Vol 17 No 9, September 2008
1674-1056/2008/17(09)/3189-05

Chinese Physics B

© 2008 Chin. Phys. Soc.
and IOP Publishing Ltd

Teleportation attack on the QSDC protocol with a random basis and order*

Gao Fei(高 飞)[a)b)†], Wen Qiao-Yan(温巧燕)[a)], and Zhu Fu-Chen(朱甫臣)[c)]

[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)] *National Laboratory for Modern Communications, Chengdu* 610041, *China*

(Received 19 February 2008; revised manuscript received 19 March 2008)

The quantum secure direct communication (QSDC) protocol with a random basis and order is analysed and an effective attack, i.e. teleportation attack, is presented. An eavesdropper can obtain half of the transmitted secret bits with the help of this special attack. It is shown that quantum teleportation can be employed to weaken the role of the order-rearrangement encryption at least in a certain circumstance. Meanwhile, a possible improvement on this protocol is proposed, which makes it secure against this kind of attack.

Keywords: quantum secure direct communication, quantum cryptography, cryptanalysis, teleportation

PACC: 0365, 0155

Based on fundamental theories of quantum mechanics, quantum cryptography[1] can obtain unconditional security in theory. Since the first protocol was proposed by Bennett and Brassard,[2] quantum cryptography has attracted a great deal of attention. In a quantum cryptographic protocol, any effective eavesdropping could be discovered through the process of detection, which ensures its security. For example, in a quantum key distribution (QKD) protocol,[2−4] the users, Alice and Bob, can share a sequence of key bits. If they find that effective eavesdropping happens, they discard these key bits and try it later. Otherwise a secure key will be obtained after some additional processes such as error correction and privacy amplification.

Quantum secure direct communication (QSDC)[5−8] is another branch of quantum cryptography and many QSDC protocols were proposed recently.[9−21] It allows that the sender transmits directly the secret (not a random key) to the receiver in a deterministic and secure manner. The security demands are strict in QSDC as compared with those in QKD because the transmitted secret can never be leaked out whether the eavesdropping would be detected or not (in the QKD the key is just composed of random bits, and their leakage is not strictly forbidden because it would be discovered by the legal users and then the key can be discarded). However, a carefully designed QSDC protocol can also attain unconditional security in theory.[22−24]

As is known, high security is both the advantage of and the crucial requirement for quantum cryptography. However, not all the proposed schemes can reach this requirement. For example, some protocols were attacked successfully by subtle strategies which were not concerned when these protocols were originally designed.[25−35] Recently, Song *et al* [36] presented a novel QSDC protocol based on blind polarization bases and particles' transmitting order. However, here we demonstrate a special attack on this protocol, by which the eavesdropper Eve can obtain half of the secret bits that Alice sends to Bob. Moreover, an improved scheme against this kind of attack is given. For simplicity, we will call this protocol the SZZ protocol[36] later.

It is necessary to give a brief description of the

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

†Corresponding author. E-mail: hzpe@sohu.com

SZZ protocol first. The QSDC process of this protocol consists of the following steps.

(1) Alice prepares n polarized qubits ($|\psi\rangle_1^1$, $|\psi\rangle_2^1$, ..., $|\psi\rangle_n^1$), and $|\psi\rangle_i^1 = \hat{U}_y(\theta_i)|0\rangle = \cos\theta_i|0\rangle - \sin\theta_i|1\rangle$ ($i = 1, 2, ..., n$), where θ_i are angles randomly chosen by Alice and $\hat{U}_y(\theta) = \cos\theta\hat{I} - \mathrm{i}\sin\hat{\sigma}_y$. Then Alice sends this sequence to Bob.

(2) After Bob has received these n qubits, he rotates their polarizations through angles of φ_i, changing the states into $|\psi\rangle_i^2 = \hat{U}_y(\varphi_i)|\psi\rangle_i^1 = \cos(\theta_i + \varphi_i)|0\rangle - \sin(\theta_i + \varphi_i)|1\rangle$. Then Bob disorders this sequence and sends these qubits to Alice in a random order.

(3) After Alice has received them, Bob publicly declares the order he used so that Alice can restore the qubit order in this sequence. Afterwards, Alice rotates the polarizations of these qubits through angles of $-\theta_i \pm \frac{\pi}{4}$, where $\pm\frac{\pi}{4}$ correspond to the secret bits 0 and 1 respectively. Under these operations the states would be changed into $|\psi\rangle_i^3 = \hat{U}_y\left(-\theta_i \pm \frac{\pi}{4}\right)|\psi\rangle_i^2 = \cos\left(\varphi_i \pm \frac{\pi}{4}\right)|0\rangle - \sin\left(\varphi_i \pm \frac{\pi}{4}\right)|1\rangle$. Then Alice sends these qubits to Bob.

(4) Bob rotates the polarizations of these qubits through angles of $-\varphi_i$, entering into the states $|\psi\rangle_i^4 = \hat{U}_y(-\varphi_i)|\psi\rangle_i^3 = \hat{U}_y\left(\pm\frac{\pi}{4}\right)|0\rangle$. Then Bob measures each qubit in the basis $\{\hat{U}_y\left(\frac{\pi}{4}\right)|0\rangle, \hat{U}_y\left(-\frac{\pi}{4}\right)|0\rangle\}$ and subsequently obtains the secret bits sent by Alice.

(5) To detect eavesdropping, Alice and Bob compare the Hash values of the message sent by Alice and the one received by Bob. If no eavesdropping happens, the QSDC protocol is achieved successfully.

As is well known, both blind polarization basis[37] and the random transmitting order[38−40] are powerful techniques to protect the security of a quantum cryptographic protocol. Therefore, it looks as if the SZZ protocol, where the above two techniques are used simultaneously, might be secure without doubt. However, things do not turn out as one wishes. Here we show a special attack which allows Eve to extract half of the secret bits sent by Alice.

The particular process of this attack is as follows.

(E1) Eve prepares n EPR states

$$|\Phi^+\rangle_{i_1 i_2} = 1/\sqrt{2}(|00\rangle + |11\rangle)_{i_1 i_2}, \tag{1}$$

where the subscript $i (i = 1, 2, ..., n)$ denotes the position of the EPR pair, and i_1 and i_2 represent different qubits in the ith entanglement pair. Eve groups all these $2n$ qubits into two ordered sequences $S_1^{\mathrm{E}} = \{1_1, 2_1, ..., i_1, ..., n_1\}$ and $S_2^{\mathrm{E}} = \{1_2, 2_2, ..., i_2, ..., n_2\}$. Furthermore, Eve generates n polarized qubits in the state $|0\rangle$, which constitute another sequence S_3^{E}.

(E2) When Alice sends her qubit sequence (denoted by S_1^{A}) to Bob in step (1), Eve intercepts it and transmits the fake sequence S_3^{E} to Bob. Because Alice and Bob would not detect eavesdropping after Bob received these qubits, Eve's interception cannot be discovered.

(E3) When Bob sends the disordered polarized qubit sequence $S_{3'}^{\mathrm{E}}$ to Alice in step (2), Eve intercepts all these qubits and sends the fake sequence S_1^{E} to Alice. Similar to the operation in step (E2), Eve's operation cannot be detected.

(E4) When Alice "restores" the qubit order of her received sequence S_1^{E} in step (3), Eve adjusts the order of the qubits in sequence S_2^{E} according to Bob's announcement about the random order used by him. Suppose that the new sequences after their reordering are $S_{1'}^{\mathrm{E}}$ and $S_{2'}^{\mathrm{E}}$ respectively. Eve's aim is to let any two qubits in the same position in $S_{1'}^{\mathrm{E}}$ and $S_{2'}^{\mathrm{E}}$ still jointly stay in the EPR state as described in expression (1). Obviously Eve can achieve this goal with the help of Bob's declaration. Afterwards, Eve performs a Bell measurement on every two qubits which are in the same position in the sequences S_1^{A} and $S_{2'}^{\mathrm{E}}$, and records the measurement results.

Without loss of generality, consider one position, for example, the jth qubit, in each sequence. The initial state of the three qubits, i.e. the jth qubits in the three sequences $S_{1'}^{\mathrm{E}}$, $S_{2'}^{\mathrm{E}}$, and S_1^{A}, can be depicted as

$$\begin{aligned}|\delta\rangle_{E_{1'}E_{2'}A_1} =& \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{E_{1'}E_{2'}}(\cos\theta_j|0\rangle \\ & - \sin\theta_j|1\rangle)_{A_1},\end{aligned} \tag{2}$$

where the subscripts $E_{1'}$, $E_{2'}$, and A_1 represent the jth qubits in the sequences $S_{1'}^{\mathrm{E}}$, $S_{2'}^{\mathrm{E}}$, and S_1^{A} respectively. It is not difficult to see that teleportation[41] will happen when Eve performs Bell measurement on qubits $E_{2'}$ and A_1. To see the possible results of this measurement, we can rewrite the state $|\delta\rangle_{E_{1'}E_{2'}A_1}$ into the form

$$\begin{aligned}|\delta\rangle_{E_{1'}E_{2'}A_1} =& \frac{1}{2}[(\cos\theta_j|0\rangle - \sin\theta_j|1\rangle)_{E_{1'}}|\Phi^+\rangle_{E_{2'}A_1} \\ & + (\cos\theta_j|0\rangle + \sin\theta_j|1\rangle)_{E_{1'}}|\Phi^-\rangle_{E_{2'}A_1} \\ & - (\sin\theta_j|0\rangle - \cos\theta_j|1\rangle)_{E_{1'}}|\Psi^+\rangle_{E_{2'}A_1} \\ & - (\sin\theta_j|0\rangle + \cos\theta_j|1\rangle)_{E_{1'}}|\Psi^-\rangle_{E_{2'}A_1}],\end{aligned} \tag{3}$$

where $|\Phi^{\pm}\rangle$ and $|\Psi^{\pm}\rangle$ are four Bell states

$$|\Phi^{\pm}\rangle = 1/\sqrt{2}(|00\rangle \pm |11\rangle)$$

and

$$|\Psi^{\pm}\rangle = 1/\sqrt{2}(|01\rangle \pm |10\rangle). \quad (4)$$

Therefore, Eve will obtain one of four Bell states $\{|\Phi^{+}\rangle, |\Phi^{-}\rangle, |\Psi^{+}\rangle, |\Psi^{-}\rangle\}$ with an equal probability of 1/4, and the state of the qubit in Alice's hand (i.e. qubit $E_{1'}$) will collapse into one of four states

$$\cos\theta_j|0\rangle - \sin\theta_j|1\rangle, \quad (5)$$

$$\cos\theta_j|0\rangle + \sin\theta_j|1\rangle, \quad (6)$$

$$\sin\theta_j|0\rangle - \cos\theta_j|1\rangle, \quad (7)$$

and

$$\sin\theta_j|0\rangle + \cos\theta_j|1\rangle, \quad (8)$$

respectively.

Consequently, when Alice performs the rotation $\hat{U}_y\left(-\theta_j \pm \frac{\pi}{4}\right)$ on qubit $E_{1'}$, its state will be changed into one of the following states:

$$\cos\left(\pm\frac{\pi}{4}\right)|0\rangle - \sin\left(\pm\frac{\pi}{4}\right)|1\rangle, \quad (9)$$

$$\cos\left(\pm\frac{\pi}{4}\right)|0\rangle - \sin\left(-2\theta_j \pm \frac{\pi}{4}\right)|1\rangle, \quad (10)$$

$$\cos\left(-\frac{\pi}{2} \pm \frac{\pi}{4}\right)|0\rangle - \sin\left(-2\theta_j + \frac{\pi}{2} \pm \frac{\pi}{4}\right)|1\rangle, \quad (11)$$

and

$$\cos\left(-\frac{\pi}{2} \pm \frac{\pi}{4}\right)|0\rangle - \sin\left(-\frac{\pi}{2} \pm \frac{\pi}{4}\right)|1\rangle, \quad (12)$$

respectively. It can be seen that the two states in expressions (9) and (12) are orthogonal and consequently can be distinguished with certainty. That is to say, if Eve obtains $|\Phi^{+}\rangle$ or $|\Psi^{-}\rangle$ in her Bell measurement, which happens with a probability of 1/2, she can obtain Alice's secret bit encoded in the corresponding qubit in the sequence $S_{1'}^{\mathrm{E}}$ by a simple polarization measurement. This is the key point of this attack strategy.

Finally, Eve will have $|\Phi^{+}\rangle$ or $|\Psi^{-}\rangle$ in half of her Bell measurements. Here we introduce the notation P to represent the set of positions where Eve obtains $|\Phi^{+}\rangle$ or $|\Psi^{-}\rangle$ in her measurements.

(E5) When Alice sends the sequence $S_{1'}^{\mathrm{E}}$ to Bob after her coding operation in step (3), Eve intercepts it and measures the qubits at the positions in P with the basis $\{|+\rangle, |-\rangle\}$, where

$$|+\rangle = 1/\sqrt{2}(|0\rangle + |1\rangle),$$

and

$$|-\rangle = 1/\sqrt{2}(|0\rangle - |1\rangle). \quad (13)$$

By these measurements Eve can read Alice's secret bits encoded in these qubits.

For example, consider the jth qubits in these sequences, too. According to Alice's coding rule as described in step (3), if the result of Eve's Bell measurement in step (E4) is $|\Phi^{+}\rangle$, the measurement results $|+\rangle$ and $|-\rangle$ in this step imply Alice's corresponding secret bits 0 and 1 respectively (see expression (9)). On the contrary, if the result in step (E4) is $|\Psi^{-}\rangle$, $|+\rangle$ and $|-\rangle$ in this step correspond to the secret bits 1 and 0 respectively (see expression (12)).

By this means Eve can obtain half of the secret bits sent by Alice after all the qubits in the positions in P are measured.

(E6) At last, Eve sends a fake sequence to Bob. In fact, this step is not necessary. From expressions (10) and (11) we can see that if Eve's measurement result on a certain qubit pair is $|\Phi^{-}\rangle$ or $|\Psi^{+}\rangle$, which happens with a probability of 1/2, Eve cannot obtain Alice's secret bit. In this condition Eve can never prepare a perfect fake qubit so that it introduces no error when Alice and Bob detect eavesdropping in step (5). It implies that the above attack will always be detected. As a result, Eve can send nothing to Bob in this step, which has no influence on the attack result. The reason why we list it here is just to make the attack strategy look unabridged.

As we discussed above, in a QSDC protocol the transmitted secret should not be leaked out whether the eavesdropping is detected or not. Therefore, SZZ protocol is insecure against this special attack because Eve can extract half of the secret bits though she would be discovered.

To understand this attack further, we recall the basic idea of it. In step (1) of SZZ protocol, Alice's sending qubits are in the states $|\psi\rangle_i^1 = \hat{U}_y(\theta_i)|0\rangle = \cos\theta_i|0\rangle - \sin\theta_i|1\rangle$, which looks as if Alice puts a lock $\hat{U}_y(\theta_i)$ on each carrier state $|0\rangle$. Similarly, in step (2) Bob also puts another lock $\hat{U}_y(\varphi_i)$ on each of them. Because θ_i and φ_i are randomly selected by Alice and Bob respectively, all locks can be removed only by the one who initially puts them on. Afterwards, Alice opens her locks by the operations $\hat{U}_y(-\theta_i)$ and encodes her secret bits by $\hat{U}_y\left(\pm\frac{\pi}{4}\right)$ in step (3). Finally Bob removes his locks by $\hat{U}_y(-\varphi_i)$ and then obtains the secret bits by measurements. To extract the transmitted bits, from the perspective of Eve who has no

keys to these locks, the only way is to acquire the qubits without any lock at a certain stage. For example, if Bob does not disorder the sequence when he sends it back to Alice in step (2), Eve can obtain the secret bits by intercepting the sequence sent by Alice in step (1), sending it back to Alice in step (2), and performing measurements when Alice sends it to Bob after her operation of unlocking and encoding in step (3). However, Bob will disorder the sequence before sending it in step (2). In this condition the simple attack would be invalid because Alice cannot remove her locks appropriately (the key and the lock for a certain qubit are not matched due to the order-restoring operation by Alice). To resolve this problem, as we introduced above, Eve can employ the technique of quantum teleportation. When Eve sends the fake sequence S_1^{E} to Alice as in step (E3), the role of the order-rearrangement encryption would be weakened because Eve can also adjust the order of his corresponding sequence S_2^{E} according to Bob's announcement as in step (E4). In the teleportation, if Eve acquires one of the results $\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$, she knows that the state of the corresponding qubit in Alice's hand would be one of $\{\hat{I}|\psi\rangle_i^1, \hat{\sigma}_z|\psi\rangle_i^1, \hat{\sigma}_x|\psi\rangle_i^1, \mathrm{i}\hat{\sigma}_y|\psi\rangle_i^1\}$ respectively. Here $\hat{I}, \hat{\sigma}_x, \hat{\sigma}_y$, and $\hat{\sigma}_z$ are four unitary operators as expressed below:

$$\hat{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \hat{\sigma}_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

$$\hat{\sigma}_y = \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix}, \text{ and } \hat{\sigma}_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{14}$$

At that time if the sequence is in the control of Eve, she can change each qubit into the (preferred) state $|\psi\rangle_i^1$ by one of the above operations and subsequently eliminate the influence of the order-rearrangement encryption completely. Unfortunately, all these qubits are in Alice's hand and Eve cannot achieve this goal. She has to wait for these qubits until Alice sends them out after her unlocking and coding operations. However, Eve can still extract secret information as described in step (E5) if she obtains $|\Phi^+\rangle$ or $|\Psi^-\rangle$ in a certain teleportation (i.e. the state of Alice's corresponding qubit is projected onto $\hat{I}|\psi\rangle_i^1$ or $\mathrm{i}\hat{\sigma}_y|\psi\rangle_i^1$), because both $\hat{I}$ and $\mathrm{i}\hat{\sigma}_y$ commute with Alice's operation $\hat{U}_y\left(-\theta_i \pm \frac{\pi}{4}\right)$, i.e. $[\hat{I}, \hat{U}_y(-\theta_i \pm \frac{\pi}{4})] = 0$ and $\left[\mathrm{i}\hat{\sigma}_y, \hat{U}_y\left(-\theta_i \pm \frac{\pi}{4}\right)\right] = 0$. On the contrary, since neither $\hat{\sigma}_x$ nor $\hat{\sigma}_z$ commutes with $\hat{U}_y\left(-\theta_i \pm \frac{\pi}{4}\right)$, i.e., $\left[\hat{\sigma}_x, \hat{U}_y\left(-\theta_i \pm \frac{\pi}{4}\right)\right] \neq 0$ and $\left[\hat{\sigma}_z, \hat{U}_y\left(-\theta_i \pm \frac{\pi}{4}\right)\right] \neq 0$, Eve cannot obtain secret information from those qubits which correspond to the Bell measurement results $|\Phi^-\rangle$ or $|\Psi^+\rangle$. The particular commutators are

$$[\hat{I}, \hat{U}_y(\Theta)] = \hat{I}\hat{U}_y(\Theta) - \hat{U}_y(\Theta)\hat{I} = 0, \tag{15}$$

$$\begin{aligned}[\mathrm{i}\hat{\sigma}_y, \hat{U}_y(\Theta)] =& \mathrm{i}\hat{\sigma}_y\hat{U}_y(\Theta) - \hat{U}_y(\Theta)\mathrm{i}\hat{\sigma}_y \\ =& \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \cos\Theta & \sin\Theta \\ -\sin\Theta & \cos\Theta \end{bmatrix} \\ & - \begin{bmatrix} \cos\Theta & \sin\Theta \\ -\sin\Theta & \cos\Theta \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = 0,\end{aligned} \tag{16}$$

$$\begin{aligned}[\hat{\sigma}_x, \hat{U}_y(\Theta)] =& \hat{\sigma}_x\hat{U}_y(\Theta) - \hat{U}_y(\Theta)\hat{\sigma}_x \\ =& \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \cos\Theta & \sin\Theta \\ -\sin\Theta & \cos\Theta \end{bmatrix} \\ & - \begin{bmatrix} \cos\Theta & \sin\Theta \\ -\sin\Theta & \cos\Theta \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \\ =& 2\sin\Theta \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix},\end{aligned} \tag{17}$$

and

$$\begin{aligned}[\hat{\sigma}_z, \hat{U}_y(\Theta)] =& \hat{\sigma}_z\hat{U}_y(\Theta) - \hat{U}_y(\Theta)\hat{\sigma}_z \\ =& \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} \cos\Theta & \sin\Theta \\ -\sin\Theta & \cos\Theta \end{bmatrix} \\ & - \begin{bmatrix} \cos\Theta & \sin\Theta \\ -\sin\Theta & \cos\Theta \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \\ =& 2\sin\Theta \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},\end{aligned} \tag{18}$$

where $\Theta = -\Theta_i \pm \frac{\pi}{4}$.

Now we consider how to improve the security of SZZ protocol against this special attack. To design a secure QSDC protocol, as pointed by Deng *et al*,[24] eavesdropping detection should be executed before the secret massage is encoded. Generally, this is a crucial point to realize a QSDC protocol with unconditional security. In the SZZ protocol, it may be expected that the security can be assured in different ways such as the techniques of blind polarization basis and random transmitting order. This is a good idea and nearly successful. Here we agree with Deng *et al* about the

viewpoints in Ref.[24] and try to add an additional detecting process before the encoding operation in the SZZ protocol. More specifically, before the operations $\hat{U}_y\left(-\theta_i \pm \frac{\pi}{4}\right)$ in Step (3), Alice samples some qubits randomly and requires Bob to declare his corresponding values of φ_i. Then Alice performs $\hat{U}_y(-\theta_i - \varphi_i)$ on each sampled qubit to remove the two "locks" on it. Afterwards Alice judges whether the state of each sampled qubit is $|0\rangle$ by a measurement in the basis $\{|0\rangle, |1\rangle\}$. If the error rate is small enough, Alice concludes that no eavesdropper exists and proceeds with other steps as in the SZZ protocol. In this condition the special attack will be useless because Eve's fake qubits cannot reach Alice's requirement in the additional detection.

In summary, we have analysed the security of the SZZ protocol and proposed an effective attack, i.e. teleportation attack, by which Eve can extract half of the secret bits. It is shown that, for an eavesdropper, quantum teleportation can be used to weaken the role of the order-rearrangement encryption in the SZZ protocol. Finally, by using an additional detection before encoding, we have modified this protocol to make it secure against this special attack.

References

[1] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
[2] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing* (New York: IEEE Press) p175
[3] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[4] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121
[5] Boström K and Felbinger T 2002 *Phys. Rev. Lett.* **89** 187902
[6] Deng F G, Long G L and Liu X S 2003 *Phys. Rev.* A **68** 042317
[7] Deng F G and Long G L 2004 *Phys. Rev.* A **69** 052319
[8] Lucamarini M and Mancini S 2005 *Phys. Rev. Lett.* **94** 140501
[9] Gao T, Yan F L and Wang Z X 2005 *Chin. Phys.* **14** 893
[10] Gao T, Yan F L and Wang Z X 2005 *Chin. Phys. Lett.* **22** 2473
[11] Man Z X, Zhang Z J and Li Y 2005 *Chin. Phys. Lett.* **22** 18
[12] Man Z X, Xia Y J and Nguyen B A 2006 *J. Phys.* B: *At. Mol. Opt. Phys.* **39** 3855
[13] Jin X R, Ji X, Zhang Y Q, Zhang S, Hong S K, Yeon K H and Um C I 2006 *Phys. Lett.* A **354** 67
[14] Zhu A D, Xia Y, Fan Q B and Zhang S 2006 *Phys. Rev.* A **73** 022338
[15] Wang J, Zhang Q and Tang C J 2006 *Phys. Lett.* A **358** 256
[16] Zhou J T, Pei W J, Wang K, Huang J and He Z Y 2006 *Phys. Lett.* A **358** 283
[17] Cao H J and Song H S 2006 *Chin. Phys. Lett.* **23** 290
[18] Wang G Y, Fang X M and Tan X H 2006 *Chin. Phys. Lett.* **23** 2658
[19] Ge H and Liu W Y 2007 *Chin. Phys. Lett.* **24** 2727
[20] Yang Y G, Wen Q Y and Zhu F C 2007 *Chin. Phys.* **16** 1838
[21] Li X H, Li C Y, Deng F G, Zhou P, Liang Y J and Zhou H Y 2007 *Chin. Phys.* **16** 2149
[22] Hoffmann H, Boström K and Felbinger T 2005 *Phys. Rev.* A **72** 016301
[23] Deng F G and Long G L 2005 *Phys. Rev.* A **72** 016302
[24] Deng F G, Li X H, Li C Y, Zhou P and Zhou H Y 2006 *Phys. Lett.* A **359** 359
[25] Zhang Y S, Li C F and Guo G C 2001 *Phys. Rev.* A **63** 036301
[26] Wójcik A 2003 *Phys. Rev. Lett.* **90** 157901
[27] Wójcik A 2005 *Phys. Rev.* A **71** 016301
[28] Gao F, Guo F Z, Wen Q Y and Zhu F C 2005 *Phys. Rev.* A **72** 036302
[29] Gao F, Guo F Z, Wen Q Y and Zhu F C 2005 *Phys. Rev.* A **72** 066301
[30] Deng F G, Li X H, Zhou H Y and Zhang Z J 2005 *Phys. Rev.* A **72** 044302
[31] Lo H K and Ko T M 2005 *Quantum Inf. Comput.* **5** 40
[32] Qin S J, Gao F, Wen Q Y and Zhu F C 2006 *Phys. Lett.* A **357** 101
[33] Gao F, Wen Q Y and Zhu F C 2007 *Phys. Lett.* A **360** 748
[34] Gao F, Qin S J, Wen Q Y and Zhu F C 2007 *Quantum Inf. Comput.* **7** 329
[35] Zhang Z J, Liu J, Wang D and Shi S H 2007 *Phys. Rev.* A **75** 026301
[36] Song J, Zhu A D and Zhang S 2007 *Chin. Phys.* **16** 621
[37] Kye W H, Kim C M, Kim M S and Park Y J 2005 *Phys. Rev. Lett.* **95** 040501
[38] Deng F G and Long G L 2003 *Phys. Rev.* A **68** 042315
[39] Zhu A D, Xia Y, Fan Q B and Zhang S 2006 *Phys. Rev.* A **73** 022338
[40] Gao F, Guo F Z, Wen Q Y and Zhu F C 2006 *Phys. Lett.* A **349** 53
[41] Bennett C H, Brassard G, Crépeau C, Jozsa R, Peres A and Wootters W K 1993 *Phys. Rev. Lett.* **70** 1895