Vol 18 No 6, June 2009
1674-1056/2009/18(06)/2137-06
Chinese Physics B
© 2009 Chin. Phys. Soc.
and IOP Publishing Ltd

Multiparty quantum secret conference based on quantum encryption with pure entangled states*

Gu Bin(顾 斌)†, Li Chuan-Qi(李传起), and Chen Yu-Lin(陈玉林)

College of Math and Physics, Nanjing University of Information Science and Technology, Nanjing 210044, *China*

(Received 8 October 2008; revised manuscript received 11 November 2008)

We present a scheme for multiparty quantum remote secret conference (MQRSC) with pure entangled states, not maximally entangled multipartite quantum systems. The conferees first share a private quantum key, a sequence of pure entangled states and then use them to encode and decode the secret messages. The conferees exploit the decoy-photon technique to ensure the security of the transmission of qubits. This MQRSC scheme is more feasible and efficient than others.

Keywords: quantum secret conference, pure entangled states, quantum encryption
PACC: 0367

The principles in quantum mechanics, such as the uncertain relation, the correlation of entangled quantum systems and the collapse in quantum measurement, provide some novel ways for secure communication. For instance, quantum key distribution (QKD), whose goal is used to create a private key between two authorized users, has become one of the most mature applications of quantum information techniques.[1−9] Quantum secret sharing (QSS) supplies a secure way not only for sharing a classical message[10−16] but also for sharing an unknown quantum state.[17−24] Quantum secure direct communication, which is used to transmit a secret message directly, has also attracted a lot of attention.[25−33] As pointed out by Deng and Long,[25−27] for direct communication, the quantum states should be transmitted in a block by block way, similar to QKD proposed by Long and Liu.[3] This feature provides a chance for the two legitimate users to complete the error rate analysis before they encode the secret message on the quantum states transmitted. It is, now, applied for a secret report in which many agents report, directly and securely, their secret messages to a boss in a one-way direction,[34] and for broadcast communication[35] with which one can broadcast their secret message securely to many legitimate receivers. Another branch of quantum communication used for transmitting a secret message is called deterministic secure quantum communication (DSQC)[36] in which the legitimate receiver can, on one hand, read out each message qubit with at least a bit of classical message exchanged.[36−44] On the other hand, it is more feasible to transmit a secret message with the present techniques as the noise in the quantum channel.[36]

Recently, Li *et al* [45] presented a good way for multiparty quantum remote secret conference (MQRSC) with multi-particle Greenberger–Horne–Zeilinger (GHZ) states and quantum memory. In a secret conference, any legitimate conferee can send securely his secret message to the other legitimate parties who participate in a remote secret conference, but a vicious eavesdropper can get nothing about the messages. They[45] exploit some controlled-not (CNOT) gates to encrypt and decrypt their secret message with a quantum key, a sequence of GHZ states which can be used repeatedly after confirming their security. Different from QSS,[10−24] all the conferees are honest and they can exploit the correlation of GHZ states to check eavesdropping securely. Moreover, every legitimate conferee can decode the quantum information, not just resort to the cooperation by all the agents in the latter. Also, there are some differences between MQRSC and QSDC. First, it is unnecessary for most parties to have the capability of possessing quantum

*Project supported by the National Natural Science Foundation of China (Grant No 10847147), the Natural Science Foundation of Jiangsu Province (Grant No BK2008437) and Jiangsu Provincial Universities (Grant No 07KJB510066) and the Science Foundation of Nanjing University of Information Science and Technology.
†Corresponding author. E-mail: gubin@nuist.edu.cn

signal sources, in particular an entangled quantum source in MQRSC. Second, MQRSC is more efficient than QSDC when it is used for sharing quantum information among some legitimate conferees. When it is used for create a private key among the legitimate parties, MQRSC is more efficient than QKD.

In this paper, we present an MQRSC scheme with quantum encryption by using a sequence of pure entangled states as the quantum key, following some ideas in Refs.[30] and [45]. We use some decoy photons[46] to share the quantum key securely among all the legitimate conferees. Similar to Ref.[45], each of the legitimate conferees can use the quantum key shared with others to encode and decode the secret message. As the asymmetry of the entangled quantum source in a practical experiment, this scheme with a pure entangled quantum-signal source is more feasible than that with a maximally entangled source in Ref.[30] at present and also any eavesdropper cannot steal the message in this scheme. As the security of all the transmission is ensured with decoy photons, all the photons in the quantum key can be used repeatedly, which makes this scheme more efficient than the original one.[45]

A GHZ-like state can be described as

$$|\psi\rangle_{ABC} = \alpha|0\rangle_A|0\rangle_B|0\rangle_C + \beta|1\rangle_A|1\rangle_B|1\rangle_C, \qquad (1)$$

where $|0\rangle$ and $|1\rangle$ represent the horizontal polarization $|H\rangle$ and the vertical polarization $|V\rangle$, respectively. $|\alpha|^2 + |\beta\rangle^2 = 1$ and $\alpha\beta \neq 0$. The subscripts A, B and C represent the three photons in this GHZ-like state. The three photons are correlated with the basis $Z = \{|0\rangle, |1\rangle\}$, but not the basis $X = \{|+x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-x\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$ as

$$\begin{aligned}|\psi\rangle_{ABC} = \frac{1}{2\sqrt{2}}\{&(\alpha+\beta)(|+x\rangle_A|+x\rangle_B|+x\rangle_C \\ &+|+x\rangle_A|-x\rangle_B|-x\rangle_C+|-x\rangle_A|+x\rangle_B|-x\rangle_C+|-x\rangle_A|-x\rangle_B|+x\rangle_C) \\ &+(\alpha-\beta)(|+x\rangle_A|+x\rangle_B|-x\rangle_C+|+x\rangle_A|-x\rangle_B|+x\rangle_C \\ &+|-x\rangle_A|+x\rangle_B|+x\rangle_C+|-x\rangle_A|-x\rangle_B|-x\rangle_C)\}. \end{aligned} \qquad (2)$$

Usually, the coefficient α does not equal β, which means the three photons in the state $|\psi\rangle_{ABC}$ do not have a deterministic correlation with the basis X.

For MQRSC, the three legitimate conferees Alice, Bob and Charlie should first share a sequence of pure entangled states securely and then use them as the quantum key for encoding and decoding the messages, similar to those in the first quantum secret conference scheme.[45] Although the three conferees cannot exploit the correlation of the three photons in the GHZ-like state $|\psi\rangle_{ABC}$ to share a quantum key, a sequence of pure entangled three-photon states, they can prepare some decoy photons[45] for checking eavesdropping during the process of sharing their quantum key.

Suppose that Alice possesses a quantum source which can produce the pure entangled three-photon state $|\psi\rangle_{ABC}$. She prepares k three-photon quantum systems which are randomly in one of the two states $\{|\psi\rangle_{ABC}, |\psi'\rangle_{ABC}\}$. Here $|\psi'\rangle_{ABC} = \beta|0\rangle_A|0\rangle_B|0\rangle_C + \alpha|1\rangle_A|1\rangle_B|1\rangle_C$ which can be prepared by flipping the bit values of the three photons in the state $\alpha|0\rangle_A|0\rangle_B|0\rangle_C + \beta|1\rangle_A|1\rangle_B|1\rangle_C$, i.e., $(\sigma_x^A \otimes \sigma_x^B \otimes \sigma_x^C)|\psi\rangle_{ABC} = |\psi'\rangle_{ABC}$, similar to Ref.[36]. Alice divides all the photons into three photon sequences, say S_A, S_B and S_C. S_A is composed of the photons A picked out by Alice from each quantum system in the state $|\psi\rangle_{ABC}$ or $|\psi'\rangle_{ABC}$, i.e., $S_A = [A_1, A_2, \cdots, A_k]$, the same as in Refs.[3] and [25]. The other two partner photons compose the sequences $S_B = [B_1, B_2, \cdots, B_k]$ and $S_C = [C_1, C_2, \cdots, C_k]$, respectively.

For efficiently checking eavesdropping, Alice should prepare some decoy photons and then insert them into the two sequences S_B and S_C randomly, the same as in Ref.[36]. Each of the decoy photons[46] can be prepared randomly in the four nonorthogonal states $\{|0\rangle, |1\rangle, |+x\rangle, |-x\rangle\}$. She can use the same method as that in Ref.[36] to get her decoy photons. It is necessary for the three conferees to exploit the decoy-photon technique[46] for sharing a sequence of pure entangled three-photon states; otherwise, an eavesdropper, for example Eve, can share the quantum key with the three conferees by entangling an

auxiliary photon with the quantum system shared by the three legitimate conferees. This action cannot be detected by the three conferees with the correlation of the quantum system in a GHZ-like state. Eve needs only to perform a controlled-not (CNOT) operation on her auxiliary photon and the photon B in each GHZ-like state. However, with decoy photons, this action will leave a trace in the samples for eavesdropping check and can be easily detected by the three conferees as the action done by Eve on the decoy photons is the same as that on the photons in the famous BB84 QKD protocol.[2]

Now, let us introduce the principle of our MQRSC scheme in detail, following some ideas in Refs.[45] and [30]. In essence, we only use a feasible entangled source, instead of the maximally entangled one in the latter. Simultaneously, the legitimate conferees can exploit the decoy-photon technique to ensure the security of the processes of both sharing a quantum key and transmitting their secret messages. All the steps of our scheme can be described as follows.

(i) The conferees create a private quantum key, a sequence of GHZ-like states. All these GHZ-like states are $|\psi\rangle_{ABC}$ or $|\psi'\rangle_{ABC}$. That is, Alice, Bob and Charlie will obtain the same outcome if they measure their photons in the state with the basis Z. In detail, Alice prepares a sequence of GHZ-like states and divides all the photons into three sequences, say S_A, S_B and S_C. All the photons A in these GHZ-like states make up the sequence S_A, so do the sequences S_B and S_C. Also Alice prepares some decoy photons and inserts them into the two sequences S_B and S_C randomly. Alice sends the sequence S_B to Bob and the sequence S_C to Charlie. After Bob and Charlie receive their photon sequences, Alice tells them which are the decoy photons and their states. Bob and Charlie check the security of the transmission of the two photon sequences by measuring the decoy photons with correlated bases. If they confirm that the transmission is secure, the three conferees can obtain a private quantum key with some other techniques such as entanglement concentration and entanglement purification[47] which can act as the role of quantum privacy amplification. If they cannot confirm whether the transmission is secure or not, they should begin their quantum communication from the beginning.

(ii) The conferees encode and decode their secret messages with their private quantum key, similar to the second step in Ref.[45]. We can also use the same figure as in Ref.[45] to demonstrate the main principle of this step, as shown in Fig.1. The difference is that we exploit some decoy photons to analyse the error rate of the secret messages transmitted, not some quantum systems in the private key.

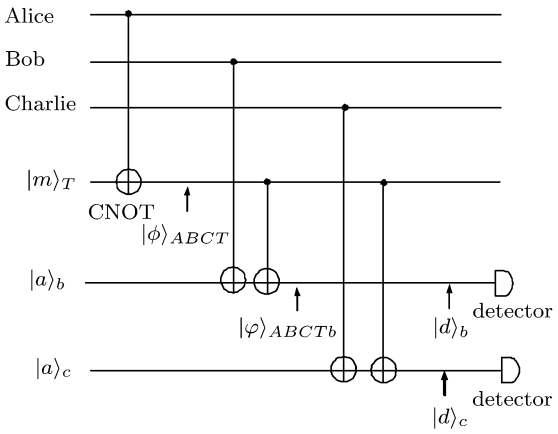


Fig.1. The principle of encoding and decoding the secret messages in our multiparty quantum remote secret conference scheme based on quantum encryption with GHZ-like states, is similar to that in Ref.[45]. CNOT presents a controlled-not gate. $|m\rangle_T$ is the message qubit transmitted. $|a\rangle_b$ and $|a\rangle_c$ are the auxiliary qubits prepared by Bob and Charlie, respectively.

Suppose that Alice wants to send her secret message to the other two conferees, Bob and Charlie. She prepares a sequence of message qubits $|m\rangle_T \in \{|0\rangle, |1\rangle\}$. Here $T = [T_1, T_2, \ldots, T_{k'}]$ and k' is the number of the bits of the secret message. Alice prepares k_d decoy photons and inserts them randomly into the message qubits. For the message qubits, Alice encrypts them with the photons in her quantum key. The same as in Ref.[45], Alice encrypts the j-th message qubit by using a controlled-not (CNOT) gate with the photon A_j in her quantum key, as shown in Fig.1. Also, the state of the message qubit $|m\rangle_T$ can be written as $|m\rangle_T = \gamma|0\rangle + \delta|1\rangle$ $(|\gamma|^2 + |\delta|^2 = 1)$ which represents the bit 0 when $\delta = 0$ or the bit 1 when $\gamma = 0$. If A_j is one of the three photons in the GHZ-like state $|\psi\rangle_{ABC}$, after the CNOT gate, the state of the four photons A_j, B_j, C_j and T_j becomes

$$\begin{aligned}|\phi\rangle_{ABCT} = {} & \alpha\gamma|0\rangle_A|0\rangle_B|0\rangle_C|0\rangle_T \\ & + \alpha\delta|0\rangle_A|0\rangle_B|0\rangle_C|1\rangle_T \\ & + \beta\gamma|1\rangle_A|1\rangle_B|1\rangle_C|1\rangle_T \\ & + \beta\delta|1\rangle_A|1\rangle_B|1\rangle_C|0\rangle_T). \end{aligned} \quad (3)$$

If A_j is one of the three photons in the GHZ-like state $|\psi'\rangle_{ABC}$, after the CNOT gate, the state of the four photons A_j, B_j, C_j and T_j becomes

$$\begin{aligned}|\phi'\rangle_{ABCT} = &\beta\gamma|0\rangle_A|0\rangle_B|0\rangle_C|0\rangle_T \\ &+ \beta\delta|0\rangle_A|0\rangle_B|0\rangle_C|1\rangle_T \\ &+ \alpha\gamma|1\rangle_A|1\rangle_B|1\rangle_C|1\rangle_T \\ &+ \alpha\delta|1\rangle_A|1\rangle_B|1\rangle_C|0\rangle_T). \end{aligned} \quad (4)$$

Alice sends the message photons T and the decoy photons to another conferee, say Bob. After Bob receives all these photons, Alice tells him which are the decoy photons and their states. Bob measures each decoy photon with the same basis as that used by Alice (Z or X). He analyses the security of the transmission between him and Alice with the outcomes of the decoy photons. After confirming that the transmission is secure, Bob decodes the secret message with his quantum key. In this time, he first prepares an auxiliary photon b_j in the state $|a\rangle_{b_j} = |0\rangle$ and then takes a CNOT gate on the photon B_j and b_j by using the photon B_j as the control qubit. Also, Bob should take another CNOT gate on the photon T_j and b_j by using the photon T_j as the control qubit. After these two CNOT gates, the state of the quantum system composed of the five photons A_j, B_j, C_j, T_j and b_j becomes

$$\begin{aligned}|\varphi\rangle_{ABCTb} = &\gamma(\alpha|0\rangle_A|0\rangle_B|0\rangle_C|0\rangle_T \\ &+ \beta|1\rangle_A|1\rangle_B|1\rangle_C|1\rangle_T)|0\rangle_b \\ &+ \delta(\alpha|0\rangle_A|0\rangle_B|0\rangle_C|1\rangle_T \\ &+ \beta|1\rangle_A|1\rangle_B|1\rangle_C|0\rangle_T)|1\rangle_b, \end{aligned} \quad (5)$$

or

$$\begin{aligned}|\varphi'\rangle_{ABCTb} = &\gamma(\beta|0\rangle_A|0\rangle_B|0\rangle_C|0\rangle_T \\ &+ \alpha|1\rangle_A|1\rangle_B|1\rangle_C|1\rangle_T)|0\rangle_b \\ &+ \delta(\beta|0\rangle_A|0\rangle_B|0\rangle_C|1\rangle_T \\ &+ \alpha|1\rangle_A|1\rangle_B|1\rangle_C|0\rangle_T)|1\rangle_b. \end{aligned} \quad (6)$$

That is, Bob can read out the secret message sent by Alice with measurements on his auxiliary qubits in the basis Z. Moreover, his measurement will not destroy the encryption done by Alice on the qubit T_j with the qubit A_j. Bob needs only to send all the message qubits to Charlie for the remote conference after he inserts some decoy photons into the message sequence randomly for the next eavesdropping check. Charlie can read out the secret message in the same way as that used by Bob.

(iii) If the transmission between Alice and Bob and that between Bob and Charlie are secure, the three conferees use their quantum key repeatedly to encode and decode their secret message in the next round. Different from Ref.[45], the three conferees need not check the security of their quantum communication by exploiting the correlation of the photons in their quantum key as the security analysis has been accomplished by choosing the decoy photons as the samples to calculate the error rate of the transmission. This modification makes using the quantum key very efficient.

In an ideal channel, this MQRSC scheme is secure as its security is ensured with the same principle as that in the famous BB84 QKD protocol. Also, an eavesdropper cannot read out the secret message carried on the message sequence as the state of each quantum system in the quantum key is randomly $|\psi\rangle_{ABC}$ or $|\psi'\rangle_{ABC}$. That is, after the encryption by a legitimate conferee, each message qubit is in the state $|0\rangle$ or $|1\rangle$ randomly. Eve's eavesdropping will give her no useful information about the secret message. Moreover, her action will be detected by the three legitimate conferees before their quantum key is used repeatedly.

The same as Ref.[45], this MQRSC scheme can also be generalized to the case with M legitimate conferees. In essence, we can complete this task with only two modifications. First, we replace the maximally entangled source in Ref.[45] with a pure entangled quantum source, a more feasible one. Second, we use some decoy photons to prevent a vicious eavesdropper from eavesdropping,[36] instead of the correlation of maximally multipartite entangled systems. With these two modifications, this MQRSC scheme is more feasible and efficient than the first MQRSC scheme proposed by Li *et al.*

Certainly, the implement of this MQRSC scheme should resort to quantum memory. Without quantum memory, the conferees can first create a common key and then use it to encrypt and decrypt the secret message, the same as the first MQRSC scheme based on a private key in Ref.[45]. Also, Alice can use decoy photons to prevent an eavesdropper from eavesdropping on the quantum communication, similar to Ref.[36].

In summary, we have presented a multiparty quantum remote secret conference scheme based on quantum encryption with a sequence of GHZ-like states. The conferees exploit the decoy-photon technique[46] to ensure the security of this scheme. As the quantum key can be used repeatedly if the quantum communication is secure, this scheme is more efficient than the original one proposed by Li *et al.*[45] Moreover, this scheme is more feasible than the latter as a real quantum source usually produces a GHZ-like state, not a GHZ state.

Acknowledgement

We would like to thank Dr. Fu-Guo Deng for his encouragement in our study of quantum information and for many helpful discussions about this work.

References

[1] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145

[2] Bennett C H and Brassad G 1984 *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing*, Bangalore, India (New York: IEEE) p175

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

[4] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901

[5] Deng F G and Long G L 2003 *Phys. Rev.* A **68** 042315

[6] Deng F G and Long G L 2004 *Phys. Rev.* A **70** 012311

[7] Lo H K, Chau H F and Ardehali M 2005 *J. Cryptology* **18** 133

[8] Li X H, Deng F G and Zhou H Y 2008 *Phys. Rev.* A **78** 022321

[9] Li X H, Deng F G and Zhou H Y 2007 *Appl. Phys. Lett.* **91** 144101

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

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

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

[13] Deng F G, Zhou H Y and Long G L 2005 *Phys. Lett.* A **337** 329
Deng F G, Long G L and Zhou H Y 2005 *Phys. Lett.* A **340** 43

[14] Zhang Z J, Li Y and Man Z X 2005 *Phys. Rev.* A **71** 044301
Deng F G, Li X H, Zhou H Y and Zhang Z J 2005 *Phys. Rev.* A **72** 044302

[15] Zhang Z J, Gao G, Wang X, Han L F and Shi S H 2007 *Opt. Commun.* **269** 418
Han L F, Liu Y M, Liu J and Zhang Z J 2008 *Opt. Commun.* **281** 2690
Zhang Z J and Man Z X 2005 *Phys. Rev.* A **72** 022303
Zhang Z J 2005 *Phys. Lett.* A **342** 60
Han L F, Liu Y M and Zhang Z J 2006 *Chin. Phys. Lett.* **23** 1988
Han L F, Liu Y M, Yuan H and Zhang Z J 2007 *Chin. Phys. Lett.* **24** 3312

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

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

[18] Deng F G, Li X H, Li C Y, Zhou P and Zhou H Y 2006 *Eur. Phys. J.* D **39** 459
Sheng Y B, Deng F G and Zhou H Y 2008 *Europ. Phys. J.* D **48** 279

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

[20] Li X H, Zhou P, Li C Y, Zhou H Y and Deng F G 2006 *J. Phys.* B **39** 1975
Li X H, Deng F G and Zhou H Y 2007 *Chin. Phys. Lett.* **24** 1151

[21] Man Z X, Xia Y J and An N B 2007 *Euro. Phys. J.* D **42** 333
Man Z X, Xia Y J and Zhang Z J 2007 *Int. J. Mod. Phys.* C **18** 1885

[22] Wang Z Y, Yuan H, Shi S H and Zhang Z J 2007 *Eur. Phys. J.* D **41** 371

[23] Zhou P 2007 *J. Phys.* A **40** 13121

[24] Zhang Y Q, Jin X R and Zhang S 2006 *Chin. Phys.* **15** 2252

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

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

[27] Deng F G, Li X H, Li C Y, Zhou P and Zhou H Y 2006 *Phys. Lett.* A **359** 359

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

[29] Wang C, Deng F G and Long G L 2005 *Opt. Commun.* **253** 15
Wang C, Li Y S and Long G L 2006 *Commun. Theor. Phys.* **46** 440

[30] Li X H, Li C Y, Deng F G, Zhou P, Liang Y J and Zhou H Y 2007 *Chin. Phys.* **16** 2149

[31] Li X H, Zhou P, Liang Y J, Li C Y, Zhou H Y and Deng F G 2006 *Chin. Phys. Lett.* **23** 1080

[32] Man Z X, Zhang Z J and Li Y 2005 *Chin. Phys. Lett.* **22** 18

[33] Zhang Z J, Liu J, Wang D and Shi S H 2007 *Phys. Rev.* A **75** 026301
Zhang Z J, Man Z X and Li Y 2004 *Phys. Lett.* A **333** 46

[34] Deng F G, Li X H, Li C Y, Zhou P, Liang Y J and Zhou H Y 2006 *Chin. Phys. Lett.* **23** 1676

[35] Wang J, Zhang Q and Tang C J 2007 *Chin. Phys.* **16** 1868

[36] Li X H, Deng F G, Li C Y, Liang Y J, Zhou P and Zhou H Y 2006 *J. Korean Phys. Soc.* **49** 1354

[37] Yan F L and Zhang X 2004 *Euro. Phys. J.* B **41** 75

[38] Gao T, Yan F L and Wang Z X 2004 *Nuovo Cimento* B **119** 313
[39] Gao T, Yan F L and Wang Z X 2005 *J. Phys.* A **38** 5761
Gao T, Yan F L and Wang Z X 2005 *Chin. Phys.* **14** 893
[40] Li X H, Deng F G and Zhou H Y 2006 *Phys. Rev.* A **74** 054302
[41] Xia Y, Fu C B, Zhang S, Hong S K, Yeon K H and Um C I 2006 *J. Korean Phys. Soc.* **48** 24
[42] Zhu A D, Xia Y, Fan Q B and Zhang S 2006 *Phys. Rev.* A **73** 022338
[43] Wang J, Zhang Q and Tang C J 2006 *Phys. Lett.* A **358** 256
[44] Cao H J and Song H S 2006 *Chin. Phys. Lett.* **23** 290
[45] Li X H, Li C Y, Deng F G, Zhou P, Liang Y J and Zhou H Y 2007 *Chin. Phys. Lett.* **24** 23
[46] Li C Y, Zhou H Y, Wang Y and Deng F G 2005 *Chin. Phys. Lett.* **22** 1049
Li C Y, Li X H, Deng F G, Zhou P, Liang Y J and Zhou H Y 2006 *Chin. Phys. Lett.* **23** 2896
[47] Bennett C H, Brassard G, Popescu S, Schumacher B, Smolin J A and Wootters W K 1996 *Phys. Rev. Lett.* **76** 722
Deutsch D, Ekert A, Jozsa R, Macchiavello C, Popescu S and Sanpera A 1996 *Phys. Rev. Lett.* **77** 2828
Sheng Y B, Deng F G and Zhou H Y 2008 *Phys. Rev.* A **77** 062325
Sheng Y B, Deng F G and Zhou H Y 2008 *Phys. Rev.* A **77** 042308