**Rapid Communication**

# Cryptanalysis and improvement of a quantum secret sharing scheme based on $\chi$-type entangled states*

Zhu Zhen-Chao(朱珍超)[a)b)], Zhang Yu-Qing(张玉清)[b)†], and Fu An-Min(付安民)[b)]

[a)] *Information Security Research Center, Southeast University, Nanjing* 210096, *China*

[b)] *National Computer Network Intrusion Protection Center, Graduate University of Chinese Academy of Sciences, Beijing* 100049, *China*

(Received 13 May 2011; revised manuscript received 7 July 2011)

In the paper [2010 *Chin. Phys.* B **19** 050306], Yang *et al.* put forward a novel three-party quantum secret sharing protocol of secure direct communication based on $\chi$-type entangled states, they claimed that the scheme is secure. However, in this paper, we study the security of the protocol and find that it is insecure. Applying intercept and resend attack, the agent Bob can obtain Alice's secret without the help from the other agent Charlie. In the end, we give our effective modification for its improvement.

**Keywords:** quantum secret sharing, quantum entanglement, bell state nonorthogonal base

**PACS:** 03.67.Dd, 03.67.Hk, 03.65.Ud **DOI:** 10.1088/1674-1056/21/1/010307

Quantum cryptography exploits the principles of quantum mechanics to enable secure distribution of private information. In 1984, Bennett and Brassard used four quantum states to put forward the first quantum key distribution (QKD) protocol[1] in which two legitimate parties, Alice and Bob, generate a secret key over a long distance and use the secret key to encrypt and decrypt secret messages. Because there are many branches in classical cryptography, there are many other interesting branches of quantum cryptography too, such as quantum secure direction communication (QSDC), quantum secret sharing (QSS), and so on. Compared with QKD and QSDC, QSS has a more complex security analysis, for both the outside eavesdropper's and the inside dishonest agent's attacks must be considered. We know that the attack power of the dishonest agent is much stronger than the outside eavesdropper. Since the first QSS protocol[2] was proposed by Hillery, Bužek and Berthiaume in 1999, the design and security analysis of QSS protocols have attracted a great deal of attention.[3−28]

In a recent paper[29], Yang *et al.* put forward a novel three-party QSS protocol (we call it the Yang protocol) of secure direct communication based on genuine four-qubit $\chi$-type entangled states.[30,31] They claimed that the scheme is secure. However, in this paper, we study the security of this protocol and find that it is insecure. Applying intercept and resend attack, one agent Bob can obtain Alice's secret without help from the other agent Charlie. We will also give our effective modification to improve it in this paper.

To maintain the integrity of the paper, let us review some properties of the $\chi$-type states that will be used throughout this paper.

An orthogonal basis of four-qubit Hilbert space can be constructed by

$$\{|\chi^{ij}\rangle_{3124} = \sigma_3^i\sigma_1^j|\chi^{00}\rangle_{3124}|i,j=0,1,2,3,\},$$

where $\sigma^i$ ($\sigma^j$) is one of the four Pauli operators, i.e.,

$$\sigma^0 = |0\rangle\langle 0| + |1\rangle\langle 1|, \quad \sigma^1 = |0\rangle\langle 0| - |1\rangle\langle 1|,$$
$$\sigma^2 = |0\rangle\langle 1| + |1\rangle\langle 0|, \quad \sigma^3 = |0\rangle\langle 1| - |1\rangle\langle 0|,$$

and

$$|\chi^{00}\rangle_{3124} = \frac{1}{2\sqrt{2}}(|0000\rangle - |0011\rangle - |0101\rangle + |0110\rangle + |1001\rangle + |1010\rangle + |1100\rangle + |1111\rangle)_{3124}.$$

We also denote the set

$$\{|\chi^{ij}\rangle_{3124} = \sigma_3^i\sigma_1^j|\chi^{00}\rangle_{3124}|i,j=0,1,2,3,\}$$

as orthonormal basis set (FMB) as that in the Yang protocol.[29] The state $|\chi^{00}\rangle_{3124}$ can be rewritten in

*Project supported by the National Natural Science Foundation of China (Grant No. 60970140).

†Corresponding author. E-mail: zhangyq@gucas.ac.cn

© 2012 Chinese Physical Society and IOP Publishing Ltd

the following way simply by regrouping terms

$$|\chi^{00}\rangle_{3124} = \frac{1}{2}(|\Phi_1^-\rangle|0+\rangle + |\Phi_1^+\rangle|0-\rangle + |\Psi_1^-\rangle|1+\rangle + |\Psi_1^+\rangle|1-\rangle)_{3124}, \quad (1)$$

$$|\chi^{00}\rangle_{3124} = \frac{1}{2}(|\Phi_2^+\rangle|+0\rangle + |\Phi_2^-\rangle|-0\rangle - |\Psi_2^+\rangle|+1\rangle - |\Psi_2^-\rangle|-1\rangle)_{3124}. \quad (2)$$

Here,

$$|\Phi_1^\pm\rangle = \frac{1}{\sqrt{2}}(|\varphi^+\rangle \pm |\psi^-\rangle), \quad |\Psi_1^\pm\rangle = \frac{1}{\sqrt{2}}(|\varphi^-\rangle \pm |\psi^+\rangle),$$
$$|\Phi_2^\pm\rangle = \frac{1}{\sqrt{2}}(|\varphi^+\rangle \pm |\psi^+\rangle), \quad |\Psi_2^\pm\rangle = \frac{1}{\sqrt{2}}(|\psi^-\rangle \pm |\varphi^-\rangle),$$

where

$$|\varphi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), \quad |\psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle),$$
$$|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle).$$

The $|\Phi_1^\pm\rangle$ and $|\Psi_1^\pm\rangle$form an orthogonal basis $\mathrm{AMB}_1$ for the two-qubit Hilbert space, while $|\Phi_2^\pm\rangle$ and $|\Psi_2^\pm\rangle$ form another orthonormal basis $\mathrm{AMB}_2$ for the two-qubit Hilbert space. If the operation $H = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |1\rangle|0\rangle + |0\rangle\langle 1| - |1\rangle\langle 1|)$ is performed on qubits 2 and 4, the states in Eqs. (1) and (2) are transformed into the following states:

$$\begin{aligned}
&(I_3 \otimes I_1 \otimes H_2 \otimes H_4)|\chi^{00}\rangle_{3124} \\
&= (I_3 \otimes I_1 \otimes H_2 \otimes H_4)\frac{1}{2}(|\Phi_1^-\rangle|0+\rangle \\
&\quad + |\Phi_1^+\rangle|0-\rangle + |\Psi_1^-\rangle|1+\rangle + |\Psi_1^+\rangle|1-\rangle)_{3124} \\
&= \frac{1}{2}(|\Phi_1^-\rangle|+0\rangle + |\Phi_1^+\rangle|+1\rangle \\
&\quad + |\Psi_1^-\rangle|-0\rangle + |\Psi_1^+\rangle|-1\rangle)_{3124}, \quad (3)
\end{aligned}$$

$$\begin{aligned}
&(I_3 \otimes I_1 \otimes H_2 \otimes H_4)|\chi^{00}\rangle_{3124} \\
&= (I_3 \otimes I_1 \otimes H_2 \otimes H_4)\frac{1}{2}(|\Phi_2^+\rangle|+0\rangle \\
&\quad + |\Phi_2^-\rangle|-0\rangle - |\Psi_2^+\rangle|+1\rangle - |\Psi_2^-\rangle|-1\rangle)_{3124} \\
&= \frac{1}{2}(|\Phi_2^+\rangle|0+\rangle + |\Phi_2^-\rangle|1+\rangle \\
&\quad - |\Psi_2^+\rangle|0-\rangle - |\Psi_2^-\rangle|1-\rangle)_{3124}. \quad (4)
\end{aligned}$$

In the following, we provide a brief review of Yang protocol.[29]

(i) Alice and her two agents, Bob and Charlie, agree that each of the 16 mutually orthogonal $\chi$-type states $\{|\chi^{ij}\rangle_{3124}|i,j=0,1,2,3\}$ represents four-bit classical information. Alice prepares an ordered $N$ four-qubit $\chi$-type entangled state sequence according to her secret message and $i+j+k$ entangled particle quartets all in the state $|\chi^{00}\rangle_{3124}$ used for eavesdropping checks. Alice randomly inserts each of the $i+j+k$ checking photon quartets one by one into the ordered $N$ photon quartet sequence and records each position. Alice takes one particle from each entangled quartet to form four ordered particle sequences: $S_1 : [P_1^1, P_1^2, \ldots, P_1^{N+i+k+j}]$, $S_2 : [P_2^1, P_2^2, \ldots, P_2^{N+i+k+j}]$, $S_3 : [P_3^1, P_3^2, \ldots, P_3^{N+i+k+j}]$, $S_4 : [P_4^1, P_4^2, \ldots, P_4^{N+i+k+j}]$. Alice keeps particle sequences $S_1$ and $S_3$ while sending the particle sequences $S_2$ and $S_4$ to Bob.

(ii) Bob first inserts a filter in front of his devices to filter out the photon signals with an illegitimate wavelength to prevent invisible photon eavesdropping (IPE) Trojan horse attack strategies.[32,33] After Bob receives sequences $S_2$ and $S_4$, Alice publicly announces the positions of the $i$ checking entanglement quartets. For each of these $i$ checking quartets, Bob measures the corresponding checking photons in his laboratory by using the basis $\mathrm{BMB}_1$ ($\{|0+\rangle, |0-\rangle, |1+\rangle, |1-\rangle\}$) or the basis $\mathrm{BMB}_2$ ($\{|+0\rangle, |-0\rangle, |+1\rangle, |-1\rangle\}$) randomly and then publishes his measurement outcome. Then Alice measures the corresponding photons using the $\mathrm{AMB}_1$ basis or the $\mathrm{AMB}_2$ basis according to what Bob has published. If the error rate exceeds the threshold, the process is aborted. Otherwise, for each two corresponding photons in the same positions in sequences $S_2$ and $S_4$, Bob randomly generates five classical bits $B_1$, $B_2$, $B_3$, $B_4$, $B_5$, and then applies the operation $\sigma^{2B_1+B_2}$ and $\sigma^{2B_3+B_4}$ on qubits 2 and 4, respectively. Then he encrypts the particles by performing the operation $H^{B_5}$, respectively. Bob sends the ordered sequences $S_2$ and $S_4$ to Charlie.

(iii) To prevent IPE Trojan horse attack strategies, Charlie first does as Bob. After confirming that Charlie has received the ordered sequences $S_2$ and $S_4$, Alice publicly announces the positions of the $k$ quartets. For each of these $k$ quartets, Charlie measures the corresponding checking photons by using the $\mathrm{BMB}_1$ basis or the $\mathrm{BMB}_2$ basis randomly and publishes his measurement outcome. Then Alice lets Bob publish the unitary operation which he has performed on the checking photons. If Bob's unitary operation is $H$, then Alice measures the corresponding checking photons by using the corresponding basis according to Eqs. (3) and (4). Otherwise, she measures the photons using the corresponding basis according to Eqs. (1) and (2). If the error rate exceeds the threshold, the process is aborted. Otherwise, Alice sends the retained $N+j$ ordered $S_1'$ and $S_3'$($S_1'$ and $S_3'$ denote the remainder photons in the $S_1$ and $S_3$ sequences except

for eavesdropping check) sequences to Charlie.

(iv) After Charlie receives the photons, if Bob and Charlie collaborate, both Bob and Charlie can obtain the raw secret message including Alice's secret message and the additional $4j$ useless bits as follows. For each photon quartet, if Bob's unitary operation is $I$, then Bob and Charlie directly measure the particles in their sites in the basis FMB. If Bob's unitary operation is $H$, they first perform a Hadamard operation on the $S_2'$ and $S_4'$($S_2'$ and $S_4'$ denote the remainder photons in the $S_2$ and $S_4$ sequences except for eavesdropping check) photons and then performs a measurement on the quartet in the basis FMB and deduces the secret bits Alice has imposed on this photon quartet. However, if Bob and Charlie do not collaborate, neither of them can access to Alice's secret message.

(v) Alice publicly announces the positions of the retained $j$ checking quartets for Bob and Charlie to extract her exact secret message from the raw secret message and to check whether the sequences $S_1'$ and $S_3'$ travelling from Alice site to Charlie's site have been attacked, which is called message authentication.

Yang *et al.* claimed that the scheme is secure. However, they only considered the situation where the dishonest participant is Charlie,[29] agent Bob in the Yang protocol has more advantages in an attack than agent Charlie as Bob can cheat while Alice lets him publish the unitary operation which he has performed on the checking photons. Applying the intercept and resend attack, Bob can obtain Alice's secret without help from Charlie.

Now, let us give an outline of our attack strategy: in (ii), after having applied operations $\sigma^{2B_1+B_2}$ and $\sigma^{2B_3+B_4}$ on qubits 2 and 4 and encrypting these particles by performing the operation $H^{B_5}$ (actually, Bob does nothing to these photons, in other words, all the classical bits $B_1$, $B_2$, $B_3$, $B_4$, $B_5$ are 00000), Bob does not send the ordered sequences $S_2$ and $S_4$ to Charlie but stores these two sequences well, then Bob prepares $N+j+k$ entangled particle quartets all in the state $|\chi^{00}\rangle_{3124}$ as that Alice does, Bob takes out photons 2 and 4 from each entangled particle quartets and constitutes the ordered sequences $S_2^{\rm F}$ and $S_4^{\rm F}$, then Bob sends $S_2^{\rm F}$ and $S_4^{\rm F}$ to Charlie. It is obvious that Bob's cheat can escape the detection of Charlie's IPE Trojan horse attack strategies. After having obtained the positions of the $k$ checking entanglement quartets announced publicly by Alice and the basis and the measurement outcome of the corresponding checking photons (photons 2 and 4) announced publicly by Charlie, Bob measures the corresponding checking photons in the ordered sequences $S_2$ and $S_4$ by using the $\rm BMB_1$ basis or the $\rm BMB_2$ basis according to Charlie's choice. Through comparing the measurement outcome with Charlie's announcement, Bob can make sure the classical bits $B_1$, $B_2$, $B_3$, $B_4$, $B_5$ which he should publish. These classical bits accord with Alice's measurement outcome. The detailed procedure is as follows. Suppose that Charlie measures the corresponding checking photons by using the $\rm BMB_1$ basis and publishes his measurement outcome $|0-\rangle$, then for each $k$, checking entanglement quartets in the ordered sequences $S_2$ and $S_4$, Bob measures the corresponding checking photons by using the $\rm BMB_1$. If Bob's measurement outcome is $|0+\rangle$, Bob publishes the unitary operations that he has performed on the checking photons. They are $\sigma^0\otimes\sigma^1$, $\sigma^0\otimes\sigma^3$, $\sigma^1\otimes\sigma^1$ or $\sigma^1\otimes\sigma^3$ (the corresponding $B_1$, $B_2$, $B_3$, $B_4$, $B_5$ are 00010, 00110, 01010 or 01110). We will show that Bob is able to evade Alice's security check efficiently. Charlie's measurement outcome (the corresponding photons in the faked ordered sequences $S_2^{\rm F}$ and $S_4^{\rm F}$) is $|0-\rangle$, through the analysis of Eq. (1), we obtain that the state of the corresponding photons in the ordered sequences $S_1'$ and $S_2'$ is $|\Phi_1^+\rangle$, as Bob's measurement outcome is $|0+\rangle$, Bob can deduce that Alice's determinate measurement outcome in the next is $|\Phi_1^-\rangle$. We have the following equation:

$$\{\sigma^0\otimes\sigma^1,\sigma^0\otimes\sigma^3,\sigma^1\otimes\sigma^1,\sigma^1\otimes\sigma^3\}|0+\rangle=|0-\rangle. \quad (5)$$

We know that Bob's measurement has four possible outcomes and Charlie's measurement also has four possible outcomes if they all use the basis $\rm BMB_1$ and the operation $H^{B_5}$ is $H^0$. We give the following Table 1 to illustrate the relations among Bob's measurement outcome, Charlie's measurement outcome and Bob's local unitary operations in the above condition that they all use the basis $\rm BMB_1$ and the operation $H^{B_5}$ is $H^0$.

While Alice sends the retained $N+j$ ordered $S_1'$ and $S_3'$ sequences to Charlie, Bob intercepts the $S_1'$ and $S_3'$ sequences, Bob performs a direct measurement on the four-qubit quartet $S_3'S_1'S_2'S_4'$ ($S_2'$ and $S_4'$ denote the remainder photons in the $S_2$ and $S_4$ sequences except for eavesdropping check in the step (ii) and step (iii), respectively) in the basis FMB. According to the outcome, Bob performs the corresponding operations $\{\sigma_3^i\sigma_1^j|i,j=0,1,2,3,\}$ on the corresponding photons in sequences $S_1^{\rm F}$ and $S_3^{\rm F}$, then Bob sends the $S_1^{\rm F}$ and $S_3^{\rm F}$ sequences to Charlie. In the next, Bob can act as

a legal agent, agent Charlie and boss Alice cannot find Bob's cheat. However, Bob can access Alice's secret message without help from Charlie.

**Table 1.** The relations among Bob's measurement outcome, Charlie's measurement outcome and Bob's local unitary operations in the above condition that they all use the basis $\mathrm{BMB}_1$ and the operation $H^{B_5}$ is $H^0$. Charlie's measurement outcome is listed in the first row, Bob's measurement outcome is listed in the first column.

| | $\|0+\rangle$ | $\|0-\rangle$ | $\|1+\rangle$ | $\|1-\rangle$ |
|---|---|---|---|---|
| $\|0+\rangle$ | $\sigma^0\otimes\sigma^0;\sigma^0\otimes\sigma^2;$ $\sigma^1\otimes\sigma^0;\sigma^1\otimes\sigma^2$ | $\sigma^0\otimes\sigma^1;$ $\sigma^0\otimes\sigma^3;$ $\sigma^1\otimes\sigma^1;$ $\sigma^1\otimes\sigma^3$ | $\sigma^2\otimes\sigma^0;$ $\sigma^2\otimes\sigma^2;$ $\sigma^3\otimes\sigma^0;$ $\sigma^3\otimes\sigma^2$ | $\sigma^2\otimes\sigma^1;$ $\sigma^2\otimes\sigma^3;$ $\sigma^3\otimes\sigma^1;$ $\sigma^3\otimes\sigma^3$ |
| $\|0-\rangle$ | $\sigma^0\otimes\sigma^1;\sigma^0\otimes\sigma^3;$ $\sigma^1\otimes\sigma^1;\sigma^1\otimes\sigma^3$ | $\sigma^0\otimes\sigma^0;$ $\sigma^0\otimes\sigma^2;$ $\sigma^1\otimes\sigma^0;$ $\sigma^1\otimes\sigma^2$ | $\sigma^2\otimes\sigma^1;$ $\sigma^2\otimes\sigma^3;$ $\sigma^3\otimes\sigma^1;$ $\sigma^3\otimes\sigma^3$ | $\sigma^2\otimes\sigma^0;$ $\sigma^2\otimes\sigma^2;$ $\sigma^3\otimes\sigma^0;$ $\sigma^3\otimes\sigma^2$ |
| $\|1+\rangle$ | $\sigma^2\otimes\sigma^0;\sigma^2\otimes\sigma^2;$ $\sigma^3\otimes\sigma^0;\sigma^3\otimes\sigma^2$ | $\sigma^2\otimes\sigma^1;$ $\sigma^2\otimes\sigma^3;$ $\sigma^3\otimes\sigma^1;$ $\sigma^3\otimes\sigma^3;$ | $\sigma^0\otimes\sigma^0;$ $\sigma^0\otimes\sigma^2;$ $\sigma^1\otimes\sigma^0;$ $\sigma^1\otimes\sigma^2$ | $\sigma^0\otimes\sigma^1;$ $\sigma^0\otimes\sigma^3;$ $\sigma^1\otimes\sigma^1;$ $\sigma^1\otimes\sigma^3$ |
| $\|1-\rangle$ | $\sigma^2\otimes\sigma^1;\sigma^2\otimes\sigma^3;$ $\sigma^3\otimes\sigma^1;\sigma^3\otimes\sigma^3$ | $\sigma^2\otimes\sigma^0;$ $\sigma^2\otimes\sigma^2;$ $\sigma^3\otimes\sigma^0;$ $\sigma^3\otimes\sigma^2$ | $\sigma^0\otimes\sigma^1;$ $\sigma^0\otimes\sigma^3;$ $\sigma^1\otimes\sigma^1;$ $\sigma^1\otimes\sigma^3$ | $\sigma^0\otimes\sigma^0;$ $\sigma^0\otimes\sigma^2;$ $\sigma^1\otimes\sigma^0;$ $\sigma^1\otimes\sigma^2$ |

In Table 1, we only give the relations among Bob's measurement outcome, Charlie's measurement outcome and Bob's local unitary operations on the condition that they all use the basis $\mathrm{BMB}_1$ and the operation $H^{B_5}$ is $H^0$. We should point out that if Charlie measures the corresponding checking photons by using the $\mathrm{BMB}_2$ basis and publishes his measurement outcome, Bob will measure the corresponding checking photons in the ordered sequences $S_2$ and $S_4$ by using the $\mathrm{BMB}_2$ basis. Bob's measurement outcome, Charlie's measurement outcome and Bob's local unitary operations have similar relations. Charlie and Alice cannot find Bob's cheat too. However, Bob can access Alice's secret message without help from Charlie. Thus, this kind of attack is very effective to the protocol.

In the above attacks, Alice lets Bob publish which unitary operation he has performed on the checking photons after Alice has publicly announced the positions of the $k$ checking entanglement quartets and Charlie has published his measurement outcome. Bob can cheat on other parties by gathering this information and making an accurate comparison with his measurement outcome. Hence, to avoid the security flaw and maintain the good properties of the original protocol, we just need to make a small modification to the Yang protocol as follows: in step (iii), after confirming that Charlie has received the ordered sequences $S_2$ and $S_4$, Alice publicly announces the positions of the $k$ quartets. Alice first lets Bob publish the unitary operation which he has performed on the checking photons. Then Alice lets Charlie measure the corresponding checking photons.

As that discussed in Ref. [34], we should pay attention to a special attack, the dense-coding attack, which was proposed by Gao *et al.*[35] very recently. In the dense-coding attack,[35] the attacker Eve intercepts the single particle sequence (denoted as $B$) sent from center to Alice and replaces B by a fake sequence $B^1$, the sequence $B^1$ is composed of the first particle of the ordered EPR pairs generated by Eve, and Eve keeps the sequence $B$ and $C^1$, which is composed of the second particle of the ordered EPR pairs. The ordered EPR pairs generated by Eve are all in the state $|\psi^-\rangle_{B^1C^1}=\frac{1}{\sqrt{2}}(|01\rangle-|10\rangle)_{B^1C^1}$. After having performed local unitary rotation on the photons in the fake sequence $B^1$, Alice will send the sequence $B^1$ to the next agent Bob. Eve intercepts the sequence $B^1$ and then performs collective measurements on the photons in the sequence $B^1$ and the corresponding photons in the sequence $C^1$, then Eve performs local unitary rotations on every legal photons in the sequence $B$ according to the collective measurement result above. In this way, it seems that dense-coding attack is effective for the Yang protocol and our improved protocol, the only difference is that the sequence in these two protocols is not formed by single particles. However, unlike the protocols discussed in Ref. [35], in step (ii) of our protocol, after Bob has received the sequences, Alice will publicly announce the positions of the checking entanglement quartets. For each of these checking quartets, Bob measures the corresponding checking photons in his laboratory by using the basis $\mathrm{BMB}_1$ or the basis $\mathrm{BMB}_2$ randomly and then publishes his measurement outcome. In this case, if Eve replaces the sequences transmitted from Alice to Bob by fake sequences, after having measured the corresponding photons according to the Bob's announcement Alice can detect Eve's cheat. In the same way, Alice can detect Eve's cheat if Eve replaces the sequences transmitted from Bob (Alice) to Charlie (Bob) by fake sequences. So the protocol can resist the dense-coding attack.

In summary, we have shown that the three-party

QSS protocol proposed by Yang *et al.* cannot prevent Bob from legally obtaining secret messages without being detected. Finally, a possible way to avoid the security flaw is also presented.

# References


[1] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. Computers, Systems, and Signal Processing* (India: Bangalore) p. 175

[2] Hillery M, Bužek V and Berthiaume A 1999 *Phys. Rev.* A **59** 1829

[3] Karlsson A, Koashi M and Imoto N 1999 *Phys. Rev.* A **59** 162

[4] Cleve R, Gottesman D and Lo H K 1999 *Phys. Rev. Lett.* **83** 648

[5] Bandyopadhyay S 2000 *Phys. Rev.* A **62** 012308

[6] Tittel W, Zbinden H and Gisin N 2001 *Phys. Rev.* A **63** 042301

[7] Karimipour V, Bahraminasab A and Bagherinezhad S 2002 *Phys. Rev.* A **65** 042320

[8] Guo G P and Guo G C 2003 *Phys. Lett.* A **310** 247

[9] Deng F G, Long G L and Liu X S 2003 *Phys. Rev.* A **68** 042317

[10] Deng F G and Long G L 2004 *Phys. Rev.* A **69** 052319

[11] Xiao L, Long G L, Deng F G and Pan J W 2004 *Phys. Rev.* A **69** 052307

[12] Lance A M, Symul T, Bowen W P, Sanders B C and Lam P K 2004 *Phys. Rev. Lett.* **92** 177903

[13] Deng F G, Zhou H Y and Long G L 2005 *Phys. Lett.* A **337** 329

[14] Zhang Z J, Li Y and Man Z X 2005 *Phys. Rev.* A **71** 044301

[15] Deng F G, Li X H, Zhou H Y and Zhang Z J 2005 *Phys. Rev.* A **72** 044302

[16] Yan F L and Gao T 2005 *Phys. Rev.* A **72** 012304

[17] Zhang Z J and Man Z X 2005 *Phys. Rev.* A **72** 022303

[18] Li C Y, Zhou H Y, Wang Y and Deng F G 2005 *Chin. Phys. Lett.* **22** 1049

[19] Deng F G, Li X H, Li C Y, Zhou P and Zhou H Y 2005 *Phys. Rev.* A **72** 044301

[20] Deng F G, Li C Y , Li Y S, Zhou H Y and Wang Y 2005 *Phys. Rev.* A **72** 022338

[21] Wang C, Deng F G, Li Y S, Liu X S and Long G L 2005 *Phys. Rev.* A **71** 044305

[22] Li X H, Deng F G and Zhou H Y 2007 *Chin. Phys. Lett.* **24** 1151

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

[24] Yang Y G and Wen Q Y 2009 *Phys. Lett.* A **373** 396

[25] Yu Y F and Zhang Z M 2009 *Chin. Phys.* B **18** 1342

[26] Song T T, Zhang J, Gao F, Wen Q Y and Zhu F C 2009 *Chin. Phys.* B **18** 1333

[27] Wang C and Zhang Y 2009 *Chin. Phys.* B **18** 3238

[28] Gu B, Li C Q, Xu F and Chen Y L 2009 *Chin. Phys.* B **18** 4690

[29] Yang Y G, Cao W F and Wen Q Y 2010 *Chin. Phys.* B **19** 050306

[30] Yeo Y and Chua W K 2006 *Phys. Rev. Lett.* **96** 060502

[31] Wang X W and Yang G J 2008 *Phys. Rev.* A **78** 024301

[32] Cai Q Y 2006 *Phys. Lett.* A **351** 23

[33] Li X H, Deng F G and Zhou H Y 2006 *Phys. Rev.* A **74** 054302

[34] Zhu Z C, Zhang Y Q and Fu A M 2011 *Chin. Phys.* B **20** 40306

[35] Gao F, Qin S J, Guo F Z and Wen Q Y 2011 *IEEE J. Quant. Electron.* **47** 630