Now the quantum information is transferred to the pure entangled state which is shared between Bob and Charlie, the distribution of quantum information is completed.

The important thing to note is that neither Bob nor Charlie can recover the state $|\phi\rangle$ by any general operations on their respective sides without communicating between themselves. They only have the amplitude information, that is not sufficient since information about the phase is not available. In order to get the phase information, they must cooperate and only one of them can possess the final qubit for the no-cloning theorem [1]. We assume Alice obtains the state $|\Phi_1\rangle$ after her GHZ basis measurement and then she declares it to Bob and Charlie over a public channel. Now the pure entangled state that Bob and Charlie share can be written as

$$|\Psi_{24}\rangle = a|11\rangle_{24} + b|00\rangle_{24}. \tag{6}$$

Similar to Ref. [3], first we rewrite the state $|\Psi_{24}\rangle$ in the following way:

$$|\Psi_{24}\rangle = \frac{1}{\sqrt{2}}\left[\frac{1}{\sqrt{2}}\big(|0\rangle_4 + |1\rangle_4\big)\big(b|0\rangle_2 + a|1\rangle_2\big) + \frac{1}{\sqrt{2}}\big(|0\rangle_4 - |1\rangle_4\big)\big(b|0\rangle_2 - a|1\rangle_2\big)\right]. \tag{7}$$

If Alice designates Bob to reconstruct the quantum state, then Charlie performs a measurement on his qubit in the X basis and the X eigenstates are defined by

$$\big|X^{\pm}\big\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle \pm |1\rangle\big). \tag{8}$$

We assume the measurement result of Charlie is $|\Psi_4\rangle$ and from Eq. (7) the state of qubit 2 will be projected onto the state $|\Psi_2\rangle$

$$|\Psi_4\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle_4 + |1\rangle_4\big),$$
$$|\Psi_2\rangle = \big(b|0\rangle_2 + a|1\rangle_2\big). \tag{9}$$

Now provided Charlie agrees to cooperate with Bob and communicates his outcome to Bob over a public channel. At this stage, Bob can reconstruct the unknown state by appropriately rotating his qubit.

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}|\Psi_2\rangle = a|0\rangle_2 + b|1\rangle_2. \tag{10}$$

It is explicit that the state described by Eq. (10) is exactly the state that Alice has sent to Bob and Charlie. Thus, Bob can reconstruct the state $|\phi\rangle$ with the help of Charlie.

Next we analyze the security of the protocol for a particular eavesdropping. Assuming one of users (say, Bob) is dishonest and he will cooperate with Eve or he is Eve himself. If Bob does not adopt any eavesdropping methods, only when Alice designates him to obtain the state, he can eavesdrop the state and his cheating will go undetected. But the probability is only 50%, still he will get nothing with a probability of 50%. He can also capture the qubit Alice sends to Charlie and then sends Charlie a qubit he has prepared before. By doing so, only when Alice designates him to reconstruct the state, he can get the state $|\phi\rangle$ and this will go undetected. If Alice designates not Bob but Charlie to reconstruct the state, the state reconstructed by Charlie will differ from the state Alice has sent. When Alice and Charlie compare a small part of the states publicly, the eavesdropping can be disclosed.

3. Multi-party generalization of quantum information secret sharing

In Section 2, we have analyzed the three-party quantum information secret sharing based on entanglement swapping, it is easy to be generalized to multi-party case. At first, Alice prepare N same Bell states and the unknown state that will be shared is still given by Eq. (2). Now the state of the system is given by [13]

$$|\Psi_s\rangle = \prod_{m=1}^{N}\left(\prod_{i=1}^{2}|u_{im}\rangle \pm \prod_{i=1}^{2}|u_{im}^c\rangle\right) \otimes \big(a|0\rangle + b|1\rangle\big), \tag{11}$$

where u_{im} is a binary variable $u_{im} \in \{0, 1\}$ and u_{im}^c is its complement defined as $u_{im}^c = 1 - u_{im}$. We suppose the N Bell states are in the state $|\Phi^+\rangle$, so the state of the system can be simplified as

$$|\Psi_s\rangle = \prod_{m=1}^{N}\big(|0_{1m}1_{2m}\rangle + |1_{1m}0_{2m}\rangle\big) \otimes \big(a|0\rangle + b|1\rangle\big). \tag{12}$$

Then Alice sends one of the two qubits of each Bell state to N users, respectively (the qubits which are sent are numbered 2, the rest are numbered 1). After Alice verifies that all of the N users have received a qubit, she performs an $(N + 1)$-particle GHZ basis measurement on her $N + 1$ qubits ($|\phi\rangle$ is numbered

$N+1$). The measurement is such that it projects the $N+1$ particles to the $(N+1)$-particle (spin-1/2) complete orthonormal basis described by Eq. (13):

$$|\Psi_{N+1}\rangle = \prod_{n=1}^{N+1} |u'_{1n}\rangle + (-1)^h \prod_{n=1}^{N+1} |u'^c_{1n}\rangle, \tag{13}$$

where $u'_{1n} \in \{0,1\}$, $u'^c_{1n} = 1 - u'_{1n}$, $h \in \{0,1\}$. After the measurement, the rest N particles are projected to the state of the type

$$\begin{aligned}|\Psi_N\rangle &= \langle \Psi_{N+1} \| \Psi_s \rangle \\ &= C_0 \prod_{m=1}^{N} |u_{2m}\rangle + C_1 \prod_{m=1}^{N} |u^c_{2m}\rangle,\end{aligned} \tag{14}$$

where

$$C_0 = \langle u'_{1(N+1)} | \phi \rangle, \qquad C_1 = (-1)^h \langle u'^c_{1(N+1)} | \phi \rangle,$$
$$u_{2m} = u'^c_{1m}, \qquad u^c_{2m} = u'_{1m}.$$

From Eq. (14) we can see clearly that the state of the rest N particles collapse to a pure entangled state which contains all the information of the state $|\phi\rangle$ after Alice's measurement. Now the distribution of the quantum information is completed. The reconstruction of the state can go like this, Alice publicly declares her measurement results, and assign one user (we call him A) to obtain the state. The rest $N-1$ users perform an X basis measurement on their own qubit. After the measurements the state of the qubit of user A is as follows

$$\begin{aligned}|\Psi_A\rangle &= \prod_{n=1}^{N-1} \left(\langle 0_{2n}| \pm \langle 1_{2n}| \right) \\ &\quad \otimes \left(C_0 \prod_{m=1}^{N} |u_{2m}\rangle + C_1 \prod_{m=1}^{N} |u^c_{2m}\rangle \right) \\ &= C_0 (-1)^p |u_{2N}\rangle + C_1 (-1)^q |u^c_{2N}\rangle,\end{aligned} \tag{15}$$

here, p is the number of event X occur (event X is defined by: $u_{2m} = 1$ and the mth user get a $|X^-\rangle$ measurement result); q is the number of event Y occur (event Y is defined by: $u_{2m} = 0$ and the mth user get a $|X^-\rangle$ measurement result). At this stage, the $N-1$ users tell their measurement results to user A, and user A performs a certain unitary transformation on his qubit according to the information that Alice and the rest $N-1$ users have sent to him (then he can decide the value of $C_0, C_1, p, q, u_{2N}, u^c_{2N}$) and finally reconstructs the state $|\phi\rangle$.

The security of the multi-party secret sharing protocol against particular eavesdropping attack is similar to the three-party case: any eavesdropping can leads to the discrepancy between the state that Alice sends and the state that legitimate user reconstructs. Thus Eve can be detected by publicly comparing a subset of the quantum states.

Comparing with protocols of using directly multi-particle GHZ state [1,3], the advantages of our protocol are as follows [12].

The users can purify partially decohered Bell pairs shared with the information sender Alice to obtain pure shared Bell pairs [14], the problem of decoherence during propagation of the Bell states can then be avoided. After the distribution of quantum information, pure multi-particle entangled states can be obtained by entanglement swapping without the necessity of purifying them.

In the time of emergency, this method can be speedy. During the free time of communication, Alice can supply qubits to the users who have consumed their qubits and ensure everyone shares some Bell states with her. In the time of need, Alice can perform an $(N+1)$-particle GHZ basis measurement on her corresponding N qubits and the unknown state to distribute quantum information. Because one does not know in advance exactly which set of users will need to share a quantum state, for the protocol of using directly multi-particle GHZ state, one should consider all possible combinations of the users and prepare multi-particle entangled states in advance, this is very uneconomical. For a ten-party system, by using our protocol, we only need 9 Bell states. But for the case of directly using multi-particle GHZ state, we should prepare 511 different multi-particle GHZ states. Of course we can prepare the desired GHZ states at the time of need and send them to the users who wish to communicate, but this is time consuming.

4. Conclusion

We present a protocol of multi-party secret sharing of quantum information based on entanglement swapping. In this protocol, Bell states are needed in order to realize the quantum information secret sharing and

it is convenient to realize the quantum secret sharing among the members of any subset of users.

Acknowledgements

This Letter was supported by the National Fundamental Research Program (Grant No. 2001CB309304), the National Natural Science Foundation of China (No. 60238010), the Shanxi Province Young Science Foundation (No. 20031005), and the Shanxi Province Foundation for Returned Overseas Chinese Scholar.

References

[1] M. Hillery, V. Buzek, A. Berthiaume, Phys. Rev. A 59 (1999) 1829.
[2] A. Karlsson, M. Koashi, N. Imoto, Phys. Rev. A 59 (1999) 162.
[3] R. Cleve, D. Gottesman, H.-K. Lo, Phys. Rev. Lett. 82 (1999) 648.
[4] A. Smith, quant-ph/0001087.
[5] S. Bandyopadhyay, Phys. Rev. A 62 (2000) 012308.
[6] D. Gottesman, Phys. Rev. A 61 (2000) 042311.
[7] V. Karimipour, S. Bagherinezhad, A. Bahraminasab, Phys. Rev. A 65 (2002) 042320.
[8] H.F. Chau, Phys. Rev. A 66 (2002) 060302.
[9] S. Bagherinezhad, V. Karimipour, Phys. Rev. A 67 (2003) 044302.
[10] W. Tittel, H. Zbinden, N. Gisin, Phys. Rev. A 63 (2001) 042301.
[11] M. Zukowski, A. Zeilinger, M.A. Horne, A.K. Ekert, Phys. Rev. Lett. 71 (1993) 4287.
[12] S. Bose, V. Vedral, P.L. Knight, Phys. Rev. A 57 (1998) 822.
[13] S. Bose, V. Vedral, P.L. Knight, in: D. Bounmeester, A.K. Ekert, A. Zeilinger (Eds.), The Physics of Quantum Information, Springer, Berlin, 2000.
[14] D. Deutsch, A. Ekert, R. Jozsa, C. Machiavello, S. Popescu, A. Sanpera, Phys. Rev. Lett. 77 (1996) 2818;
C.H. Bennett, H.J. Bernstein, S. Popescu, B. Schumacher, Phys. Rev. A 53 (1996) 2046;
C.H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J.A. Smolin, W.K. Wooters, Phys. Rev. Lett. 76 (1996) 722.