Vol 15 No 10, October 2006
1009-1963/2006/15(10)/2252-04
Chinese Physics
© 2006 Chin. Phys. Soc.
and IOP Publishing Ltd

Secret sharing of quantum information via entanglement swapping*

Zhang Ying-Qiao(张英俏)[a)b)†], Jin Xing-Ri(金星日)[b)], and Zhang Shou(张 寿)[a)b)‡]

[a)] *Center for Condensed-Matter Science and Technology, Harbin Institute of Technology, Harbin* 150001, *China*

[b)] *Department of Physics, College of Science, Yanbian University, Yanji* 133002, *China*

(Received 25 July 2005; revised manuscript received 23 May 2006)

Based on entanglement swapping, a scheme for the secret sharing of an arbitrary two-particle entangled state is proposed. If the controllers do not co-operate with the eavesdropper, the eavesdropper's successful probability decreases with the number of the controllers increasing. In addition, only the Bell-state measurements are required to realize the secret sharing scheme.

Keywords: secret sharing, two-particle entangled state, Bell-state measurements, entanglement swapping
PACC: 0367, 0365

1. Introduction

In the fascinating application of quantum mechanics theory to quantum information, in recent years there have been many interesting developments, such as quantum teleportation,[1−7] quantum dense coding (QDC),[8] quantum key distribution (QKD),[9,10] quantum secure direct communication (QSDC),[11] quantum secret sharing (QSS),[12] and so on. The basic theory of secret sharing, in which usually one dealer and n players are involved, proposed by Shamir[13] and Blakley[14] independently in 1979, is that one dealer wants to distribute secret information to n players, among them t or more than t players can cooperate to reconstruct the secret information, but the remaining $t-1$ or less than $t-1$ players have no knowledge about the secret information even if they cooperate. This is called a (t,n)-threshold scheme.

The theory of secret sharing was first applied to the quantum scenario by Hillery *et al* using Greenberger–Horne–Zeilinger (GHZ) states.[12] Since then, various methods of implementing the quantum information secret sharing have been proposed.[15−26] Entanglement swapping, as an important method in quantum information process,[27] has already been applied to quantum secret sharing.[28−30] Zhang and Man[29] and Li *et al*[30] proposed the QSS protocols via entanglement swapping using the Bell-state measurements and GHZ-basis measurements, respectively. Deng *et al*[31] suggested a scheme for the multiparty quantum state sharing of an arbitrary two-particle entanglement with Einstein–Podolsky–Rosen (EPR) pairs, in which multi-particle GHZ-state measurements are necessary.

Here we propose a scheme for the quantum secret sharing of an arbitrary two-particle entangled state via entanglement swapping using the Bell-state measurements. A comparison of our protocol with the scheme in Ref.[31] shows that the former consumes a few particles and performs the easy Bell-state measurements instead of the difficult-to-perform multi-particle GHZ-state measurements. In Section 2, the QSS protocol with two agents is discussed in detail, and the generalization to N agents is given in Section 3. A concise summary of the present study is given in Section 4.

2. Secret sharing of an arbitrary two-particle entanglement with two agents

We consider a system consisting of Alice, Bob, and Charlie (see Fig.1). Bob and Charlie are Alice's

*Project supported by the National Natural Science Foundation of China (Grant No 60261002) and the Science Foundation of Yanbian University (Grant No 2005-20).
†E-mail: yqzhang@ybu.edu.cn
‡E-mail: szhang@ybu.edu.cn

two agents in a remote place. Particles p, q, 1 and 3 belong to Alice, particles 4 and 5 belong to Charlie, and particles 2 and 6 belong to Bob. The state of particles p and q, an arbitrary two-particle entangled state, which Alice wants to send to Bob and Charlie, is

$$|\Psi\rangle_{pq} = (\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle)_{pq}, \quad (1)$$

where α, β, γ, and δ are unknown coefficients, and they satisfy $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$. The states of particles 1 and 2, particles 3 and 4 and particles 5 and 6 are all in EPR pairs. An EPR pair is in one of the following four Bell states:

$$|\psi^{\pm}\rangle_{mn} = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)_{mn}, \quad (2)$$

$$|\phi^{\pm}\rangle_{mn} = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)_{mn}, \quad (3)$$

where $|0\rangle$ and $|1\rangle$ are the eigenvectors of the operator σ_z. Here we suppose that all the EPR pairs are in the states of $|\psi^+\rangle_{mn}$.

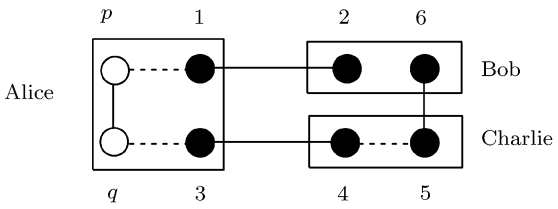


Fig.1. Illumination of particles distribution. Particles p, q, 1, and 3 belong to Alice, particles 4 and 5 belong to Charlie, and particles 2 and 6 belong to Bob. The bold lines connect the two particles in an EPR pair or an arbitrary two-particle entangled state. The dashed lines connect the two particles on which the Bell-state measurements are to be performed (Supposing that Bob wants to recover the unknown state).

The joint state of the eight particles can be expressed as

$$|\Psi\rangle = |\Psi\rangle_{pq} \otimes |\psi^+\rangle_{12} \otimes |\psi^+\rangle_{34} \otimes |\psi^+\rangle_{56}. \quad (4)$$

Firstly, Alice performs the Bell-state measurements on the particles p, 1, and q, 3, respectively, and then she informs Bob and Charlie of her measurement results via a classical communication. If Alice's measurement results are $|\psi^+\rangle_{p1}$ and $|\phi^+\rangle_{q3}$, the states of particles 2, 4, 5, and 6 collapse into

$$\begin{aligned}|\Psi\rangle_{2456} =& \frac{1}{4}(\alpha|01\rangle + \beta|00\rangle + \gamma|11\rangle \\ &+ \delta|10\rangle)_{24} \otimes |\psi^+\rangle_{56}. \end{aligned} \quad (5)$$

So the quantum information has been transferred to Bob and Charlie successfully via entangled swapping. The distribution of quantum information is completed.

We can see that neither Bob nor Charlie can recover the state $|\Psi\rangle_{pq}$ by performing any local operation themselves without communication between themselves. If they agree to cooperate with each other, only one of them can recover the desired state for the no-cloning theorem. We rewrite the state in Eq.(5) as

$$\begin{aligned}|\Psi\rangle_{2456} =& \frac{1}{4\sqrt{2}}[|\psi^+\rangle_{45}(\beta|00\rangle + \delta|10\rangle \\ &+ \alpha|01\rangle + \gamma|11\rangle)_{26} \\ &+ |\psi^-\rangle_{45}(\beta|00\rangle + \delta|10\rangle - \alpha|01\rangle - \gamma|11\rangle)_{26} \\ &+ |\phi^+\rangle_{45}(\beta|01\rangle + \delta|11\rangle + \alpha|00\rangle + \gamma|10\rangle)_{26} \\ &+ |\phi^-\rangle_{45}(\beta|01\rangle + \delta|11\rangle - \alpha|00\rangle - \gamma|10\rangle)_{26}]. \end{aligned} \quad (6)$$

If any one of them (say, the first one) is assigned to recover the state $|\Psi\rangle_{pq}$, the second one needs to perform the Bell-state measurement on his two particles and informs the first one of his measurement result. According to the second one's measurement result, the first one can recover the state.

We describe the process in detail. We suppose that Alice assigns Bob to recover the quantum state $|\Psi\rangle_{pq}$, then Charlie must perform the Bell-state measurement on the particles 4, 5, and inform Bob of his measurement result via a classical communication. If Charlie's measurement result is $|\psi^-\rangle_{45}$, the states of particles 2 and 6 collapse into

$$|\Psi\rangle_{26} = (\beta|00\rangle + \delta|10\rangle - \alpha|01\rangle - \gamma|11\rangle)_{26}. \quad (7)$$

Under this condition, Bob can recover the unknown state by performing the local operation $I_x^2 \otimes \mathrm{i}\sigma_y^6$ on particles 2 and 6

$$I_x^2 \otimes \mathrm{i}\sigma_y^6 |\Psi\rangle_{26} = (\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle)_{26}. \quad (8)$$

So Bob recovers the state $|\psi\rangle_{pq}$ with the help of Charlie.

We continue to discuss the security of the scheme. Suppose that there exists an eavesdropper (either Bob or Charlie). The eavesdropper (say, Bob) wants to eavesdrop Alice's information, with no cheat detected. If Alice assigns Bob to receive the state and Charlie agrees to cooperate with Bob, then Bob can eavesdrop the secret with a successful probability of 1, and the cheat will not be detected. If Alice assigns Bob to

receive the state and Charlie does not agree to cooperate with Bob, so there appear two possibilities: (I) Charlie does not tell Bob his measurement result, in this case Bob can also eavesdrop the state, but the successful probability is only $\frac{1}{4}$, he will receive nothing with a probability of $\frac{3}{4}$. (II) Charlie lies about his measurement result to Bob or he does not make a measurement on his two particles, in this case Bob cannot recover the state with a probability of 1. On the other hand, Alice and Charlie can prevent Bob from obtaining any information about the secret using a special technique. This case is analysed in Ref.[32].

3. Secret sharing of an arbitrary two-particle entanglement with N agents

It is easy to generalize the secret sharing scheme to the case of N agents. Supposing that Charlie$_i$ ($i = 1, 2, \ldots, N-1$) and Bob are Alice's N agents in a remote place. Alice still possesses four particles, p, q, 1, and 3. Each agent possesses a pair of particles.

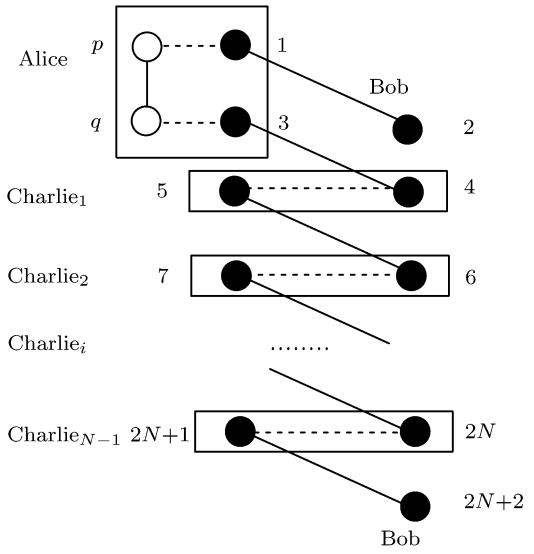


Fig.2. Illumination of the particles distribution. Particles p, q, 1, and 3 belong to Alice, particles 4 and 5 belong to Charlie$_1$, and particles 6 and 7 belong to Charlie$_2$,..., particles $2N$ and $2N+1$ belong to Charlie$_{N-1}$. Particles 2 and $2N+2$ belong to Bob. The bold lines connect the two particles in an EPR pair or an arbitrary two-particle entangled state. The dash lines connect the two particles on which the Bell-state measurements are to be performed (Supposing that Bob is designed to recover the unknown state).

The particle distribution is described in Fig.2 in detail. An arbitrary two-particle entangled state that Alice wants to transfer to Charlie$_i$ and Bob is still in the form of Eq.(1). $N+1$ pairs of particles $2j+1$, $2j+2$ ($j = 0, 1, 2, \ldots, N$) are all in the states of $|\psi^+\rangle_{mn}$.

The joint state of the particles p, q, 1, 2,..., $2N+2$ can be expressed as

$$|\Psi\rangle = |\Psi\rangle_{pq} \otimes \prod_{j=0}^{N} |\psi^+\rangle_{2j+1,2j+2}. \tag{9}$$

Firstly, Alice performs the Bell-state measurements on particles p, 1 and q, 3, respectively, and publishes the measurement results to Charlie$_i$ and Bob via a classical communication. Then the N agents can obtain the state of their $2N$ particles. And the state contains all the information of $|\Psi\rangle_{pq}$. Any one of the N agents can recover the unknown state if the remaining $N-1$ agents agree to cooperate with him. We suppose that Bob is assigned to recover the state $|\Psi\rangle_{pq}$. Then the $N-1$ controllers, Charlie$_i$ ($i = 1, 2, \ldots, N-1$), need to perform the Bell-state measurements on their $N-1$ pairs of particles, respectively, and inform Bob of the measurement results via the classical communication. According to the measurement results from Alice and the $N-1$ controllers, Bob can recover the state $|\Psi\rangle_{pq}$ by performing appropriate local operations on his two particles 2, $2N+2$.

The security of the secret sharing scheme with N agents is the same as that in Section 2. We discuss only the security for a special case. We suppose that Bob is the eavesdropper and Alice has already published her measurement results to the N agents. If any one of the $N-1$ controllers does not agree to inform Bob of his measurement result, Bob has a probability of $\frac{1}{4}$ to eavesdrop the secret. And if any ϵ ($\epsilon \leq N-1$) people from among the $N-1$ controllers do not agree to inform Bob of their measurement results, Bob has a probability of $\left(\frac{1}{4}\right)^{\epsilon}$ to eavesdrop the secret. When ϵ is large enough, Bob's successful eavesdropping probability approaches zero. So Bob's successful eavesdropping probability decreases with the number of the controllers increasing if Bob cannot obtain any help from the controllers.

4. Summary

We have proposed a scheme for the secret sharing of an arbitrary two-particle entangled state via

entanglement swapping. We find that eavesdropper's successful eavesdropping probability decreases with the number of the controllers increasing if the eavesdropper can not receive the help from the controllers. When the number of the controllers is large enough, the eavesdropper's successful eavesdropping probability approaches zero. In the present scheme, only the Bell-state measurements are required in order to realize the secret sharing.

References

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

[2] Bouwmeester D, Pan J W, Mattle K, Eible M, Weinfurter H and Zeilinger A 1997 *Nature* **390** 575

[3] Cai X H 2003 *Chin. Phys.* **12** 1066

[4] Zheng Y Z, Gu Y J, Wu G C and Guo G C 2003 *Chin. Phys.* **12** 1070

[5] Dai H Y, Li C Z and Chen P X 2003 *Chin. Phys.* **12** 1354

[6] Song T Q 2004 *Acta. Phys. Sin.* **53** 3358 (in Chinese)

[7] Dai H Y, Chen P X, Liang L M and Li C Z 2004 *Acta Phys. Sin.* **53** 441 (in Chinese)

[8] Bennett C H and Wiesner S J 1992 *Phys. Rev. Lett.* **69** 2881

[9] Zhang Q, Tang C J and Zhang S Q 2002 *Acta Phys. Sin.* **51** 1439 (in Chinese)

[10] Yang L, Wu L A and Liu S H 2002 *Acta Phys. Sin.* **51** 2446 (in Chinese)

[11] Beige A, Englert B G, Kurtsiefer C and Weinfurter H 2002 *Acta Phys. Pol.* A **101** 357

[12] Hillery M, Bužek V and Berthiaume A 1999 *Phys. Rev.* A **59** 1829

[13] Shamir A 1979 *Commun. ACM* **22** 612

[14] Blakely G 1979 *Proc. AFIPS* **48** 313

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

[16] Gottesman D 2000 *Phys. Rev.* A **61** 042311

[17] Chau H F 2002 *Phys. Rev.* A **66** 060302

[18] Bagherinezhad S and Karimipour V 2003 *Phys. Rev.* A **67** 044302

[19] Scarani V and Gisin N 2001 *Phys. Rev. Lett.* **87** 117901

[20] Lance A M, Symul T, Bowen W P, Sanders B C and Lam P K 2004 *Phys. Rev. Lett.* **92** 177903

[21] Karlsson A, Koashi M and Imoto N 1999 *Phys. Rev.* A **59** 162

[22] Bandyopadhyay S 2000 *Phys. Rev.* A **62** 012308

[23] Karimipour V, Bahraminasab A and Bagherinezhad S 2002 *Phys. Rev.* A **65** 042320

[24] Guo G P and Guo G C 2003 *Phys. Lett.* A **310** 247

[25] Xiao L, Long G L, Deng F G and Pan J W 2004 *Phys. Rev.* A **69** 052307

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

[27] Zhan Y B 2004 *Chin. Phys.* **13** 1801

[28] Zhang Y Q, Jin X R and Zhang S 2005 *Phys. Lett.* A **341** 380

[29] Zhang Z J and Man Z X quant-ph/0406103

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

[31] Deng F G, Li X H, Li C Y, Zhou P and Zhou H Y 2005 *Phys. Rev.* A **72** 044301

[32] Deng F G, Zhou H Y and Long G L 2005 *Phys. Lett.* A **337** 329