Vol 18 No 4, April 2009
1674-1056/2009/18(04)/1333-05

Chinese Physics B

© 2009 Chin. Phys. Soc.
and IOP Publishing Ltd

Participant attack on quantum secret sharing based on entanglement swapping*

Song Ting-Ting(宋婷婷)[a)b)†], Zhang Jie(张 劼)[c)], Gao Fei(高 飞)[a)],
Wen Qiao-Yan(温巧燕)[a)], and Zhu Fu-Chen(朱甫臣)[d)]

[a)] *State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*

[b)] *State Key Laboratory of Integrated Services Network, Xidian University, Xi'an* 710071, *China*

[c)] *School of Science, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*

[d)] *National Laboratory for Modern Communications, P.O. Box* 810, *Chengdu* 610041, *China*

(Received 8 July 2008; revised manuscript received 5 August 2008)

The security of quantum secret sharing based on entanglement swapping is revisited and a participant attack is presented. In this attack two dishonest agents together can illegally recover the secret quantum state without the help of any other controller, and it will not be detected by any other users. Furthermore, by modifying the distribution process of particles and adding a detection step after each distribution process, we propose an improved protocol which can resist this kind of attack.

Keywords: quantum secret sharing, entanglement swapping, the Bell measurement, two-particle entangled state

PACC: 0367, 0365

Entanglement, the root of Bell theorem, is usually considered to be a consequence of some interaction among the particles in their common past. Entanglement swapping (ES),[1] which means entangling with particles in set S by appropriately projecting other particles previously not entangled with particles of S has been found to have a number of applications in quantum information such as constructing the quantum teleportation[2] speeding up the distribution of quantum key[3−5] correcting errors in Bell states, and generalizing multiparticle entangled states.[6]

The theory of quantum secret sharing (QSS), which had been proposed first by Hillery *et al* [7] through using Greenberger–Horne–Zeilinger (GHZ) states, was introduced from classical (t, n) threshold scheme. In the same year, Richard *et al* [8] proposed how to share a quantum secret state.[8] Since then, many protocols about QSS have been proposed.[9−15] As an important property of entanglement, the ES has been extensively applied to secret sharing.[16,17] In a recent paper, Zhang *et al* [18] proposed a scheme for the secret sharing of an arbitrary two-particle entangled state. For simplicity, we call this scheme ZJZ protocol hereafter. Its security under several kinds of attacks was proved. And it claimed that the eavesdropper's successful probability decreased with the number of the controllers increasing. However, we point out that it is not secure under a particular strategy, i.e. the participant attack[19−21] in which Bob can illegally obtain Alice's secret quantum state with the help of only one controller without introducing any error.

To start with, we give a brief description of ZJZ protocol[18] in the case of N agents. Here we use the same notations and scenarios as those in Ref.[18]. Bob and Charlie$_i$ $(i = 1, 2, \ldots, N-1)$ are Alice's N agents. Each participant possesses a pair of particles which is in the state $|\Psi^+\rangle$. $|\Psi^+\rangle$ is one of the following four Bell states:[18]

$$|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle),$$
$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle). \quad (1)$$

And the arbitrary two-particle entangled state which

*Project supported by the National High Technology Research and Development Program of China (Grant No 2006AA01Z419), the Major Research Plan of the National Natural Science Foundation of China (Grant Nos 90604023, 60873191 and 60821001), the National Laboratory for Modern Communications Science Foundation of China (Grant No 9140C1101010601), the Natural Science Foundation of Beijing, China (Grant No 4072020), and the Integrated Service Network Open Foundation.

†Corresponding author. E-mail: songtingting@bupt.cn

Alice wants to send to N agents is

$$|\Psi\rangle_{pq} = (\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle)_{pq}, \quad (2)$$

where α, β, γ and δ are unknown coefficients and satisfy $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$. The joint system of the particles $p, q, 1, 2, \ldots, 2N+2$ is in the form of

$$|\Psi\rangle = |\Psi\rangle_{pq} \otimes \prod_{i=0}^{N} |\Psi^+\rangle_{2i+1,2i+2}. \quad (3)$$

After the distribution process of the particles, Alice possesses four particles p, q, 1 and 3. Particles $2i+2$, $2i+3$ belong to Charlie$_i$ ($i = 1, 2, \cdots, N-1$), and particles 2, $2N+2$ belong to Bob. All participants detect whether the eavesdropper exists in the distributing particle process. A particular description is as shown in Ref.[18].

The distribution of particles has been described hereinbefore. Now we introduce the process of the sharing secret. Alice performs Bell measurements on particles p, 1 and particles q, 3 respectively, and announces the measurement results to Bob and Charlie$_i$ by using a public channel. As indicated in Ref.[18], we also suppose that Bob is assigned to recover the state $|\Psi\rangle_{pq}$. Then the remaining $N-1$ controllers, Charlie$_i$, perform Bell measurements on their $N-1$ pairs of particles respectively, and they all tell Bob the measurement results via the classical channels. 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 and $2N+2$.

Based on the security of all the particles controlled by the N agents, the ZJZ protocol proves that Bob cannot eavesdrop the secret state alone without being detected if Bob is assigned to acquire the secret state. But the situation where there are two dishonest users is overlooked. We will show that two dishonest agents could illegally achieve the secret state.

Now we describe how Bob and Charlie$_1$ can illegally obtain the secret quantum state. After the secure distribution process of the particles, Alice performs Bell measurements on particles p, 1 and particles q, 3 and announces the measurement results through the classical channel. If Alice's measurement results are in states of $|\Psi^+\rangle_{p1}$ and $|\Phi^+\rangle_{q3}$, the state of other particles would be projected onto

$$|\Psi\rangle_{2,4,5,\ldots,2N+2} = (\alpha|01| + \beta|00| + \gamma|11| + \delta|10|)_{24} \otimes \prod_{i=2}^{N} |\Psi^+\rangle_{2i+1,2i+2}. \quad (4)$$

At an appropriate time, if Charlie$_1$ cooperates with Bob and sends particle 4 to Bob, Bob just performs σ_x on particle 4, and then particles 2 and 4 would be in state $|\Psi\rangle_{pq}$. So Bob obtains the secret state in an illegal way. In the ZJZ protocol, the process of detection aims to detect whether the particles have securely arrived at each agent. Our strategy is performed after this process, so it cannot be detected by other users. In a word, our strategy can successfully attack the ZJZ protocol.

In order to avoid the participant attack, we present an improved version of ZJZ protocol. We also suppose that Alice wants to transmit the arbitrary two-particle state to Bob as done in Eq.(2). Then the modified protocol is described as follows:

(i) Alice prepares the states $|\Psi^+\rangle_{12}$, $|\Psi^+\rangle_{34}$, …, $|\Psi^+\rangle_{2N+1,2N+2}$ and $|\Psi^+\rangle_{34}$.

(ii) Alice performs Bell measurements on particles 2, 5 and particles 4, 7, and then sends particles 4, 5 to Charlie$_1$. Charlie$_1$ chooses one of the following two modes, i.e (a) the checking mode (with probability c) and (b) the message mode. In mode (a), i.e. in the checking mode, Charlie$_1$ randomly chooses one of the bases $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$ to separately measure particle 4 and particle 5. After Charlie$_1$ has told Alice the measurement bases and results of the two particles, Alice separately measures particles 7 and 2 by using the same measurement bases as those for particles entangling with them (i.e. particle 4 and particle 5 respectively). Then Alice compares their measurement results and detects the eavesdropping. If the results satisfy the expected correlations, the particles were not eavesdropped when they were transmitted in the quantum channel. Otherwise eavesdropping exists and Alice aborts this communication. In mode (b) i.e. in the message mode Alice measures the Bell operator on particles 2 and 7.

(iii) Alice performs Bell measurement on particles 6 and 9, and then sends particles 6 and 7 to Charlie$_2$. Analogously to Charlie$_1$, Charlie$_2$ also has two choices, i.e. (a) the checking mode (with probability c), where Alice and Charlie$_2$ perform local measurements on particles 6 and 9, 7 and 2, and compare the measurement results to detect eavesdropping (the detail of this process is similar to the above detecting steps in (ii)), and (b) the message mode where Alice performs Bell measurement on particles 2 and 9.

(iv) The next procedures for Charlie$_3$, Charlie$_4$, … and Charlie$_{N-1}$ are analogous to that for Charlie$_2$. For example, for Charlie$_{i-1}$, Alice performs

Bell measurement on particles $2i$ and $2i+3$, and sends particles $2i$ and $2i+1$ to Charlie$_{i-1}$. Charlie$_{i-1}$ also has two choices: (a) the checking mode (with probability c) and (b) the message mode. If he chooses the message mode, Alice would measure particles 2 and $2i+3$ by using the Bell basis. For Charlie$_{N-1}$, Alice measures particles $2N$ and 1, and sends particles $2N$ and $2N+1$ to Charlie$_{N-1}$. The next process is similar to other agents.

(v) Finally, Alice makes particles $2N+2$ and 3 project onto the Bell basis, and sends particles 2 and $2N+2$ to Bob. Similarly, Bob has two choices: (a) the checking mode (with probability c) and (b) the message mode. If there is no eavesdropping, Alice performs Bell measurements on particles p and 1, q and 3, and announces the results to the N agents.

If the controllers agree to the fact that Bob can recover the original arbitrary state at the moment, they would measure the Bell operator on their particles and inform Bob of the measurement results. According to their results, Bob will recover the state through performing a unitary operation on the corresponding particle.

To describe the improved protocol more clearly, here we give a particular example of this protocol with four users: Alice, Charlie$_1$, Charlie$_2$ and Bob.

(i) Alice prepares the states $|\Psi^+\rangle_{12}$, $|\Psi^+\rangle_{34}$, $|\Psi^+\rangle_{56}$ and $|\Psi^+\rangle_{78}$.

(ii) Alice executes Bell measurements on particles 5, 2 and particles 7, 4, and sends particles 5, 4 to Charlie$_1$. Charlie$_1$ chooses one of the following procedures i.e. (a) the checking mode (with probability c) and (b) the message mode. In procedure (a), i.e. in the message mode, Charlie$_1$ randomly chooses one of the bases $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$ to separately measure particle 5 and particle 4. After Charlie$_1$ has told Alice the measurement bases and results of the two particles, Alice measures the corresponding particles (i.e. particle 2 and particle 7) by using the same measurement bases. Then Alice compares their measurement results and detects the eavesdropping. If the results do not satisfy the expected correlations, the eavesdropping exists and Alice aborts this communication. In procedure (b), i.e. in the message mode Alice performs Bell measurement on particles 7 and 2.

(iii) Alice performs Bell measurement on particles 1 and 6, and then sends particles 7 and 6 to Charlie$_2$. The next step, including both the checking mode and the message mode, is analogous to that for Charlie$_1$. In particular, in the message mode Alice performs Bell measurement on particles 1 and 2.

(iv) Alice measures particles 3 and 8 by using the Bell basis, and then sends particles 2 and 8 to Bob. Analogously to Charlie$_2$, Bob also has two choices, i.e. the checking mode and the message mode. If all the channels are secure, Alice executes Bell measurements on particles p, 1 and particles q, 3, and announces the results via the classical communication. At some appropriate time, other controllers would cooperate with each other to make Bob recover the secret state.

After ascertaining that all the channels are secure, Alice measures the Bell operator on particles p, 1 and q, 3 and announces the measurement results. Without loss of generality, suppose that particles p, 1 and q, 3 are in states of $|\Psi^+\rangle_{p1}$ and $|\Psi^+\rangle_{q3}$. Charlie$_1$ Charlie$_2$ perform Bell measurements on their particles, and announce their results to Bob. Suppose they are in states of $|\Phi^+\rangle_{54}$ and $|\Psi^+\rangle_{76}$, then Bob will know that the system of particles 4, 5, 6, 7, 8 and 2 collapses into

$$|\Psi\rangle_{456782} = (\alpha|01\rangle + \beta|00\rangle + \gamma|11\rangle + \delta|10\rangle)_{28} \otimes |\Phi^+\rangle_{54} \otimes |\Psi^+\rangle_{76} \tag{5}$$

and can recover the unknown state by performing the local operation $I \otimes \sigma_x$ on particles 2 and 8

$$I \otimes \sigma_x |\Psi\rangle_{28} = (\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle)_{28}. \tag{6}$$

Similarly, whatever the agents' results are, Bob can recover the arbitrary state $|\Psi\rangle_{pq}$ with the help of Charlie$_1$ and Charlie$_2$.

Because only Charlie$_1$ knows the result of particles 5 and 4, and after each step Alice would measure some particles, the information about the state would be divided into some parts. Only when every agent cooperates with each other can the state be recovered. For example, Bob and Charlie$_1$ are two dishonest agents. According to our protocol, particle 2 and particle 4 are not entangled, so they are not changed into the secret state under any local operation, even though Charlie$_1$ submits particle 4 to Bob. So the modified protocol could resist the participant attack.

In order to validate the security of the modified protocol, we consider some other attack strategies, i.e. (a) intercept–resend attack and (b) auxiliary particle attack. In strategy (a), i.e. in intercept–resend attack, dishonest participants or eavesdroppers want to acquire some information about the transmitting particles by this attack strategy. Suppose that Bob intercepts the particles from Alice to Charlie$_1$. If he performs Bell measurement on particles 4, 5, particle 5 and 2 would be not entangled with each other. So in the checking mode Bob would be detected. If he randomly chooses one of the bases $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$ to separately measure particles 4 and 5, and Charlie$_1$ uses the conjugated basis to the moment, Bob also would be detected. So though Bob can acquire some information through using this attack, he would be detected. In strategy (b) i.e. in auxiliary particle attack dishonest participant also wants to acquire a knowledge of particles submitted. When Alice sends particles 4 and 5 to Charlie$_1$, Bob obtains auxiliary particles separately. Suppose that Alice's measurement results are in states of $|\Phi^+\rangle_{52}$ and $|\Psi^+\rangle_{74}$, and the system will be

$$\begin{aligned} &\left|\Phi^+\right\rangle_{52} \otimes \left|\Psi^+\right\rangle_{74} \otimes |00\rangle_{5_1 4_1} \\ &= (|01\rangle + |10\rangle)_{52} \otimes |0\rangle_{5_1} \otimes (|00\rangle + |11\rangle)_{74} \otimes |0\rangle_{4_1} . \end{aligned} \tag{7}$$

Then Bob performs CNOT operation: particle 5 is source and particle 5_1 is target; particle 4 is source and particle 4_1 is target. And then the system changes into

$$\begin{aligned} |\Psi\rangle_{525_1744_1} &= (|010\rangle + |101\rangle)_{525_1} \otimes (|000\rangle + |111\rangle)_{744_1} \\ &= |010000\rangle_{525_1744_1} + |101000\rangle_{525_1744_1} + |010111\rangle_{525_1744_1} + |101111\rangle_{525_1744_1} \\ &= |01\rangle_{72}|00\rangle_{54}|00\rangle_{5_14_1} + |00\rangle_{72}|10\rangle_{54}|10\rangle_{5_14_1} + |11\rangle_{72}|01\rangle_{54}|01\rangle_{5_14_1} + |10\rangle_{72}|11\rangle_{54}|11\rangle_{5_14_1} \\ &= \left(\left|\Phi^+\right\rangle_{72}\left|\Psi^+\right\rangle_{54} + \left|\Phi^-\right\rangle_{72}\left|\Psi^-\right\rangle_{54}\right)\left|\Psi^+\right\rangle_{5_14_1} + \left(\left|\Phi^+\right\rangle_{72}\left|\Psi^-\right\rangle_{54} + \left|\Phi^-\right\rangle_{72}\left|\Psi^+\right\rangle_{54}\right)\left|\Psi^-\right\rangle_{5_14_1} \\ &\quad + \left(\left|\Psi^+\right\rangle_{72}\left|\Phi^+\right\rangle_{54} - \left|\Psi^-\right\rangle_{72}\left|\Phi^-\right\rangle_{54}\right)\left|\Phi^+\right\rangle_{5_14_1} \\ &\quad + \left(\left|\Psi^+\right\rangle_{72}\left|\Phi^-\right\rangle_{54} - \left|\Psi^-\right\rangle_{72}\left|\Phi^+\right\rangle_{54}\right)\left|\Phi^-\right\rangle_{5_14_1} . \end{aligned} \tag{8}$$

If the states of particles 5, 2 and particles 7, 4 are assured, according to expression (8), there is a probability of 1/2 with which Bob cannot introduce errors. Bob can acquire some information when he measures the auxiliary particles. In our protocol, Bob only needs 2 bit information to recover the secret state. Each controller would publish 2-bit information about their measurement results. In the 2 bits, there is only 1 bit useful to Bob. And in the auxiliary particle attack, Bob only obtains the redundant information about each controller, while the redundant information is not useful for recovering the secret state. Above all, our protocol can resist this attack.

In summary, we have reviewed the ZJZ protocol which is based on entanglement swapping and presented a participant attack on it. In this attack two dishonest agents cooperating with each other can illegally recover the secret quantum state $|\Psi\rangle_{pq}$ without the help of any other controller, and it will not be detected by any other users. Furthermore, by modifying the distribution process of particles, we propose an improved protocol which can resist the participant attack and some other attacks.

References

[1] Zukowski M, Zeilinger A and Horne M A 1993 *Phys. Rev. Lett.* **71** 4287

[2] Bennett C H and DiVincenzo D P 2000 *Nature* **404** 247

[3] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing* (New York: IEEE Press) 175

[4] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[5] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121
[6] Bose S, Vedral V and Knight P L 1998 *Phys. Rev.* A **57** 822
[7] Hillery M, Buzek V and Berthiaume A 1999 *Phys. Rev.* A **59** 1829
[8] Cleve R, Gottesman D and Lo H K 1999 *Phys. Rev. Lett.* **83** 648
[9] Cabello A 2000 *Phys. Rev.* A **61** 052312
[10] Zhang Y S, Li C F and Guo G C 2000 *Phys. Rev.* A **61** 052312
[11] Cabello A 2001 *Phys. Rev.* A **63** 036301
[12] Cabello A 2001 *Phys. Rev.* A **64** 024301
[13] Qin S J, Gao F, Wen Q Y and Zhu F C 2007 *Phys. Rev.* A **76** 062324
[14] Deng F G, Li X H, Li C Y, Zhou P and Zhou H Y 2005 *Phys. Rev.* A **72** 044301
[15] Chen P, Deng F G and Long G L 2007 *Prog. Nat. Sci.* **17** 26
[16] Li Y M, Zhang K S and Peng K C 2004 *Phys. Lett.* A **324** 420
[17] Zhang Y Q, Jin X R and Zhang S 2005 *Phys. Lett.* A **341** 380
[18] Zhang Y Q, Jin X R and Zhang S 2006 *Chin. Phys.* **15** 2252
[19] Gao F, Qin S J and Wen Q Y 2007 *Quantum Inf. Comput.* **7** 329
[20] Lin S, Gao F, Guo F Z, Wen Q Y and Zhu F C 2007 *Phys. Rev.* A **76** 036301
[21] Gao F, Wen Q Y and Zhu F C 2007 *Phys. Lett.* A **360** 748