Efficient quantum secret sharing scheme with two-particle entangled states*

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

[a)] *Key Lab of Computer Networks and Information Security of Ministry of Education, Xidian University, Xi'an* 710071, *China*

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

(Received 1 July 2010; revised manuscript received 30 November 2010)

This paper proposes a protocol for multi-party quantum secret sharing utilizing four non-orthogonal two-particle entangled states following some ideas in the schemes proposed by Liu *et al.* (2006 *Chin. Phys. Lett.* **23** 3148) and Zhang *et al.* (2009 *Chin. Phys.* B **18** 2149) respectively. The theoretical efficiency for qubits of the new protocol is improved from 50% to approaching 100%. All the entangled states can be used for generating the private key except those used for the eavesdropping check. The validity of a probable attack called opaque cheat attack to this kind of protocols is considered in the paper for the first time.

Keywords: quantum secret sharing, quantum entanglement, Bell state nonorthogonal base

PACS: 03.67.Dd, 03.67.Hk, 03.65.Ud **DOI:** 10.1088/1674-1056/20/4/040306

Suppose that the president of a bank knows the combination that gives access to the banks vault, this vault has to be opened regularly; but unfortunately, the president is often away. Therefore, he or she wants the remaining staff to have access to the vault as well, but meanwhile, he or she does not want to tell them the combination individually. In the field of cryptography, this problem is known as secret sharing. In 1979, Shamir addressed a generalization of the above problem and proposed the first secret sharing scheme,[1] he used polynomials to show how to divide a secret into n shares such that at least t of those shares can be used to reconstruct the secret, while any $t-1$ or fewer shares have no information about the secret at all. This is an example of a (t, n) threshold scheme. We call these kinds of cryptosystems classical secret sharing schemes, which are designed on the basis of certain unproven computational assumptions such as the infeasibility of factoring large integers and solving discrete logarithms. Unfortunately, quantum algorithms are capable of factoring large integers and solving discrete logarithm,[2] with the rapid development of quantum computing technology many classical secret sharing schemes which are based on these unproven classical computational assumptions would become unsecure and worthless. Fortunately, when quantum mechanics enters the field of secret sharing, the story is changed; in contrast to classical secret sharing, the security of quantum secret sharing (QSS) relies on quantum mechanical principles rather than on computational complexity, the principles in quantum mechanics, such as the uncertainty relation, the correlation of entangled quantum systems and the collapse in quantum measurement, provide some novel ways for secure communication.

The original QSS scheme was proposed by Hillery, Bužek and Berthiaume (we called HBB quantum secret sharing protocol) in 1999,[3] accomplished by using a three-photon entangled Greenberger–Horne–Zeilinger (GHZ) state. Subsequently Karlsson, Koashi and Imoto (we called KKI QSS protocol) put forward another QSS scheme[4] with a two-photon polarization entangled state. Since these two QSS protocols[3,4] were presented, quantum secret sharing has progressed quickly in recent years.[5−30] In Ref. [31], Liu *et al.* proposed a protocol of quantum secret sharing with two-particle entangled state (we called LLLY protocol). By performing local unitary operations and individual measurements on either of two particles, the agents can finally share a

*Project supported by the Key Program of the National Natural Science Foundation of China (Grant No. 90718007) and the National Natural Science Foundation of China (Grant Nos. 60773135 and 60970140).

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

© 2011 Chinese Physical Society and IOP Publishing Ltd

secret key in the LLLY protocol. Because only simple two-particle entanglement sources as well as linear optical elements are employed in the LLLY protocol, the protocol seems secure and realizable with present-day. In a recent paper,[32] Zhang *et al.* presented a powerful attack against LLLY protocol, by applying entangled photons as fake signals, the attacker Eve could successfully steal the exact information without being revealed. They also gave an effective modification to improve the protocol (we called ZWHL protocol). However, the theoretical efficiency for qubits $\eta_{\rm q} = q_{\rm u}/q_{\rm t}$ in these two protocols is only 50%, because half of the instances are discarded as the last recipients choosing incompatible measuring bases (MBs), where $q_{\rm u}$ is the useful qubits and $q_{\rm t}$ is the total qubits transmitted.[33,34] We also point out that there is a serious problem existed in these two protocols, that is, having obtained the announcement of the operations' classification, the last recipients can make sure which runs are valid and then deduce all the information of the boss.

In this paper, we propose an efficient QSS scheme with four non-orthogonal two-particle entangled states instead of utilizing a certain state as that in LLLY protocol[31] and ZWHL protocol.[32] In our scheme, the last recipients of each particle send the photons to the boss Alice, Alice chooses some corresponding samples for checking–eavesdropping with the help of all the agents, so the above problem existed in LLLY protocol and ZWHL protocol does not exist in our protocol. In our protocol, all the Einstein–Podolsky–Rosen (EPR) pairs except those used for eavesdropping check are retained for secret sharing; the intrinsic theoretical efficiency for qubits is approaching 100%. Now, let us give the details of the QSS scheme.

(i) Alice prepares a sequence of entangled pairs randomly in one of the following four entangled states

$$\begin{aligned}
\left|\psi^+\right\rangle_{\rm BC} &= \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right)_{\rm BC},\\
\left|\phi^-\right\rangle_{\rm BC} &= \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right)_{\rm BC},\\
|+\rangle_{\rm BC} &= \frac{1}{\sqrt{2}}\left(\left|\phi^-\right\rangle + \left|\psi^+\right\rangle\right)_{\rm BC},\\
|-\rangle_{\rm BC} &= \frac{1}{\sqrt{2}}\left(\left|\phi^-\right\rangle - \left|\psi^+\right\rangle\right)_{\rm BC}. \qquad (1)
\end{aligned}$$

The inner products of these four entangled states satisfy the following relations:

$$\begin{aligned}
&\left\langle\psi^+\right|\left.\phi^-\right\rangle = 0, \quad \langle +|-\rangle = 0,\\
&\left|\left\langle\psi^+\right.|\pm\rangle\right|^2 = \left|\left\langle\phi^-\right.|\pm\rangle\right|^2 = \frac{1}{2}. \qquad (2)
\end{aligned}$$

So these four entangled states are not orthogonal, which forbids any one to copy them perfectly, same as that in Ref. [4]. Alice makes a record of the entangled states and sends the photons B to $\rm Bob_1$ and C to $\rm Charlie_1$ respectively.

(ii) As shown in Ref. [35], to improve the security of the protocol, $\rm Bob_1$ and $\rm Charlie_1$ must have the ability to detect a multi-photon 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.[36,37] When cascading the PNS or PBS, if there is only one photon in the original signal, they can only obtain one outcome, otherwise they will obtain two. For the invisible multiple photons,[35] all they 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. Then $\rm Bob_1$ and $\rm Charlie_1$ perform local unitary rotations U_{α_1} and U_{β_1} on the corresponding photons in the sequence B and C,

$$\begin{aligned}
U_{\alpha_1} &= \begin{pmatrix} \cos\alpha_1 & \sin\alpha_1 \\ -\sin\alpha_1 & \cos\alpha_1 \end{pmatrix},\\
U_{\beta_1} &= \begin{pmatrix} \cos\beta_1 & \sin\beta_1 \\ -\sin\beta_1 & \cos\beta_1 \end{pmatrix}, \qquad (3)
\end{aligned}$$

where $\alpha_1, \beta_1 \in \{0, \pi/4, \pi/2, 3\pi/4\}$. $\rm Bob_1$ and $\rm Charlie_1$ send the sequence B and sequence C to $\rm Bob_2$ and $\rm Charlie_2$ respectively.

(iii) Upon receiving the sequence B and sequence C from $\rm Bob_{\it i-1}$ and $\rm Charlie_{\it j-1}$ respectively, $\rm Bob_{\it i}$ and $\rm Charlie_{\it j}$ choose a subset of photons to detect the multi-photon signal as $\rm Bob_1$ and $\rm Charlie_1$, then they perform U_{α_i} and U_{β_j} on the corresponding photons in the sequences B and C respectively,

$$\begin{aligned}
U_{\alpha_i} &= \begin{pmatrix} \cos\alpha_i & \sin\alpha_i \\ -\sin\alpha_i & \cos\alpha_i \end{pmatrix},\\
U_{\beta_j} &= \begin{pmatrix} \cos\beta_j & \sin\beta_j \\ -\sin\beta_j & \cos\beta_j \end{pmatrix}, \qquad (4)
\end{aligned}$$

where $\alpha_i, \beta_j \in \{0, \pi/4, \pi/2, 3\pi/4\}$. $\rm Bob_{\it i}$ and $\rm Charlie_{\it j}$ send the sequences B and C to $\rm Bob_{\it i+1}$ and $\rm Charlie_{\it j+1}$ respectively.

(iv) $\rm Bob_{\it m}$ and $\rm Charlie_{\it n}$ send the sequences B and C to Alice. Alice chooses a subset of photons to detect the multi-photon signal as $\rm Bob_1$ and $\rm Charlie_1$. Alice chooses some corresponding samples from the

sequences B and C for checking–eavesdropping. That is, all the agents publicly announce their operation information α_i, β_j corresponding to the samples in a random sequential order. Alice makes the deterministic measurements on the samples according to the operation information performed on the samples by all the agents and the initial states of the samples. Alice makes the error rate analysis of the transmission. If Alice confirms that the transmissions are secure, she publishes the initial states of the remaining entangled pairs. The remaining final states of entangled pairs can be used for secret sharing. If and only if all these $m+n$ partners cooperate (all the partners keep their values of operation information as secret bits; when all these $m+n$ partners want to cooperate to recover the secret, they may choose a special agent who is in charge of the secret recovery; then other agents safely transmit their secret bits to this special agent), can they deduce the secret sharing.

Now, let us think about why the secret sharing can be completed. After passing by all the agents (Bob_i and $\mathrm{Charlie}_j$, $i = 1, 2, \ldots, m; j = 1, 2, \ldots, n$), the rotations by different partners are independent, Alice's entangled pair is in the set of the following states

$$
\begin{aligned}
&U_{\alpha_1}U_{\alpha_2}\ldots, U_{\alpha_m} \otimes U_{\beta_1}U_{\beta_2}\ldots, U_{\beta_n} \\
&\times \left\{\left|\psi^+\right\rangle, \left|\phi^-\right\rangle, |+\rangle, |-\rangle\right\} \\
&= \prod_{i=1}^{m} \begin{pmatrix} \cos\alpha_i & \sin\alpha_i \\ -\sin\alpha_i & \cos\alpha_i \end{pmatrix} \otimes \prod_{j=1}^{n} \begin{pmatrix} \cos\beta_j & \sin\beta_j \\ -\sin\beta_j & \cos\beta_j \end{pmatrix} \\
&\times \left\{\left|\psi^+\right\rangle, \left|\phi^-\right\rangle, |+\rangle, |-\rangle\right\} \\
&= \begin{pmatrix} \cos\sum\limits_{i=1,2,\ldots,m} \alpha_i & \sin\sum\limits_{i=1,2,\ldots,m} \alpha_i \\ -\sin\sum\limits_{i=1,2,\ldots,m} \alpha_i & \cos\sum\limits_{i=1,2,\ldots,m} \alpha_i \end{pmatrix} \\
&\otimes \begin{pmatrix} \cos\sum\limits_{j=1,2,\ldots,n} \beta_j & \sin\sum\limits_{j=1,2,\ldots,n} \beta_j \\ -\sin\sum\limits_{j=1,2,\ldots,n} \beta_j & \cos\sum\limits_{j=1,2,\ldots,n} \beta_j \end{pmatrix} \\
&\times \left\{\left|\psi^+\right\rangle, \left|\phi^-\right\rangle, |+\rangle, |-\rangle\right\}. \qquad (5)
\end{aligned}
$$

As we know that $\alpha_i, \beta_j \in \{0, \pi/4, \pi/2, 3\pi/4\}$, so we can deduce that $\sum\limits_{i=1,2,\ldots,m} \alpha_i \bmod \pi$,

$$
\sum_{j=1,2,\ldots,n} \beta_j \bmod \pi \in \left\{0, \frac{\pi}{4}, \frac{\pi}{2}, \frac{3\pi}{4}\right\}
$$

and

$$
\begin{pmatrix} \cos\sum\limits_{i=1,2,\ldots,m} \alpha_i & \sin\sum\limits_{i=1,2,\ldots,m} \alpha_i \\ -\sin\sum\limits_{i=1,2,\ldots,m} \alpha_i & \cos\sum\limits_{i=1,2,\ldots,m} \alpha_i \end{pmatrix}
$$

$$
\begin{aligned}
&\otimes \begin{pmatrix} \cos\sum\limits_{j=1,2,\ldots,n} \beta_j & \sin\sum\limits_{j=1,2,\ldots,n} \beta_j \\ -\sin\sum\limits_{j=1,2,\ldots,n} \beta_j & \cos\sum\limits_{j=1,2,\ldots,n} \beta_j \end{pmatrix} \\
&\times \left\{\left|\psi^+\right\rangle, \left|\phi^-\right\rangle, |+\rangle, |-\rangle\right\} \\
&= \left\{\left|\psi^+\right\rangle, \left|\phi^-\right\rangle, |+\rangle, |-\rangle\right\}. \qquad (6)
\end{aligned}
$$

The final states of the remaining entangled pairs can be determined by the initial states and all agents' operation information. After Alice has published the initial states of the remaining entangled pairs, the final states of the remaining entangled pairs are only determined by the operation information of all the agents. The special agent who is in charge of the secret recovery can recover the secret with the help of the other agents. As a result, the secret sharing can be completed

Compared with quantum key distribution (QKD) protocols, which is the most promising branch of quantum cryptography, the security of QSS is much more complicated. In QKD, the problem of security is mainly preventing eavesdropping of an active external eavesdropper. However, in QSS, both the onslaught of an external eavesdropper and the participant's attack threaten the security; the qubits are usually passed by the agents which means eavesdropper 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.

As the security of the proposed scheme is based on the public statistical analysis of the error rate of the samples chosen randomly by Alice, it must be guaranteed against an eavesdropper (especially the dishonest agent, we know that the QSS scheme is secure if the scheme is secure to insider attack.) with unlimited computing power whose technology is limited only by the laws of quantum mechanics.[38] Without loss of generality, we assume that the dishonest agent is Bob_i, $i = 1, 2, \ldots, m$. If Bob_i tries to attack on one of the two entangled particles, which will introduce errors that Alice will discover by publicly comparing the error rates of the samples in the checking–eavesdropping process. Also, Bob_i's measurement on the states of either particle (received by any agents or the boss Alice) will give no information since the state of the particle is unclear. Even though Bob_i intercepts the corresponding two entangled particles and then performs Bell measurement, we know that the four states $\left|\psi^+\right\rangle, \left|\phi^-\right\rangle, |+\rangle$ and $|-\rangle$ belong to two different bases, as for the following two reasons: i) each entangled

particle is chosen randomly in one of the four states $|\psi^+\rangle, |\phi^-\rangle, |+\rangle$ and $|-\rangle$; ii) α and β are chosen randomly from $\{0, \pi/4, \pi/2, 3\pi/4\}$. So Bob_i measures on the states in a wrong basis with a probability 1/2. In the case that there are L agents which are dishonest in the protocol, where $1 \leq L \leq m+n-1$, these L agents cooperate and share among themselves their operation information, through the analysis of the protocol, the operation information randomly chosen by other $m+n-L$ agents will also make the intermediate (the final) entangled pairs received by the agents (Alice) randomly in one of the four states $|\psi^+\rangle, |\phi^-\rangle, |+\rangle$ and $|-\rangle$, this will make these L agents cannot steal Alice's information through performing Bell measurement on the corresponding two entangled particles.

We should pay attention to a special attack, the dense-coding attack, which was proposed by Gao *et al.*[39] very recently. In the dense-coding attack,[39] the attacker Eve intercepts the sequence B (or C) sent from Bob_{i-1} (or Charlie_{j-1}) to Bob_i (or Charlie_j) and replaces B (or C) by a fake sequence B^1 (or C^1), the sequence B^1 (or C^1) is composed of the first particles of the ordered EPR pairs generated by Eve, Eve keeps the sequence B^2 (or C^2), which is composed by the second particles of the ordered EPR pairs and the sequence B (or C) in his hand, the ordered EPR pairs are in the state $|\psi^-\rangle_{\text{BC}} = (1/\sqrt{2})(|01\rangle - |10\rangle)_{\text{BC}}$. After having performed local unitary rotation U_{α_i} (or U_{β_j}) on the photons in the fake sequence B^1 (or C^1), Bob_i (or Charlie_j) will send the sequence B^1 (or C^1) to the next agent. Eve intercepts the sequence B^1 (or C^1) and then performs collective measurements on every pair of the photons in the sequence B^1 (or C^1) and the corresponding photons in the sequence B^2 (or C^2), then Eve performs local unitary rotations on every legal photons in the sequence B (or C) according to the collective measurement result as mentioned above. In this way, it seems that the attacker Eve can obtain all the agents' operation information and our scheme is completely unsecure. However, through carefully analysing the following equations, we find that the four possible states of the corresponding EPR pairs are not orthogonal

$$\left\{ \begin{pmatrix} \cos\alpha_i & \sin\alpha_i \\ -\sin\alpha_i & \cos\alpha_i \end{pmatrix}_{\alpha_i \in \left\{0, \frac{\pi}{4}, \frac{\pi}{2}, \frac{3\pi}{4}\right\}} \right\} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \frac{\sqrt{2}}{2} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \frac{\sqrt{2}}{2} \begin{pmatrix} -1 & 1 \\ -1 & -1 \end{pmatrix} \right\}, \quad (7)$$

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes I, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \otimes I, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \otimes I, \frac{1}{\sqrt{2}} \begin{pmatrix} -1 & 1 \\ -1 & -1 \end{pmatrix} \otimes I \right\} |\psi^-\rangle_{\text{BC}}$$

$$= \left\{ \begin{array}{l} |\psi^-\rangle_{\text{BC}} = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)_{\text{BC}}, |\phi^+\rangle_{\text{BC}} = \frac{1}{2}(|11\rangle + |00\rangle)_{\text{BC}}, \\ |\Omega^+\rangle_{\text{BC}} = \frac{1}{\sqrt{2}}(|\phi^+\rangle + |\psi^-\rangle)_{\text{BC}}, |\Omega^-\rangle_{\text{BC}} = \frac{1}{\sqrt{2}}(|\phi^+\rangle - |\psi^-\rangle)_{\text{BC}} \end{array} \right\}. \quad (8)$$

These four states satisfy the following equations

$$\begin{aligned} &\langle\psi^- | \phi^+\rangle = 0, \\ &\langle\Omega^- | \Omega^+\rangle = 0, \\ &|\langle\psi^- | \Omega^\pm\rangle|^2 = |\langle\phi^+ | \Omega^\pm\rangle|^2 = \frac{1}{2}. \end{aligned} \quad (9)$$

Obviously, these four states are not orthogonal. It is easy to verify that the final four possible states are not orthogonal while the fake EPR pairs generated by Eve are in the state $|\psi^+\rangle_{\text{BC}}, |\phi^-\rangle_{\text{BC}}$ or $|\phi^+\rangle_{\text{BC}}$ respectively which will forbid the attacker Eve to copy them perfectly. So the scheme is secure against dense-coding attack.

Through the above analyses, we believe that if and only if all the $m+n$ partners cooperate can they deduce the secret sharing in our protocol. Even if Eve (or the dishonest agent) only wants to disturb the transmission (i.e., denial of service attack) without considering of being discovered, he/she cannot obtain any useful information about the secret messages. As in the ZWHL protocol, to make sure the protocol secure against invisible photon eavesdropping attack and the delay-photon Trojan horse attacker, we have adopted PNS technology and added wavelength filters in every receiver's laboratory in the protocol.

In Ref. [40], Deng *et al.* presented an opaque cheat attack scheme which reveals that a class of QSS schemes based on entanglement and collective eavesdropping check are completely insecure if the transmission efficiencies of the schemes are lower than 50%. The dishonest agent can eavesdrop fully and freely, including the two original works, the HBB scheme[3]

and the KKI scheme.[4] Through the analysis, it seems that opaque cheat attack is effective to our proposed protocol, LLLY protocol and ZWHL protocol. Fortunately, the transmission efficiencies of most protocols with present-day in quantum private communication are higher than 50%. For example, the error rates threshold of commercial quantum encryption transmission systems based on BB84[41] are usually defined as 20%, that is, if the error rate is higher than 20%, we determine that the transmission is unsecure; in other words, the transmission efficiency of this system based on BB84 is at least more than 80%. In a recent experiment, Jin *et al.* have succeeded in transporting quantum information over a free space distance of 16 km,[42] much further than the few hundred meters previously achieved, which brings us closer to transmitting information over long distances without the need for a traditional signal. The average fidelity of the teleportation achieved was 89 % in this experiment.

Recently, Xu *et al.* showed that classical and quantum correlations can remain unaffected under certain decoherence areas,[43] which will have important roles in distinguishing correlations and designing robust quantum protocols based only on quantum correlation. The early conjecture that classical correlation is always found to be larger than the entanglement and non-entanglement quantum correlation in the experiment is disproved by their experimental results. They also showed that the sudden change in behaviour in the decay rates of correlations and their immunity against certain decoherences. This finding will greatly reduce the interaction between correlated systems and the environment, so the transmission efficiencies of the corresponding quantum protocols based on entangled photons will be great improved in the future, including our QSS protocol proposed in the paper. Through the above analyses, we believe that our proposed protocol in this paper is secure against opaque cheat attack both now and in the future.

In conclusion, we have proposed an efficient QSS scheme with four non-orthogonal two-particle entangled states instead of utilizing a certain state; in the protocol, the last recipients of each particles send the photons to the boss Alice, Alice chooses some corresponding samples for checking–eavesdropping with the help of all the agents. Invisible photon eavesdropping attack, the delay-photon Trojan horse attack and dense-coding attack can be counterchecked. The validity of a probable attack called opaque cheat attack to this kind of protocols is also considered in the paper. All the EPR pairs except those used for eavesdropping check can be retained for secret sharing; the intrinsic theoretical efficiency for qubits of the protocol is approaching 100%.

Acknowledgement

The first author is grateful to Dr. Gao Fei for his helpful discussions on the security of the scheme.

References

[1] Shamir A 1979 *Comm. ACM.* **22** 612
[2] Shor P W 1994 *Proc. 35th Annual Symp. on Foundations of Computer Science* (New York: IEEE) p. 124
[3] Hillery M, Bužek V and Berthiaume A 1999 *Phys. Rev.* A **59** 1829
[4] Karlsson A, Koashi M and Imoto N 1999 *Phys. Rev.* A **59** 162
[5] Cleve R, Gottesman D and Lo H K 1999 *Phys. Rev. Lett.* **83** 648
[6] Bandyopadhyay S 2000 *Phys. Rev.* A **62** 012308
[7] Tittel W, Zbinden H and Gisin N 2001 *Phys. Rev.* A **63** 042301
[8] Karimipour V, Bahraminasab A and Bagherinezhad S 2002 *Phys. Rev.* A **65** 042320
[9] Guo G P and Guo G C 2003 *Phys. Lett.* A **310** 247
[10] Deng F G, Long G L and Liu X S 2003 *Phys. Rev.* A **68** 042317
[11] Deng F G and Long G L 2004 *Phys. Rev.* A **69** 052319
[12] Xiao L, Long G L, Deng F G and Pan J W 2004 *Phys. Rev.* A **69** 052307
[13] Lance A M, Symul T, Bowen W P, Sanders B C and Lam P K 2004 *Phys. Rev. Lett.* **92** 177903
[14] Deng F G, Zhou H Y and Long G L 2005 *Phys. Lett.* A **337** 329
[15] Zhang Z J, Li Y and Man Z X 2005 *Phys. Rev.* A **71** 044301
[16] Deng F G, Li X H, Zhou H Y and Zhang Z J 2005 *Phys. Rev.* A **72** 044302
[17] Yan F L and Gao T 2005 *Phys. Rev.* A **72** 012304
[18] Zhang Z J and Man Z X 2005 *Phys. Rev.* A **72** 022303
[19] Li C Y, Zhou H Y, Wang Y and Deng F G 2005 *Chin. Phys. Lett.* **22** 1049
[20] Deng F G, Li X H, Li C Y, Zhou P and Zhou H Y 2005 *Phys. Rev.* A **72** 044301
[21] Deng F G, Li C Y, Li Y S, Zhou H Y and Wang Y 2005 *Phys. Rev.* A **72** 022338
[22] Wang C, Deng F G, Li Y S, Liu X S and Long G L 2005 *Phys. Rev.* A **71** 044305

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

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

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

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

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

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

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

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

[31] Liu W T, Liang L M, Li C Z and Yuan J M 2006 *Chin. Phys. Lett.* **23** 3148

[32] Zhang B B, Wang D Q, Huang S S and Liu Y 2009 *Chin. Phys.* B **18** 2149

[33] Long G L and Liu X S 2002 *Phys. Rev.* A **65** 032302

[34] Cabello A 2000 *Phys. Rev. Lett.* **85** 5635

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

[36] Deng F G, Zhou P, Li X H, Li C Y and Zhou H Y 2005 *arXiv:quant-ph*/0508168

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

[38] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)

[39] Gao F, Qin S J, Guo F Z and Wen Q Y 2010 *arXiv: quant-ph*/1009.2545

[40] Deng F G, Li X H and Zhou H Y 2007 *arXiv: quant-ph*/07050279

[41] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing* (New York: IEEE) p. 175

[42] Jin X M, Ren J G, Yang B, Yi Z H, Zhou F, Xu X F, Wang S K, Yang D, Hu Y F, Jiang S, Yang T, Yin H, Chen K, Peng C Z and Pan J W 2010 *Nat. Photonics* **4** 376

[43] Xu J S, Xu X Y, Li C F, Zhang C J, Zou X B and Guo G C 2010 *Nat. Commun.* **1** 7