Vol 18 No 4, April 2009
1674-1056/2009/18(04)/1342-04
Chinese Physics B
© 2009 Chin. Phys. Soc.
and IOP Publishing Ltd

Proof of the insecurity of quantum secret sharing based on the Smolin bound entangled states*

Yu Ya-Fei(於亚飞) and Zhang Zhi-Ming(张智明)†

Laboratory of Photonic Information Technology, School of Information and Photoelectronic Science and Engineering, South China Normal University, Guangzhou 510006, China

(Received 11 August 2008; revised manuscript received 2 September 2008)

This paper reconsiders carefully the possibility of using the Smolin bound entangled states as the carrier for sharing quantum secret. It finds that the process of quantum secret sharing based on Smolin states has insecurity though the Smolin state was reported to violate maximally the two-setting Bell-inequality. The general proof is given.

Keywords: quantum secret sharing, Smolin bound entangled state
PACC: 0367

1. Introduction

The principle of quantum mechanics provides us quantum cryptography,[1] a technique permitting parties to communicate over an open channel in a secure way, which has been extensively explored from the theoretical and experimental perspectives. Quantum key distribution (QKD)[2] is the most promising branch of quantum cryptography, dealing with the secure communication between two parties. The problem of security is mainly to prevent eavesdropping of an active external. There exists a link between the security of a QKD protocol against individual attacks by the eavesdropper and the violation of some Bell's inequality of a shared quantum state.[3] The further researches show the existence of strong connection between the amount of pure entanglement and the private key which can be distilled from the shared quantum state.[4−7] Extending the secure communication to more than two parties, we consider quantum secret sharing (QSS).[8−10] In QSS, both the onslaught of an eavesdropper and the participant's attack threaten the security. There seems to exist the relation between security and the violation of some Bell's inequality.[11] It was argued that a strong violation of multiqubit Bell inequality[12] by the state that acts as the carrier in secret sharing can be a criterion for security of the secret sharing against individual attacks by an eavesdropper.[13] Here, however, we give an example that though Smolin bound entangled state, the carrier state, maximally violate the two-setting Bell inequality, the protocol of QSS with the Smolin states is insecure against the internal attack. We prove the insecurity in Section 2. The conclusion is given in Section 3.

2. Proof of the insecurity of QSS with the Smolin states

The generalized Smolin bound entangled state[14,15] can be expressed in a recursive form,

$$\rho_4 = \frac{1}{4}\sum_{m=0}^{3} U_2^{(m)}\rho_2 U_2^{(m)} \otimes U_2^{(m)}\rho_2 U_2^{(m)}, \ldots, \tag{1}$$

$$\rho_{2n} = \frac{1}{4}\sum_{m=0}^{3} U_{2(n-1)}^{(m)}\rho_{2(n-1)}U_{2(n-1)}^{(m)} \otimes U_2^{(m)}\rho_2 U_2^{(m)}, \tag{2}$$

where

$$\rho_2 = \left|\Psi^-\right\rangle\left\langle\Psi^-\right| = \frac{1}{2}(|0\rangle_z|1\rangle_z - |1\rangle_z|0\rangle_z)(\langle 0|_z\langle 1|_z - \langle 1|_z\langle 0|_z)$$

with $|0\rangle_z$ and $|1\rangle_z$ being the eigenstates of σ_z, $U_n^{(m)} = I^{\otimes(n-1)}\otimes\sigma_m$, $(m = 0, 1, 2, 3, n = 2, 3, ...)$, $\sigma_0 = I$ is the identity acting on C^2 and σ_m $(m = 1, 2, 3)$ are the standard Pauli matrices. Consider a correlation

*Project supported by the National Natural Science Foundation of China (Grant Nos 10404007 and 60578055), and the State Key Program for Basic Research of China (Grant No 2007CB925204).
†Corresponding author. E-mail: zmzhang@scnu.edu.cn

function

$$E_{k_1,...,k_{2n}}(\rho_{2n}) = \mathrm{Tr}(\rho_{2n}\hat{O}_{k_1}^{(1)} \otimes ... \otimes \hat{O}_{k_{2n}}^{(2n)}), \quad (3)$$

where $\hat{O}_{k_j}^{(j)} = \hat{n}_{k_j}^{(j)} \bullet \sigma \quad (k_j = 1, 2, \quad j = 1, 2, ..., 2n)$, $\hat{n}_{k_j}^{(j)}$ stands for unit vector from R^3. Choosing $\hat{n}_1^{(j)} = \hat{x}, \hat{n}_2^{(j)} = \hat{y},$ for $j = 1, 2, ..., 2n-1$ and $\hat{n}_1^{(2n)} = \frac{\hat{x}+\hat{y}}{\sqrt{2}}$, $\hat{n}_2^{(2n)} = \frac{\hat{x}-\hat{y}}{\sqrt{2}}$, one can get

$$\begin{aligned} &E_{1,1,..,1,1}(\rho_{2n}) + E_{1,1,..,1,2}(\rho_{2n}) + ... \\ &+ E_{2,2,..,2,1}(\rho_{2n}) - E_{2,2,..,2,2}(\rho_{2n}) \\ =&(-1)^n 2\sqrt{2}, \end{aligned} \quad (4)$$

which maximally violates a multi-particle CHSH-type Bell inequality of the form

$$\begin{aligned} &|E_{1,1,..,1,1}(\rho_{2n}) + E_{1,1,...,1,2}(\rho_{2n}) + ... \\ &+ E_{2,2,...,2,1}(\rho_{2n}) - E_{2,2,...,2,2}(\rho_{2n})| \leq 2. \end{aligned}$$

It means that the Smolin state may be considered as a useful resource for quantum cryptography. We address a protocol of QSS using the Smolin states in the following.

Suppose that Alice has some private information to be secretly distributed among $2n-1$ Bobs in a way that all the Bobs must cooperate to recover the message. She uses the generalized Smolin states shared between Alice and Bobs as the vehicle. Alice and Bobs randomly choose between the observables σ_x and σ_y to measure their respective particle, and get results r_i. When the choice is same, the results satisfy $r_A \oplus r_{B_1} \oplus ... \oplus r_{B_{2n-1}} = n \bmod 2$ ($\oplus$ means addition modulo 2). If all Bobs act in concert, they can obtain Alice's secret bits.

From the recursive form of the $2n$-qubit Smolin state in Eq.(2), one can see that if a Bell-basis measurement is performed on each pair of qubits, after $(n-1)$ times of measurement a pure maximal entangled state can be ultimately discriminated between the residual two qubits. Therefore the protocol of QSS is secure against the external eavesdropping as proved in Ref.[14].

The most serious threat to the security of the QSS comes from the participant's attack, now we analyse it in detail. For convenience, the recursive form of the generalized Smolin state in Eq.(2) is outspread in the σ_z basis $\{|0\rangle, |1\rangle\}$ with the subscript being omitted,

$$\begin{aligned} \rho_{2n} =& \frac{1}{4^{n-1}} \sum_{P=0}^{2^{2n-1}-1} \frac{|P\rangle + (-1)^n \left|\bar{P}\right\rangle}{\sqrt{2}} \\ &\otimes \frac{\langle P| + (-1)^n \left\langle \bar{P}\right|}{\sqrt{2}}, \end{aligned} \quad (5)$$

where $P \in \{0, ..., 2^{2n-1}-1\}$ and $|P\rangle = |P_1 P_2 ... P_{2n}\rangle$, $\left|\bar{P}\right\rangle = \left|\bar{P}_1 \bar{P}_2 ... \bar{P}_{2n}\right\rangle$, with $P_i \in \{0, 1\}$ and $\bar{P}_i = 1 - P_i$. Whenever n is even, $|P\rangle$ and $\left|\bar{P}\right\rangle$ are arrays consisted of even $|0\rangle$s. Take an example, for $n = 2$,

$$\begin{aligned} \rho_4 =& \frac{1}{4}\Big\{ \frac{|0000\rangle + |1111\rangle}{\sqrt{2}} \otimes \frac{\langle 0000| + \langle 1111|}{\sqrt{2}} + \frac{|0011\rangle + |1100\rangle}{\sqrt{2}} \otimes \frac{\langle 0011| + \langle 1100|}{\sqrt{2}} \\ &+ \frac{|0110\rangle + |1001\rangle}{\sqrt{2}} \otimes \frac{\langle 0110| + \langle 1001|}{\sqrt{2}} + \frac{|0101\rangle + |1010\rangle}{\sqrt{2}} \otimes \frac{\langle 0101| + \langle 1010|}{\sqrt{2}} \Big\}. \end{aligned}$$

While n is odd, $|P\rangle$ and $\left|\bar{P}\right\rangle$ are arrays of odd $|0\rangle$s. In fact, it can be realized that the states $\frac{|P\rangle + (-1)^n \left|\bar{P}\right\rangle}{\sqrt{2}}$ are the eigenstates of ρ_{2n}.

Now in the Bobs there is one or more cheater who wants to cooperate with the eavesdropper to access the Alice's secret bits illegally and undetectably. For simplicity, we first consider the case of one cheater, assuming Bob $_{2n-1}$ is the cheater. For the sake of the symmetry of the Smolin state under exchange of qubits, the final conclusion is same for the other cheater. When qubits are sent out by Alice, Bob$_{2n-1}$lets an ancilla interact with the qubits and resends them to the other Bobs. With the help of the interaction followed by local operation, he can construct a purification of ρ_{2n}

$$|\Psi\rangle_{1,2,...,2n,E} = \frac{1}{\sqrt{4^{n-1}}} \sum_P \frac{|P\rangle_{1,2,...,2n} + (-1)^n \left|\bar{P}\right\rangle_{1,2,...,2n}}{\sqrt{2}} \left|\phi^P\right\rangle_E, \quad (6)$$

where $\left|\phi^{P}\right\rangle_{E}$ is the normalized state of Bob_{2n-1}'s ancilla corresponding to the eigenstate $\dfrac{|P\rangle+(-1)^{n}\left|\bar{P}\right\rangle}{\sqrt{2}}$, and is mutually orthogonal for different eigenstate, that is, the dimension of the ancilla system is 4^{n-1}, which is equal to the number of the eigenstates of ρ_{2n}. It is obvious that a partial trace over H_E yields ρ_{2n}. Immediately, the intervention of Bob_{2n-1} causes no increase in the error rate of QSS, and is undetectable. On the other hand, after tracing over $H_{\mathrm{Bob}_1}\otimes H_{\mathrm{Bob}_2}\otimes ...\otimes H_{\mathrm{Bob}_{2n-2}}$ one gets

$$\begin{aligned}\rho_{\mathrm{A,B},E}=&\frac{1}{4^{n-1}\times 2}\Bigg\{\sum_{P_{\mathrm{I}}}\Big[\Big(|00\rangle_{\mathrm{A,B}}\left|\phi_E^{P_{\mathrm{I}}}\right\rangle+|11\rangle_{\mathrm{A,B}}\left|\phi_E^{\bar{P}_{\mathrm{I}}}\right\rangle\Big)\Big({}_{\mathrm{A,B}}\langle 00|\left\langle\phi_E^{P_{\mathrm{I}}}\right|+{}_{\mathrm{A,B}}\langle 11|\left\langle\phi_E^{\bar{P}_{\mathrm{I}}}\right|\Big)\\&+\Big(|11\rangle_{\mathrm{A,B}}\left|\phi_E^{P_{\mathrm{I}}}\right\rangle+|00\rangle_{\mathrm{A,B}}\left|\phi_E^{\bar{P}_{\mathrm{I}}}\right\rangle\Big)\Big({}_{\mathrm{A,B}}\langle 11|\left\langle\phi_E^{P_{\mathrm{I}}}\right|+{}_{\mathrm{A,B}}\langle 00|\left\langle\phi_E^{\bar{P}_{\mathrm{I}}}\right|\Big)\Big]\\&+\sum_{P_{\mathrm{II}}}\Big[\Big(|01\rangle_{\mathrm{A,B}}\left|\phi_E^{P_{\mathrm{II}}}\right\rangle+|10\rangle_{\mathrm{A,B}}\left|\phi_E^{\bar{P}_{\mathrm{II}}}\right\rangle\Big)\Big({}_{\mathrm{A,B}}\langle 01|\left\langle\phi_E^{P_{\mathrm{II}}}\right|+{}_{\mathrm{A,B}}\langle 10|\left\langle\phi_E^{\bar{P}_{\mathrm{II}}}\right|\Big)\\&+\Big(|10\rangle_{\mathrm{A,B}}\left|\phi_E^{P_{\mathrm{II}}}\right\rangle+|01\rangle_{\mathrm{A,B}}\left|\phi_E^{\bar{P}_{\mathrm{II}}}\right\rangle\Big)\Big({}_{\mathrm{A,B}}\langle 10|\left\langle\phi_E^{P_{\mathrm{II}}}\right|+{}_{\mathrm{A,B}}\langle 01|\left\langle\phi_E^{\bar{P}_{\mathrm{II}}}\right|\Big)\Big]\Bigg\},\end{aligned}\tag{7}$$

for n even, and

$$\begin{aligned}\rho_{\mathrm{A,B},E}=&\frac{1}{4^{n-1}\times 2}\Bigg\{\sum_{P_{\mathrm{I}}}\Big[\Big(|01\rangle_{\mathrm{A,B}}\left|\phi_E^{P_{\mathrm{I}}}\right\rangle-|10\rangle_{\mathrm{A,B}}\left|\phi_E^{\bar{P}_{\mathrm{I}}}\right\rangle\Big)\Big({}_{\mathrm{A,B}}\langle 01|\left\langle\phi_E^{P_{\mathrm{I}}}\right|-{}_{\mathrm{A,B}}\langle 10|\left\langle\phi_E^{\bar{P}_{\mathrm{I}}}\right|\Big)\\&+\Big(-|10\rangle_{\mathrm{A,B}}\left|\phi_E^{P_{\mathrm{I}}}\right\rangle+|01\rangle_{\mathrm{A,B}}\left|\phi_E^{\bar{P}_{\mathrm{I}}}\right\rangle\Big)\Big(-{}_{\mathrm{A,B}}\langle 10|\left\langle\phi_E^{P_{\mathrm{I}}}\right|+{}_{\mathrm{A,B}}\langle 01|\left\langle\phi_E^{\bar{P}_{\mathrm{I}}}\right|\Big)\Big]\\&+\sum_{P_{\mathrm{II}}}\Big[\Big(|00\rangle_{\mathrm{A,B}}\left|\phi_E^{P_{\mathrm{II}}}\right\rangle-|11\rangle_{\mathrm{A,B}}\left|\phi_E^{\bar{P}_{\mathrm{II}}}\right\rangle\Big)\Big({}_{\mathrm{A,B}}\langle 00|\left\langle\phi_E^{P_{\mathrm{II}}}\right|-{}_{\mathrm{A,B}}\langle 11|\left\langle\phi_E^{\bar{P}_{\mathrm{II}}}\right|\Big)\\&+\Big(-|11\rangle_{\mathrm{A,B}}\left|\phi_E^{P_{\mathrm{II}}}\right\rangle+|00\rangle_{\mathrm{A,B}}\left|\phi_E^{\bar{P}_{\mathrm{II}}}\right\rangle\Big)\Big(-{}_{\mathrm{A,B}}\langle 11|\left\langle\phi_E^{P_{\mathrm{II}}}\right|+{}_{\mathrm{A,B}}\langle 00|\left\langle\phi_E^{\bar{P}_{\mathrm{II}}}\right|\Big)\Big]\Bigg\}\end{aligned}\tag{8}$$

for n odd, where the subscript A and B denote the qubits belonging to Alice and Bob_{2n-1}, respectively. The superscript $P_{\mathrm{I}}\in\{0,...,2^{2n-1}-1\}$ refers to an array $(P_1P_2...P_{2n})$ in which the subarray $(P_2...P_{2n-1})$ excluding qubit 1 contains even 0 s, while the superscript $P_{\mathrm{II}}\in\{0,...,2^{2n-1}-1\}$ represents another array $(P_1P_2...P_{2n})$ in which the subarray $(P_2...P_{2n-1})$ contains odd 0 s.

The reduced density operators can be rewritten in the form of

$$\begin{aligned}\rho^{\mathrm{even}}_{\mathrm{A,B},E}=&\frac{1}{4^{n-1}}\Bigg\{\sum_{P_{\mathrm{I}}}\Bigg[\left|\Phi^{+}\right\rangle_{\mathrm{A,B}}\left\langle\Phi^{+}\right|\otimes\frac{\left|\phi_E^{P_{\mathrm{I}}}\right\rangle+\left|\phi_E^{\bar{P}_{\mathrm{I}}}\right\rangle}{\sqrt{2}}\frac{\left\langle\phi_E^{P_{\mathrm{I}}}\right|+\left\langle\phi_E^{\bar{P}_{\mathrm{I}}}\right|}{\sqrt{2}}\\&+\left|\Phi^{-}\right\rangle_{\mathrm{A,B}}\left\langle\Phi^{-}\right|\otimes\frac{\left|\phi_E^{P_{\mathrm{I}}}\right\rangle-\left|\phi_E^{\bar{P}_{\mathrm{I}}}\right\rangle}{\sqrt{2}}\frac{\left\langle\phi_E^{P_{\mathrm{I}}}\right|-\left\langle\phi_E^{\bar{P}_{\mathrm{I}}}\right|}{\sqrt{2}}\Bigg]\\&+\sum_{P_{\mathrm{II}}}\Bigg[\left|\Psi^{+}\right\rangle_{\mathrm{A,B}}\left\langle\Psi^{+}\right|\otimes\frac{\left|\phi_E^{P_{\mathrm{II}}}\right\rangle+\left|\phi_E^{\bar{P}_{\mathrm{II}}}\right\rangle}{\sqrt{2}}\frac{\left\langle\phi_E^{P_{\mathrm{II}}}\right|+\left\langle\phi_E^{\bar{P}_{\mathrm{II}}}\right|}{\sqrt{2}}\\&+\left|\Psi^{-}\right\rangle_{\mathrm{A,B}}\left\langle\Psi^{-}\right|\otimes\frac{\left|\phi_E^{P_{\mathrm{II}}}\right\rangle-\left|\phi_E^{\bar{P}_{\mathrm{II}}}\right\rangle}{\sqrt{2}}\frac{\left\langle\phi_E^{P_{\mathrm{II}}}\right|-\left\langle\phi_E^{\bar{P}_{\mathrm{II}}}\right|}{\sqrt{2}}\Bigg]\Bigg\},\end{aligned}\tag{9}$$

$$\begin{aligned}\rho^{\mathrm{odd}}_{\mathrm{A,B},E}=&\frac{1}{4^{n-1}}\Bigg\{\sum_{P_{\mathrm{I}}}\Bigg[\left|\Psi^{+}\right\rangle_{\mathrm{A,B}}\left\langle\Psi^{+}\right|\otimes\frac{\left|\phi_E^{P_{\mathrm{I}}}\right\rangle-\left|\phi_E^{\bar{P}_{\mathrm{I}}}\right\rangle}{\sqrt{2}}\frac{\left\langle\phi_E^{P_{\mathrm{I}}}\right|-\left\langle\phi_E^{\bar{P}_{\mathrm{I}}}\right|}{\sqrt{2}}\\&+\left|\Psi^{-}\right\rangle_{\mathrm{A,B}}\left\langle\Psi^{-}\right|\otimes\frac{\left|\phi_E^{P_{\mathrm{I}}}\right\rangle+\left|\phi_E^{\bar{P}_{\mathrm{I}}}\right\rangle}{\sqrt{2}}\frac{\left\langle\phi_E^{P_{\mathrm{I}}}\right|+\left\langle\phi_E^{\bar{P}_{\mathrm{I}}}\right|}{\sqrt{2}}\Bigg]\end{aligned}$$

$$+\sum_{P_{\rm II}}\left[\left|\Phi^{+}\right\rangle_{\rm A,B}\left\langle\Phi^{+}\right|\otimes\frac{\left|\phi_E^{P_{\rm II}}\right\rangle-\left|\phi_E^{\bar{P}_{\rm II}}\right\rangle}{\sqrt{2}}\frac{\left\langle\phi_E^{P_{\rm II}}\right|-\left\langle\phi_E^{\bar{P}_{\rm II}}\right|}{\sqrt{2}}\right.$$
$$\left.+\left|\Phi^{-}\right\rangle_{\rm A,B}\left\langle\Phi^{-}\right|\otimes\frac{\left|\phi_E^{P_{\rm II}}\right\rangle+\left|\phi_E^{\bar{P}_{\rm II}}\right\rangle}{\sqrt{2}}\frac{\left\langle\phi_E^{P_{\rm II}}\right|+\left\langle\phi_E^{\bar{P}_{\rm II}}\right|}{\sqrt{2}}\right]\Bigg\}. \quad (10)$$

From Eqs.(9) and (10), we can see that it is possible for the cheater Bob_{2n-1} to purify a Bell state shared between Alice and him through a local measurement on his ancilla. Resorting to the Bell state, Bob_{2n-1} can steal Alice's secret bits by a measurement on his qubit when the observables used to establish secret key are determined. And his steal cannot be detected because his intervention has no effect on the shared state of ρ_{2n} manifested by Eq.(6). Hence, the QSS protocol of the Smolin bound entangled states is frail against the attack of one participant. As an example, an attack protocol of the participant can be found in Ref.[16]. And it can be found that the more dishonest participant is, the frailer the protocol is.

3. Conclusion

In this paper we have analysed the security of QSS protocol with the Smolin bound entangled states as the channel, which has been reported to violate maximally a multi-particle CHSH-type Bell inequality.[14,15] Owing to the quantum correlation between the cheat participants and other parties, the cheaters can manage to steal the secret bit of the sender (Alice) without being detected. The protocol is insecure against the participant's attack. This counterexample shows that in the quantum secure communication involving more than two parties, the maximal violation to Bell inequality cannot act as a criterion for security of QSS against the participant's attack. Only the maximal violation to Bell inequality cannot ensure the security. More effort is needed for seeking the true criterion for the security of multiparty quantum secure communication.

References

[1] Gisin N, Ribordy G, Tittle W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145

[2] Bennett C and Brassard G 1984 in *Proceedings of the International Conference on Computer, System and Signal Processing* Bangalore India (New York: IEEE)
Ekert A 1991 *Phys. Rev. Lett.* **67** 661
Bennett C, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557
Bennett C, Bessete F, Brassard G, Savail L and Smolin J 1992 *J. Cryptology* **5** 3

[3] Huttner B and Gisin N 1997 *Phys. Lett.* A **228** 13
Fuchs C A, Gisin N, Griffiths R B, Niu C S and Peres A 1997 *Phys. Rev.* A **56** 1163
Cirac J I and Gisin N 1997 *Phys. Lett.* A **229** 1

[4] Acin A, Masanes L and Gisin N 2003 *Phys. Rev. Lett.* **91** 167901

[5] Bruss D, Christand M, Ekert A, Englert B G, Kaszlikowski D and Macchiavello C 2003 *Phys. Rev. Lett.* **91** 097901

[6] Gisin N and Wolf S 1999 *Phys. Rev. Lett.* **83** 4200

[7] Horodecki K, Horodecki M, Horodecki P and Oppenheim J 2005 *Phys. Rev. Lett.* **94** 160502

[8] Hillery M, Bužek V and Berthiaume A 1999 *Phys. Rev.* A **59** 1829
Cleve R, Gottesman D and Lo H K 1999 *Phys. Rev. Lett.* **83** 648

[9] Zhang Y Q, Jin X R and Zhang S 2006 *Chin. Phys.* **15** 2252
Li Y and Zeng G H 2007 *Chin. Phys.* **16** 2875
Tao Y J, Tian D P, Hu M L and Qin M 2008 *Chin. Phys.* B **17** 624

[10] Du J Z, Qin S J, Sun Y, Wen Q Y and Zhu F C 2008 *Acta Phys. Sin.* **57** 4689 (in Chinese)

[11] Scarani V and Gisin N 2001 *Phys. Rev.* A **65** 012311
Scarani V and Gisin N 2001 *Phys. Rev. Lett.* **87** 117901

[12] Zukowski M and Brukner C 2002 *Phys. Rev. Lett.* **88** 210401
Weinfurter H and Zukowski M 2001 *Phys. Rev.* A **64** 010102(R)
Werner R F and Wolf M M 2001 *Phys. Rev.* A **64** 032112

[13] Sen(De) A, Sen U and Zukowski M 2003 *Phys. Rev.* A **68** 032309

[14] Augusiak R and Horodecki P 2006 *Phys. Rev.* A **73** 012318

[15] Augusiak R and Horodecki P 2006 *Phys. Rev.* A **74** 010305(R)

[16] Yu Y F 2007 *Phys. Rev.* A **75** 066301