Vol 18 No 6, June 2009
1674-1056/2009/18(06)/2149-05

Chinese Physics B

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

Enhancing the security of quantum secret sharing against multiphoton attack

Zhang Bin-Bin(张彬彬)[a)†], Wang Da-Qing(王大庆)[a)], Huang Shan-Shan(黄珊珊)[b)], and Liu Yu(刘 玉)[b)‡]

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

[b)] *Department of Electronic Science and Engineering, Huazhong University of Science and Technology, Wuhan* 430074, *China*

(Received 29 October 2008; revised manuscript received 5 December 2008)

It is generally believed that nonorthogonal operations which can realize the state transformation between two nonorthogonal bases may ensure the security of many quantum communication protocols. However, in this paper, we present a powerful attack against quantum secret sharing protocols of these kinds. Applying entangled photons as fake signals, Eve can successfully steal the exact information without being revealed. We also give our effective modification to improve it. Under the suggested checking strategy, even to Eve's most general attack, it is robust and secure.

Keywords: quantum secret sharing, cryptanalysis, entangled photons，security
PACC: 0367, 0365

1. Introduction

Applied with quantum mechanics, many quantum cryptography systems have been intensively studied in the last decades.[1,2] Among them, quantum secret sharing (QSS) is a counterpart of classical secret sharing,[3,4] which allows a secret key transmitted by a sender shared between several receivers in such a way that it can be extracted if and only if all receivers collaborate. After the first QSS scheme using the three-particle Greenberger–Horne–Zeilinger (GHZ) state proposed by Hillery *et al*,[5] variations of multiparty quantum secret sharing protocols using the GHZ state are presented.[6−10] Schemes based on other entangled states with entanglement swapping and local unitary operations are reported, too.[11−20,21,22] Through the sequential communication of a single qubit instead of entangled states, these schemes[23−32] can also achieve the goal of secret sharing.

However, compared with that of most quantum key distribution (QKD) protocols, the security of QSS is much more complicated. One reason is that, the dishonst agents could be eavesdroppers during the process and another reason is that, the qubits are usually passed by the agents which means Eve often has two opportunities to intercept the line. Therefore, it is really necessary for any QSS protocol to possess a powerful and efficient checking strategy which will hold back all the possible attacks.

In Ref.[14], Liu *et al* proposed a protocol of quantum secret sharing with two-particle entangled states. By performing local unitary operations and individual measurements on either of two particles, the agents can finally share a secret key. Because only simple two-particle entanglement sources as well as linear optical elements are employed, it seems more practical and realizable than some other protocols.[14] Though several attacks have been discussed, we find it is insecure if Eve (who could be also one of the agents) resorts to multiphoton attacks. In this letter, we give a brief description of the protocol first and present this kind of attack in the following. Then we suggest a modification to make sure of the invalidation of this attack, thus enhancing its security. Later, by analyzing the modified protocol, we show its unconditional security against Eve's most general attack. We also point out the generality of our proposed eavesdropping strategy in many other QSS protocols, and conclude it finally.

2. Quantum secret sharing protocol and multiphoton attack

Let us first briefly review the initial QSS protocol[14]. Each of two particles of an EPR pair prepared by the boss (in state $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle+|1\rangle|0\rangle)$)

†Corresponding author. E-mail: binbinoe@gmail.com
‡Corresponding author. E-mail: liuyu@mail.hust.edu.cn

is distributed in two different directions. On receiving the j-th qubit, each agent performs a local unitary rotation $R_j^n(\theta_j^n)$ with the randomly chosen value of $\theta_j^n \in \left\{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\right\}$, where

$$R_j^n(\theta_j^n) = \begin{pmatrix} \cos\frac{\theta_j^n}{2} & \sin\frac{\theta_j^n}{2} \\ -\sin\frac{\theta_j^n}{2} & \cos\frac{\theta_j^n}{2} \end{pmatrix} . \tag{1}$$

After passing by all the agents, the state becomes

$$|\Omega\rangle = \frac{1}{\sqrt{2}}[\cos\frac{\sum_{i=1}^{N}\theta_i^b + \sum_{i=1}^{M}\theta_i^c}{2}(|0\rangle|1\rangle + |1\rangle|0\rangle) + \sin\frac{\sum_{i=1}^{N}\theta_i^b + \sum_{i=1}^{M}\theta_i^c}{2}(|0\rangle|0\rangle - |1\rangle|1\rangle)] . \tag{2}$$

For $\theta_i^b, \theta_i^c \in \left\{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\right\}$, the final state $|\Omega\rangle \in \{|\psi^+\rangle, |+\rangle, |\phi^+\rangle, |-\rangle\}$, where $|+\rangle = \frac{1}{\sqrt{2}}(|\psi^+\rangle + |\phi^+\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(-|\psi^+\rangle + |\phi^+\rangle)$. Then they publicly announce their operation bases $\{0, \pi\}$ or $\left\{\frac{\pi}{2}, \frac{3\pi}{2}\right\}$ while keeping the values secret. After that procedure, the valid run in which $|\Omega\rangle \in \{|\psi^+\rangle, |\phi^+\rangle\}$, can be used for secret sharing. Any subset of the $M+N-1$ partners can release the secret bits of the reminding one, if and only if they cooperate. So the quantum secret sharing process is accomplished. To ensure its security, all the agents also need to check the possible eavesdropping, no matter whehterh it comes from outside or inside. The checking procedure is that for a certain selected subset of valid runs they compare their secret bits through a classical channel, and the order for public announcement is randomly chosen each time. It is believed that "by comparing these bits they can reveal any eavesdropping strategy".[14] However, inconsistent with what is to be expected, the protocol can be attacked as follows.

Suppose Eve intercepts the transmitted qubit, and replaces it with a fake signal, which contains several sophisticatedly prepared photons in a pulse. Then after the honest agent, say Alice, has performed the operation on the pulse, she intercepts the channel again. By separating these photons and measuring them in pairs, Eve can steal Alice's information fully and freely. Consequently, she may encode the initial qubit with the same operation as Alice does, avoiding causing error in the checking procedure. Since the previous checking procedure cannot find out the existence of Eve in this situation, the protocol is insecure.

Now, we would like to describe Eve's mode of operation in detail. Assuming that there are three photons in each fake pulse which are composed of two particles of an EPR pair (in state $|\psi^+\rangle$, we denote as $|\psi^+\rangle_1$) and one particle of another EPR pair (also in state $|\psi^+\rangle$, we denote as $|\psi^+\rangle_2$). The other particle of $|\psi^+\rangle_2$ is kept in Eve's hand. Then after Alice's unitary rotation $R_j^n(\theta_j^n)$ on the fake pulse, the three particles are encoded to be the same. And states of the two EPR pairs read

$$\begin{aligned}
|\Xi\rangle_1^* &= R_j^n(\theta_j^n) \otimes R_j^n(\theta_j^n)|\psi^+\rangle_1 \\
&= \frac{1}{\sqrt{2}}\left[R_j^n(\theta_j^n)|0\rangle \otimes R_j^n(\theta_j^n)|1\rangle + R_j^n(\theta_j^n)|1\rangle \otimes R_j^n(\theta_j^n)|0\rangle\right] \\
&= \frac{1}{\sqrt{2}}\left[\begin{pmatrix} \cos\frac{\theta_j^n}{2} & \sin\frac{\theta_j^n}{2} \\ -\sin\frac{\theta_j^n}{2} & \cos\frac{\theta_j^n}{2} \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} \cos\frac{\theta_j^n}{2} & \sin\frac{\theta_j^n}{2} \\ -\sin\frac{\theta_j^n}{2} & \cos\frac{\theta_j^n}{2} \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix}\right. \\
&\quad \left. + \begin{pmatrix} \cos\frac{\theta_j^n}{2} & \sin\frac{\theta_j^n}{2} \\ -\sin\frac{\theta_j^n}{2} & \cos\frac{\theta_j^n}{2} \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} \cos\frac{\theta_j^n}{2} & \sin\frac{\theta_j^n}{2} \\ -\sin\frac{\theta_j^n}{2} & \cos\frac{\theta_j^n}{2} \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right] \\
&= \frac{1}{\sqrt{2}}\begin{pmatrix} \cos\frac{\theta_j^n}{2}\sin\frac{\theta_j^n}{2} + \sin\frac{\theta_j^n}{2}\cos\frac{\theta_j^n}{2} \\ -\sin\frac{\theta_j^n}{2}\sin\frac{\theta_j^n}{2} + \cos\frac{\theta_j^n}{2}\cos\frac{\theta_j^n}{2} \\ \cos\frac{\theta_j^n}{2}\cos\frac{\theta_j^n}{2} - \sin\frac{\theta_j^n}{2}\sin\frac{\theta_j^n}{2} \\ -\sin\frac{\theta_j^n}{2}\cos\frac{\theta_j^n}{2} - \cos\frac{\theta_j^n}{2}\sin\frac{\theta_j^n}{2} \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} \sin\theta_j^n & \cos\theta_j^n & \cos\theta_j^n & -\sin\theta_j^n \end{pmatrix}^{\mathrm{T}} ,
\end{aligned} \tag{3}$$

and

$$
\begin{aligned}
|\Xi\rangle_2^* &= R_j^n(\theta_j^n)\otimes I|\psi^+\rangle_2 \\
&= \frac{1}{\sqrt{2}}[R_j^n(\theta_j^n)|0\rangle\otimes|1\rangle + R_j^n(\theta_j^n)|1\rangle\otimes|0\rangle] \\
&= \frac{1}{\sqrt{2}}\left[\begin{pmatrix} \cos\dfrac{\theta_j^n}{2} & \sin\dfrac{\theta_j^n}{2} \\ -\sin\dfrac{\theta_j^n}{2} & \cos\dfrac{\theta_j^n}{2}\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}0\\1\end{pmatrix}\right. \\
&\quad \left. + \begin{pmatrix} \cos\dfrac{\theta_j^n}{2} & \sin\dfrac{\theta_j^n}{2} \\ -\sin\dfrac{\theta_j^n}{2} & \cos\dfrac{\theta_j^n}{2}\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix}\right] \\
&= \frac{1}{\sqrt{2}}\begin{pmatrix}\sin\dfrac{\theta_j^n}{2} & \cos\dfrac{\theta_j^n}{2} & \cos\dfrac{\theta_j^n}{2} & -\sin\dfrac{\theta_j^n}{2}\end{pmatrix}^{\mathrm{T}} .
\end{aligned} \tag{4}
$$

When θ_j^n chooses from $\left\{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\right\}$, the corresponding states are

$$|\Xi\rangle_1^* \in \{|\psi^+\rangle, |\phi^+\rangle, |\psi^+\rangle, |\phi^+\rangle\} , \tag{5}$$

$$|\Xi\rangle_2^* \in \{|\psi^+\rangle, |+\rangle, |\phi^+\rangle, |-\rangle\} . \tag{6}$$

So Eve can take a joint Bell-state measurement at $|\Xi\rangle_1^*$ first, classifying θ_j^n into two categories $\{0, \pi\}$ and $\left\{\frac{\pi}{2}, \frac{3\pi}{2}\right\}$ according to the result (5). As to the former category, Eve may measure the corresponding $|\Xi\rangle_2^*$ straight, distinguishing 0 from π directly. While to the latter, before the joint Bell-state measurement, Eve must perform a rotation $R(\frac{\pi}{2})$ on $|\Xi\rangle_2^*$ first. The state reads

$$
\begin{aligned}
|\Xi\rangle_2^{**} = R(\frac{\pi}{2})|\Xi\rangle_2^* &= \frac{1}{\sqrt{2}}\begin{pmatrix} \sin\left(\dfrac{\theta_j^n}{2}+\dfrac{\pi}{2}\right) \\ \cos\left(\dfrac{\theta_j^n}{2}+\dfrac{\pi}{2}\right) \\ \cos\left(\dfrac{\theta_j^n}{2}+\dfrac{\pi}{2}\right) \\ -\sin\left(\dfrac{\theta_j^n}{2}+\dfrac{\pi}{2}\right)\end{pmatrix} \\
&\in \{|+\rangle, |\psi^+\rangle, |-\rangle, |\phi^+\rangle\} .
\end{aligned} \tag{7}
$$

Therefore, she can measure $|\Xi\rangle_2^{**}$ at this time, and distinguish $\frac{\pi}{2}$ from $\frac{3\pi}{2}$. Till now, we have shown clearly that Eve can get all the exact information of the rotation without awareness of the honest agent. And in the previous checking procedure, she would not be found since she can encode the same rotation precisely on the initial qubit.

3. Improved protocol and its security analysis

To improve the security of the protocol, the honest parties must have the ability to detect a multiphoton fake signal. For the operating wavelength multiple photons, they can use a photon number splitter (PNS: 50 / 50) or even a photon beam splitter (PBS: 50 / 50) to divide each sample signal into two pieces, which are measured by two detectors.[33,34] When cascading the PNS or PBS, if there is only one photon in the original signal, they can only get one outcome, otherwise they will obtain two. And for the invisible multiple photons,[35] all the parties need to do is to add a wavelength filter (WF) or an isolator on each signal before they deal with it. This move can prevent the invisible photons from entering the operation system. Hence, with little modification above, it can be ensured that each pulse they receive contains at most one photon in the ideal situation.[1]

Now let us analyze the modified protocol against the most general single-photon attack. Suppose Eve intercepts the initial photon and resends a new one which is one particle of the entangled state $|\Sigma\rangle$. Then after an agent Alice's rotation $R_j^n(\theta_j^n)$ ($\theta_j^n \in \left\{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\right\}$), the state turns to

$$R(0)|\Sigma\rangle = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}|\Sigma\rangle \equiv |\Sigma\rangle_{00} , \tag{8}$$

$$R(\frac{\pi}{2})|\Sigma\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ -1 & 1\end{pmatrix}|\Sigma\rangle \equiv |\Sigma\rangle_{01} , \tag{9}$$

$$R(\pi)|\Sigma\rangle = \begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}|\Sigma\rangle \equiv |\Sigma\rangle_{10} , \tag{10}$$

$$R\left(\frac{3\pi}{2}\right)|\Sigma\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}-1 & 1\\ -1 & -1\end{pmatrix}|\Sigma\rangle \equiv |\Sigma\rangle_{11} . \tag{11}$$

For the reason

$$
\begin{aligned}
R\left(\frac{\pi}{2}\right) &= \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ -1 & 1\end{pmatrix} \\
&= \frac{1}{\sqrt{2}}\left[\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} + \begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}\right] \\
&= \frac{1}{\sqrt{2}}[R(0) + R(\pi)] ,
\end{aligned} \tag{12}
$$

and

$$R(\frac{3\pi}{2}) = \frac{1}{\sqrt{2}}\begin{pmatrix} -1 & 1 \\ -1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}}\left[-\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right] = \frac{1}{\sqrt{2}}[-R(0) + R(\pi)] \ , \tag{13}$$

we obtain

$$|\Sigma\rangle_{01} = \frac{1}{\sqrt{2}}(|\Sigma\rangle_{00} + |\Sigma\rangle_{10}) \ , \tag{14}$$

$$|\Sigma\rangle_{11} = \frac{1}{\sqrt{2}}(-|\Sigma\rangle_{00} + |\Sigma\rangle_{10}) \ . \tag{15}$$

Note here that Eve's effective Hilbert space is at most two-dimensional, so she cannot distinguish the four states $\{|\Sigma\rangle_{00}, |\Sigma\rangle_{01}, |\Sigma\rangle_{10}, |\Sigma\rangle_{11}\}$ from each other at once, which means Eve cannot tell exactly the operation performed by Alice. The consequence is that she will be detected in the checking procedure. In fact, we can even see Eve would not get any exact useful information in this situation. We write the four states in the orthogonal basis $\{|\varepsilon_0\rangle, |\varepsilon_1\rangle\}$ (Here, $\langle\varepsilon_0|\varepsilon_0\rangle = \langle\varepsilon_1|\varepsilon_1\rangle = 1$ and $\langle\varepsilon_0|\varepsilon_1\rangle = 0$), obtaining

$$\begin{cases} |\Sigma\rangle_{00} = a|\varepsilon_0\rangle + b|\varepsilon_1\rangle, \\ |\Sigma\rangle_{10} = c|\varepsilon_0\rangle + d|\varepsilon_1\rangle, \\ |\Sigma\rangle_{01} = \frac{1}{\sqrt{2}}(a+c)|\varepsilon_0\rangle + \frac{1}{\sqrt{2}}(b+d)|\varepsilon_1\rangle, \\ |\Sigma\rangle_{11} = \frac{1}{\sqrt{2}}(-a+c)|\varepsilon_0\rangle + \frac{1}{\sqrt{2}}(-b+d)|\varepsilon_1\rangle, \end{cases} \tag{16}$$

where $a^2 + b^2 > 0, c^2 + d^2 > 0, (a+c)^2 + (b+d)^2 > 0$ and $(a-c)^2 + (b-d)^2 > 0$. If Eve wants to get any exact information of the operation, she must be able to distinguish at least one of the four states from the others, i.e. satisfying one of the following equations:

$$\langle\Sigma_{00}|\Sigma_{01}\rangle = \langle\Sigma_{00}|\Sigma_{10}\rangle = \langle\Sigma_{00}|\Sigma_{11}\rangle = 0 \ , \tag{17}$$

$$\langle\Sigma_{01}|\Sigma_{00}\rangle = \langle\Sigma_{01}|\Sigma_{10}\rangle = \langle\Sigma_{01}|\Sigma_{11}\rangle = 0 \ , \tag{18}$$

$$\langle\Sigma_{10}|\Sigma_{00}\rangle = \langle\Sigma_{10}|\Sigma_{01}\rangle = \langle\Sigma_{10}|\Sigma_{11}\rangle = 0 \ , \tag{19}$$

$$\langle\Sigma_{11}|\Sigma_{00}\rangle = \langle\Sigma_{11}|\Sigma_{01}\rangle = \langle\Sigma_{11}|\Sigma_{10}\rangle = 0 \ , \tag{20}$$

which can also be calculated as four equation sets:

$$\begin{cases} a^*(a+c) + b^*(b+d) = 0, \\ a^*c + b^*d = 0, \\ a^*(-a+c) + b^*(-b+d) = 0, \end{cases} \tag{21}$$

$$\begin{cases} (a^* + c^*)a + (b^* + d^*)b = 0, \\ (a^* + c^*)c + (b^* + d^*)d = 0, \\ (a^* + c^*)(-a+c) + (b^* + d^*)(-b+d) = 0, \end{cases} \tag{22}$$

$$\begin{cases} c^*a + d^*b = 0, \\ c^*(a+c) + d^*(b+d) = 0, \\ c^*(-a+c) + d^*(-b+d) = 0, \end{cases} \tag{23}$$

$$\begin{cases} (-a^* + c^*)a + (-b^* + d^*)b = 0, \\ (-a^* + c^*)(a+c) + (-b^* + d^*)(b+d) = 0, \\ (-a^* + c^*)c + (-b^* + d^*)d = 0. \end{cases} \tag{24}$$

Unfortunately, no matter what values have been applied to a, b, c and d, none of the four equation sets can be satisfied. That is to say, Eve cannot tell the exact state among the four states, which also means Eve cannot get the exact information about the rotation at all. Furthermore, the cheating behavior will be obviously found in the previous checking procedure.

4. Discussion

Up to now, we have shown clearly the vulnerability of the proposed quantum secret sharing protocol against multiphoton attack and suggested our effective solution. In fact, it can apply to many other QSS protocols.[19,30,32] It is generally believed in these protocols that, when the operations performed by communication parties can realize the state transformation between two nonorthogonal bases, then the security of them is instinctively ensured. However, from what has been discussed above, one can find there indeed exists a way for an eavesdropper to distinguish the nonorthogonal operations when entangled pairs are used as fake signals. And due to the good feature of entanglement, Eve can get the secret information fully and exactly, instead of with possibility. Since high performance in security is the essential requirement and the most striking feature of quantum cryptography, it is really necessary to make sure a quantum communication protocol can hold back all the possible attacks including this kind. And because of its generality in the related field, it is worthwhile receiving more attention in the future.

5. Conclusion

To summarize, we present an effective attack against the proposed quantum secret sharing protocol when entangled fake photons are employed. We show Eve's mode of action completely and clearly. We also point out the generality of this loophole in other protocols. However, with a little improvement work as suggested above, we see that the security of these protocols can be successfully guaranteed.

References

[1] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
[2] Lo H K and Zhao Y 2008 *arXiv:quant-ph*/0803.2507
[3] Blakely G R 1979 *Proc. AFIPS National Computer Conf.* (New York) **48** (Montvale, NJ: AFIPS Press) p313
[4] Shamir A 1979 *Commun. ACM* **22** 612
[5] Hillery M, Bužek V and Berthiaume A 1999 *Phys. Rev.* A **59** 1829
[6] Xiao L, Long G L, Deng F G and Pan J W 2004 *Phys. Rev.* A **69** 052307
[7] Li X H, Zhou P and Deng F G 2006 *J. Phys.* B: *At. Mol. Opt. Phys* **39** 1975
[8] Xue Z Y, Yi Y M and Cao Z L 2006 *Chin. Phys.* **15** 1421
[9] Deng F G, Zhou P, Li X H, Li C Y and Zhou H Y 2006 *Chin. Phys. Lett.* **23** 1084
[10] Li Y and Zeng G H 2007 *Chin. Phys.* **16** 2875
[11] Li Y M, Zhang K S and Peng K C 2004 *Phys. Lett.* A **324** 420
[12] Zhang Z J and Man Z X 2005 *Phys. Rev.* A **72** 022303
[13] Deng F G, Li X H and Li C Y 2006 *Phys. Lett.* A **354** 190
[14] Liu W T, Liang L M, Li C Z and Yuan J M 2006 *Chin. Phys. Lett.* **23** 3148
[15] Zhou P, Li X H, Deng F G and Zhou H Y 2007 *Chin. Phys.* **16** 2867
[16] Deng F G, Li X H and Zhou H Y 2008 *Phys. Lett.* A **372** 1957
[17] Guo Y, Huang D Z, Zeng G H and Lee M H 2008 *Chin. Phys. Lett.* **25** 16
[18] Zhou P, Li X H, Liang Y J, Deng F G and Zhou H Y 2007 *Physica* A **381** 164
[19] Zhang Z J 2005 *Phys. Lett.* A **342** 60
[20] Yan F L, Gao T and Li Y C 2008 *Chin. Phys. Lett.* **25** 1187
[21] Gao T, Yan F L and Li Y C 2006 *arXiv:quant-ph*/0601111
[22] Yan F L, Gao T and Li Y C 2007 *Sci. Chin.* G **50** 572
[23] Guo G P and Guo G C 2003 *Phys. Lett.* A **310** 247
[24] Zhang Z J, Li Y and Man Z X 2005 *Phys. Rev.* A **71** 044301
[25] Schmid C, Trojek P and Bourennane M 2005 *Phys. Rev. Lett.* **95** 230505
[26] Deng F G, Zhou H Y and Long G L 2005 *Phys. Lett.* A **337** 329
[27] Zhou P, Li X H, Deng F G and Zhou H Y 2007 *Chin. Phys. Lett.* **24** 2181
[28] Hsu L Y and Li C M 2005 *Phys. Rev.* A **71** 022321
[29] Yan F L and Gao T 2005 *Phys. Rev.* A **72** 012304
[30] Liu W T, Liang L M, Li C Z and Yuan J M 2007 *Chin. Phys. Lett.* **24** 1147
[31] Yang Y G and Wen Q Y 2008 *Chin. Phys.* **17** 0419
[32] Han L F, Liu Y M, Liu J and Zhang Z J 2008 *Opt. Commun.* **281** 2690
[33] Deng F G, Zhou P, Li X H, Li C Y and Zhou H Y 2005 *arXiv:quant-ph*/0508168
[34] Li X H, Deng F G and Zhou H Y 2006 *Phys. Rev.* A **74** 054302
[35] Cai Q Y 2006 *Phys. Lett.* A **351** 23