Partially secret broadcasting, partially secret splitting with quantum entanglement

Liu Yu(刘 玉)[a)] and Zhang Bin-Bin(张彬彬)[b)†]

[a)] *Department of Electronics and Information Engineering, Huazhong University of Science and Technology, Wuhan* 430074, *China*
[b)] *College of Optoelectronic Science and Engineering, Huazhong University of Science and Technology, Wuhan* 430074, *China*

(Received 17 April 2009; revised manuscript received 8 July 2009)

In this paper, we propose a classical secret broadcasting and splitting joint protocol in a quantum scenario. With those genuinely entangled states, the boss can always broadcast some of his secrets and split some others to multi-receivers at the same time. The efficiency of the joint protocol is also compared with that of two separate ones which realise classical secret broadcasting and classical secret splitting respectively, and based on the comparison we can see the promising advantage of our joint protocol is that it can realise the two tasks more efficiently and more conveniently.

Keywords: secret broadcasting, secret splitting, quantum entanglement

PACC: 0367, 0365

1. Introduction

Entanglement, the heart of quantum information theory, has allowed many interesting applications—such as teleportation,[1−7] dense coding,[8−12] unconditionally secure key distribution[13−16]—to come true. It is also employed in the communication systems for authentication,[17,18] secret splitting,[19−31] secret broadcasting[32] and so on. With the method of quantum technology, the above systems could possess high performance in their security. However, entanglement, as an important resource for a variety of existing tasks and possible unknown ones, still requires thorough research and investigation. For example, since the first quantum secret splitting protocol using the Greenberger–Horne–Zeilinger (GHZ) state was proposed by Hillery *et al.*[19] and then extended by Xiao *et al.*,[20] the study utilizing this kind of entangled state in the field of quantum communication, especially in the multiparty communication case, has never stopped, and many surprising results have been found.[21−31] Very recently, Wang *et al.*[32] also presented a classical information broadcasting scheme based on this kind of state. In this paper, we want to explore another new research direction in which the classical scenario of secret broadcasting and secret splitting can be realised with the entangled qubits at the same time. We first present the three-party protocol, analyse it in detail and then generalise it to the n-party one.

2. Joining secret broadcasting and secret sharing together

Suppose the boss Kathleen wants to broadcast a less confidential classical message and split a more confidential one in an honest group. To our best knowledge, there is no way for Kathleen to accomplish this task at once, so far. In the following, we would like to introduce a skilful method resorting to multipartite entanglement to solve the problem.

As an example, we first consider the case where there are three honest agents in the group, say Alice, Bob and Charlie. To achieve the goal above, the parties act as follows:

Step (a) Kathleen, the boss, prepares a sequence of entangled photons in one of the following four six-particle maximally entangled state:

$$|\gamma_1\rangle = \frac{1}{\sqrt{2}}(|000000\rangle + |111111\rangle), \quad (1)$$

$$|\gamma_2\rangle = \frac{1}{\sqrt{2}}(|000000\rangle - |111111\rangle), \quad (2)$$

$$|\gamma_3\rangle = \frac{1}{\sqrt{2}}(|010101\rangle + |101010\rangle), \quad (3)$$

$$|\gamma_4\rangle = \frac{1}{\sqrt{2}}(|010101\rangle - |101010\rangle). \quad (4)$$

Because the four two-qubit Bell states are

$$|\mathcal{B}_{xy}\rangle = \frac{1}{\sqrt{2}}(|0, 0 \oplus y\rangle + (-1)^x|1, 1 \oplus y\rangle), \quad (5)$$

†Corresponding author. E-mail: binbinoe@gmail.com

© 2010 Chinese Physical Society and IOP Publishing Ltd

where $x, y \in \{0, 1\}$, we can rewrite the states (1), (2), (3) and (4) as

$$|\gamma_1\rangle = \frac{1}{2}(|\mathcal{B}_{00}\rangle|\mathcal{B}_{00}\rangle|\mathcal{B}_{00}\rangle + |\mathcal{B}_{00}\rangle|\mathcal{B}_{10}\rangle|\mathcal{B}_{10}\rangle + |\mathcal{B}_{10}\rangle|\mathcal{B}_{00}\rangle|\mathcal{B}_{10}\rangle + |\mathcal{B}_{10}\rangle|\mathcal{B}_{10}\rangle|\mathcal{B}_{00}\rangle), \quad (6)$$

$$|\gamma_2\rangle = \frac{1}{2}(|\mathcal{B}_{00}\rangle|\mathcal{B}_{00}\rangle|\mathcal{B}_{10}\rangle + |\mathcal{B}_{00}\rangle|\mathcal{B}_{10}\rangle|\mathcal{B}_{00}\rangle + |\mathcal{B}_{10}\rangle|\mathcal{B}_{00}\rangle|\mathcal{B}_{00}\rangle + |\mathcal{B}_{10}\rangle|\mathcal{B}_{10}\rangle|\mathcal{B}_{10}\rangle), \quad (7)$$

$$|\gamma_3\rangle = \frac{1}{2}(|\mathcal{B}_{01}\rangle|\mathcal{B}_{01}\rangle|\mathcal{B}_{01}\rangle + |\mathcal{B}_{01}\rangle|\mathcal{B}_{11}\rangle|\mathcal{B}_{11}\rangle + |\mathcal{B}_{11}\rangle|\mathcal{B}_{01}\rangle|\mathcal{B}_{11}\rangle + |\mathcal{B}_{11}\rangle|\mathcal{B}_{11}\rangle|\mathcal{B}_{01}\rangle), \quad (8)$$

$$|\gamma_4\rangle = \frac{1}{2}(|\mathcal{B}_{01}\rangle|\mathcal{B}_{01}\rangle|\mathcal{B}_{11}\rangle + |\mathcal{B}_{01}\rangle|\mathcal{B}_{11}\rangle|\mathcal{B}_{01}\rangle + |\mathcal{B}_{11}\rangle|\mathcal{B}_{01}\rangle|\mathcal{B}_{01}\rangle + |\mathcal{B}_{11}\rangle|\mathcal{B}_{11}\rangle|\mathcal{B}_{11}\rangle). \quad (9)$$

Step (b) The boss distributes the first and the second particles of each state to Alice, the third and the fourth to Bob, and the fifth and the sixth to Charlie. Note that Kathleen transmits the six particles step by step, namely time-separatedly, and after each transmission, the parties check whether there is any eavesdropper as follows.

Step (c) The checking procedures are: after each particle transmission, all the parties agree to choose a subset of the entangled states to detect an eavesdropper and they measure each corresponding particle in a state with the same measuredment basis $\{|+90^{\rm o}\rangle, |-90^{\rm o}\rangle\}$ or $\{|+45^{\rm o}\rangle, |-45^{\rm o}\rangle\}$. After that, each agent tells the boss their measured results in a random order, and Kathleen judges the existence of the eavesdropper. If there is no cheating on line, they go to the next step, otherwise they restart the establishment of communication.

Step (d) After ensuring there is no eavesdropper on line, all the recievers perform Bell state measurement on each pair of the recieved particles separately. Following the rule that the measurement outcomes $\{|\mathcal{B}_{00}\rangle, |\mathcal{B}_{10}\rangle\}$ stand for the broadcasting classical bit 0 and $\{|\mathcal{B}_{01}\rangle, |\mathcal{B}_{11}\rangle\}$ for 1, Alice, Bob and Charlie can easily and directly obtain the secret from Kathleen. However, when Kathleen encodes the secret to be shared obeying that if the measured results of Alice, Bob and Charlie contain odd numbers of $|\mathcal{B}_{00}\rangle$ or $|\mathcal{B}_{01}\rangle$, namely Kathleen chooses state $|\gamma_1\rangle$ or $|\gamma_3\rangle$, the secret is 0 (otherwise the secret is 1), then the three agents can share the confidential information, while no subset of the three members is sufficient to read the information, but the entire group is.

For example, if Kathleen prepares the initial state in $|\gamma_3\rangle$, then the possible measured results of the three receivers are in one of the following four sets, namely $\{|\mathcal{B}_{01}\rangle|\mathcal{B}_{01}\rangle|\mathcal{B}_{01}\rangle\}$, $\{|\mathcal{B}_{01}\rangle|\mathcal{B}_{11}\rangle|\mathcal{B}_{11}\rangle\}$, $\{|\mathcal{B}_{11}\rangle|\mathcal{B}_{01}\rangle|\mathcal{B}_{11}\rangle\}$ and $\{|\mathcal{B}_{11}\rangle|\mathcal{B}_{11}\rangle|\mathcal{B}_{01}\rangle\}$. However, no matter which one of the four sets the measured results would be, each receiver can read the broadcast information directly, because $|\mathcal{B}_{01}\rangle$ and $|\mathcal{B}_{11}\rangle$ both stand for the broadcast information 1. On the other hand, they cannot attain the splitting information alone until they cooperate later to know there are all together odd numbers of $|\mathcal{B}_{00}\rangle$ or $|\mathcal{B}_{01}\rangle$ (in this case, the number of $|\mathcal{B}_{01}\rangle$ would be one or three), then obtain the splitting information 0.

Now, we would like to look into its security performance. Because the secret is meant to be partially broadcast among the group, we assume all the agents are honest. What we focus on is the cheating behaviour from outside. Because there is no information needed for the decoding phase, it is free of classical information leakage. So if the eavesdropper wants to steal the secret, she has to disturb the quantum line. No matter what eavesdropping strategy she has applied (the measure-and-send attack, the intercept-and-resend attack, the entanglement attack and so on), it will be obviously detected if she gets any information. We can see this from the aspect of information theory below.[33]

Assume that the state $\rho = |\gamma_i\rangle\langle\gamma_i|$, $(i = 1, 2, 3, 4)$ turns to ρ^* after Eve's eavesdropping. The classical information Eve can obtain from ρ^* is less than the Holevo quantity $\chi(\rho^*)$, which is

$$\chi(\rho^*) = S(\rho^*) - \sum_i p_i S(p_i), \quad (10)$$

where $S(\rho^*)$ is the von-Neumann entropy of the state ρ^* and the upper bound of $\chi(\rho^*)$. Define

$$\alpha = 1 - F(|\gamma_i\rangle, \rho^*)^2 = 1 - \langle\gamma_i|\rho^*|\gamma_i|\rangle, \quad (11)$$

in which $F(|\gamma_i\rangle, \rho^*)$ is the fidelity of the states $|\gamma_i\rangle$ and ρ^*,[34] $0 \le \alpha \le 1$.

Since the state ρ^* is composed of six qubits, the maximal entropy of ρ^* is

$$S(\rho^*)_{\max} = -(1-\alpha)\log_2(1-\alpha) - (2^6-1)\times[\alpha/(2^6-1)]\log_2[\alpha/(2^6-1)]. \quad (12)$$

Under the above two bases detection strategies, we obtain that $d \ge \alpha/2$.[33] From the result of Eq. (12), it can be seen that when $\alpha = 0$, which is the only chance for $d = 0$, the maximal information Eve can gain is

$S(\rho^*) = 0$. Therefore, if the eavesdropper wants to attack the quantum channel effectively, she has to face a nonzero detective probability.

A similar checking strategy has also been applied in Ref. [35], and very recently, Tan *et al.*[36] also proved that it is impossible to identify orthogonally time-seperated entangled states without disturbing them. Thus our protocol is robust and secure.

3. Comparing the joint protocol with the previous separate ones

In this section, we would compare briefly the efficiency of our proposed protocol with that of the previous separate ones.[19,32] In Ref. [19], to realise one bit of information splitting between two parties, it should at least consume one three-photon GHZ state. In Ref. [32], to broadcast one bit of information between two parties with entanglement swapping, it should also at least consume one three-photon GHZ state. In a word, if one wanted to split one bit of information and broadcast another between two parties before, he had to resort to the above two different protocols and spend at least two three-photon GHZ states. However, with our protocol, if one wants to realise the same task, then the procedure is more convenient and only one four-photon GHZ state should be spent (note that the six-photon states used in the previous section are meant to deal with the case where there are three receivers). As a result, from the aspect of quantum state consumption, using the protocol we proposed seems more efficient than using the previous separate ones if the same amount of information is to be broadcast and split at the same time.

4. Generalized protocol

Now, we would generate it to n-party classical secret broadcasting and secret splitting. The procedures are analogous while the only difference is that we employ a $2n$-particle entangled state here. The $2n$-particle entangled state is in one of the following forms:

$$|\Gamma_1\rangle = \frac{1}{\sqrt{2}}(|0000\ldots00\rangle_{2n} + |1111\ldots11\rangle_{2n}), \quad (13)$$

$$|\Gamma_2\rangle = \frac{1}{\sqrt{2}}(|0000\ldots00\rangle_{2n} - |1111\ldots11\rangle_{2n}), \quad (14)$$

$$|\Gamma_3\rangle = \frac{1}{\sqrt{2}}(|0101\ldots01\rangle_{2n} + |1010\ldots10\rangle_{2n}), \quad (15)$$

$$|\Gamma_4\rangle = \frac{1}{\sqrt{2}}(|0101\ldots01\rangle_{2n} - |1010\ldots10\rangle_{2n}). \quad (16)$$

When n is even, we can rewrite the states as

$$|\Gamma_1\rangle = \sqrt{\frac{1}{2^{n-1}}}(|\mathcal{B}_{00}\rangle^{\otimes n} + |\mathcal{B}_{00}\rangle^{\otimes(n-2)}|\mathcal{B}_{10}\rangle^{\otimes 2} + \ldots + |\mathcal{B}_{00}\rangle^{\otimes(n-2k)}|\mathcal{B}_{10}\rangle^{\otimes 2k} + \ldots + |\mathcal{B}_{10}\rangle^{\otimes n}); \quad (17)$$

$$|\Gamma_2\rangle = \sqrt{\frac{1}{2^{n-1}}}(|\mathcal{B}_{00}\rangle^{\otimes(n-1)}|\mathcal{B}_{10}\rangle^{\otimes 1} + |\mathcal{B}_{00}\rangle^{\otimes(n-3)} |\mathcal{B}_{10}\rangle^{\otimes 3} + \ldots + |\mathcal{B}_{00}\rangle^{\otimes(n-1-2k)}|\mathcal{B}_{10}\rangle^{\otimes(1+2k)} + \ldots + |\mathcal{B}_{00}\rangle^{\otimes 1}|\mathcal{B}_{10}\rangle^{\otimes(n-1)}); \quad (18)$$

$$|\Gamma_3\rangle = \sqrt{\frac{1}{2^{n-1}}}(|\mathcal{B}_{01}\rangle^{\otimes n} + |\mathcal{B}_{01}\rangle^{\otimes(n-2)}|\mathcal{B}_{11}\rangle^{\otimes 2} + \ldots + |\mathcal{B}_{01}\rangle^{\otimes(n-2k)}|\mathcal{B}_{11}\rangle^{\otimes 2k} + \ldots + |\mathcal{B}_{11}\rangle^{\otimes n}); \quad (19)$$

$$|\Gamma_4\rangle = \sqrt{\frac{1}{2^{n-1}}}(|\mathcal{B}_{01}\rangle^{\otimes(n-1)}|\mathcal{B}_{11}\rangle^{\otimes 1} + |\mathcal{B}_{01}\rangle^{\otimes(n-3)} |\mathcal{B}_{11}\rangle^{\otimes 3} + \ldots + |\mathcal{B}_{01}\rangle^{\otimes(n-1-2k)}|\mathcal{B}_{11}\rangle^{\otimes(1+2k)} + \ldots + |\mathcal{B}_{01}\rangle^{\otimes 1}|\mathcal{B}_{11}\rangle^{\otimes(n-1)}); \quad (20)$$

and if n is odd, the states become

$$|\Gamma_1\rangle = \sqrt{\frac{1}{2^{n-1}}}(|\mathcal{B}_{00}\rangle^{\otimes n} + |\mathcal{B}_{00}\rangle^{\otimes(n-2)}|\mathcal{B}_{10}\rangle^{\otimes 2} + \ldots + |\mathcal{B}_{00}\rangle^{\otimes(n-2k)}|\mathcal{B}_{10}\rangle^{\otimes 2k} + \ldots + |\mathcal{B}_{00}\rangle^{\otimes 1} |\mathcal{B}_{10}\rangle^{\otimes(n-1)}); \quad (21)$$

$$|\Gamma_2\rangle = \sqrt{\frac{1}{2^{n-1}}}(|\mathcal{B}_{00}\rangle^{\otimes(n-1)}|\mathcal{B}_{10}\rangle^{\otimes 1} + |\mathcal{B}_{00}\rangle^{\otimes(n-3)} |\mathcal{B}_{10}\rangle^{\otimes 3} + \ldots + |\mathcal{B}_{00}\rangle^{\otimes(n-1-2k)}|\mathcal{B}_{10}\rangle^{\otimes(1+2k)} + \ldots + |\mathcal{B}_{10}\rangle^{\otimes n}); \quad (22)$$

$$|\Gamma_3\rangle = \sqrt{\frac{1}{2^{n-1}}}(|\mathcal{B}_{01}\rangle^{\otimes n} + |\mathcal{B}_{01}\rangle^{\otimes(n-2)}|\mathcal{B}_{11}\rangle^{\otimes 2} + \ldots + |\mathcal{B}_{01}\rangle^{\otimes(n-2k)}|\mathcal{B}_{11}\rangle^{\otimes 2k} + \ldots + |\mathcal{B}_{00}\rangle^{\otimes 1} |\mathcal{B}_{10}\rangle^{\otimes(n-1)}); \quad (23)$$

$$|\Gamma_4\rangle = \sqrt{\frac{1}{2^{n-1}}}(|\mathcal{B}_{01}\rangle^{\otimes(n-1)}|\mathcal{B}_{11}\rangle^{\otimes 1} + |\mathcal{B}_{01}\rangle^{\otimes(n-3)} |\mathcal{B}_{11}\rangle^{\otimes 3} + \ldots + |\mathcal{B}_{01}\rangle^{\otimes(n-1-2k)}|\mathcal{B}_{11}\rangle^{\otimes(1+2k)} + \ldots + |\mathcal{B}_{11}\rangle^{\otimes n}). \quad (24)$$

Note that $|\mathcal{B}_{00}\rangle^{\otimes(n-2k)}|\mathcal{B}_{10}\rangle^{\otimes 2k}$ does not mean one term here, it represents every possible state containing $(n-2k)$ $|\mathcal{B}_{00}\rangle$ and $2k|\mathcal{B}_{10}\rangle$, namely containing C_n^{2k} terms all together. For example, when $n = 4$, $k = 1$,

$|\mathcal{B}_{00}\rangle^{\otimes(n-2k)}|\mathcal{B}_{10}\rangle^{\otimes 2k}$ can be displayed as $C_4^2 = 6$ terms, which are

$$\begin{aligned}
&|\mathcal{B}_{00}\rangle \otimes |\mathcal{B}_{00}\rangle \otimes |\mathcal{B}_{10}\rangle \otimes |\mathcal{B}_{10}\rangle,\\
&|\mathcal{B}_{00}\rangle \otimes |\mathcal{B}_{10}\rangle \otimes |\mathcal{B}_{00}\rangle \otimes |\mathcal{B}_{10}\rangle,\\
&|\mathcal{B}_{10}\rangle \otimes |\mathcal{B}_{00}\rangle \otimes |\mathcal{B}_{00}\rangle \otimes |\mathcal{B}_{10}\rangle,\\
&|\mathcal{B}_{00}\rangle \otimes |\mathcal{B}_{10}\rangle \otimes |\mathcal{B}_{10}\rangle \otimes |\mathcal{B}_{00}\rangle,\\
&|\mathcal{B}_{10}\rangle \otimes |\mathcal{B}_{00}\rangle \otimes |\mathcal{B}_{10}\rangle \otimes |\mathcal{B}_{00}\rangle,\\
&|\mathcal{B}_{10}\rangle \otimes |\mathcal{B}_{10}\rangle \otimes |\mathcal{B}_{00}\rangle \otimes |\mathcal{B}_{00}\rangle. \qquad (25)
\end{aligned}$$

As to

$$|\mathcal{B}_{00}\rangle^{\otimes(n-1-2k)}|\mathcal{B}_{10}\rangle^{\otimes(1+2k)}, \quad |\mathcal{B}_{10}\rangle^{\otimes(n-2k)}|\mathcal{B}_{11}\rangle^{\otimes 2k}$$

and

$$|\mathcal{B}_{10}\rangle^{\otimes(n-1-2k)}|\mathcal{B}_{11}\rangle^{\otimes(1+2k)},$$

it is similar and analogous. So, following the same encoding and decoding rules, the boss can always fulfil the task to broadcast some secret and split some among multiparties as well. The detailed procedures are:

Step (A) First of all, the boss prepares a sequence of entangled photons in one of the above four maximally entangled $2n$-particle states to establish a quantum channel.

Step (B) The boss distributes the first two particles of a state to agent 1, the second two to agent 2 and the third two to agent 3, ... , and the last two to the last agent. The particle transmissions are step by step, and after each transmission all the parties check whether there is an eavesdropper.

Step (C) The checking procedures are similar to that of the three-party case. All the parties agree to choose a subset of the entangled states and measure each corresponding particle in a state with the same measurement basis $\{|+90^{\rm o}\rangle, |-90^{\rm o}\rangle\}$ or $\{|+45^{\rm o}\rangle, |-45^{\rm o}\rangle\}$. After that, each agent tells the boss the measured results in a random order, and the boss judges the existence of the eavesdropper. If there is no cheating on line, they go to the next step, otherwise they restart the establishment of the quantum channel.

Step (D) After ensuring there is no cheating behaviour on line, they perform Bell state measurement on each pair of the received particles respectively. Following the rule that the measured outcomes $\{|\mathcal{B}_{00}\rangle, |\mathcal{B}_{10}\rangle\}$ represent the broadcasting classical bit 0 and $\{|\mathcal{B}_{01}\rangle, |\mathcal{B}_{11}\rangle\}$ stand for 1, all the agents can easily and directly obtain the broadcasting secret from the boss. However, when the boss encodes the secret to be shared obeying the rule that if the measured results of all the agents contain odd numbers of $|\mathcal{B}_{00}\rangle$ or $|\mathcal{B}_{01}\rangle$, namely she chooses state $|\Gamma_1\rangle$ or $|\Gamma_3\rangle$, the secret is 0, otherwise the secret is 1, then the agents can share the confidential information. Also, no subset of all the members, but only the entire group, is sufficient to read it. Thus the process is completed and since the checking procedure is similar to what has been discussed above, the scheme holds its security.

5. Conclusion

In summary, we have combined classical secret broadcasting and splitting in a quantum scenario and discussed it intensively in this paper. What we are aiming at is to inspire related researchers to find novel applications with quantum entanglement. In fact, due to the spooky feature of entanglement, many classically impossible tasks can be accomplished easily in the quantum area. So we hope those researchers can dig out more along this line in the future.

References

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

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

[3] Furusawa A, Srensen J L, Braunstein S L, Fuchs C A, Kimble H J and Polzik E S 1998 *Science* **282** 706

[4] Boschi D, Branca S, Martini F D, Hardy L and Popescu S 1998 *Phys. Rev. Lett.* **80** 1121

[5] Lee J and Kim M S 2000 *Phys. Rev. Lett.* **84** 4236
Lee J, Kim M S, Park Y J and Lee S 2000 *J. Mod. Opt.* **47** 2151

[6] Zhan X G, Li H M, Ji H and Zeng H S 2007 *Chin. Phys.* **16** 2880

[7] Du Q H, Lin X M, Chen Z H, Lin G W, Chen L B and Gu Y J 2008 *Chin. Phys.* B **17** 0807

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

[9] Mattle K, Weinfurter H, Kwiat P G and Zeilinger A 1996 *Phys. Rev. Lett.* **76** 4656

[10] Bose S, Plenio M B and Vedral V 2000 *J. Mod. Opt.* **47** 291

[11] Lee H J, Ahn D and Hwang S W 2002 *Phys. Rev.* A **66** 024304

[12] Yan F L and Wang M Y 2004 *Chin. Phys. Lett.* **21** 1195

[13] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
[14] Bennett C H and Brassad G 1984 *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing* Bangalore, India (New York: IEEE) p175
[15] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[16] Lo H K and Zhao Y 2008 arXiv:0803.2507v1 [quant-ph]
[17] Ljunggren D, Bourennane M and Karlsson A 2000 *Phys. Rev.* A **62** 022305
[18] Mihara T 2002 *Phys. Rev.* A **65** 052326
[19] Hillery M, Bužek V and Berthiaume A 1999 *Phys. Rev.* A **59** 1829
[20] Xiao L, Long G L, Deng F G and Pan J W 2004 *Phys. Rev.* A **69** 052307
[21] Li Y and Zeng G H 2007 *Chin. Phys.* **16** 2875
[22] Yan F L, Gao T and Li Y C 2008 *Chin. Phys. Lett.* **25** 1187
[23] Zhang Z J, Li Y and Man Z X 2005 *Phys. Rev.* A **71** 044301
[24] Schmid C, Trojek P and Bourennane M 2005 *Phys. Rev. Lett.* **95** 230505
[25] Yan F L and Gao T 2005 *Phys. Rev.* A **72** 012304
[26] Yang Y G and Wen Q Y 2008 *Chin. Phys.* B **17** 0419
[27] Han L F, Liu Y M, Liu J and Zhang Z J 2008 *Opt. Commun.* **281** 2690
[28] Gao T, Yan F L and Li Y C 2006 arXiv:0601.111v1 [quant-ph]
[29] Yan F L, Gao T and Li Y C 2007 *Science in China* Series G **50** 572
[30] Zhou P, Li X H, Deng F G and Zhou H Y 2007 *Chin. Phys.* **16** 2867
[31] Deng F G, Li X H and Zhou H Y 2008 *Phys. Lett.* A **372** 1957
[32] Wang J, Zhang Q and Tang C J 2007 *Chin. Phys.* **16** 1868
[33] Cai Q Y and Li B W 2004 *Phys. Rev.* A **69** 05430
[34] Fuchs C A 1996 arxiv:9601.020v1 [quant-ph]
Barnum H, Caves C M, Fuchs C A, Jozsa R, and Schumacher B 1996 *Phys. Rev. Lett.* **76** 2818
[35] Deng F G, Long G L and Liu X S 2003 *Phys. Rev.* A **68** 042317
[36] Tan Y G, Cai Q Y and Shi T Y 2008 *Chin. Phys.* B **17** 3194