Controlled quantum teleportation with Bell states*

Wang Tian-Yin(王天银)[a)b)†] and Wen Qiao-Yan(温巧燕)[a)]

[a)] *State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*

[b)] *School of Mathematical Science, Luoyang Normal University, Luoyang* 471022, *China*

(Received 9 May 2010; revised manuscript received 17 November 2010)

We propose a new scheme for controlled quantum teleportation with Bell states in which classical keys for controllers' portion are used. We also discuss the security of the proposed scheme and show that it can satisfy the requirements for controlled quantum teleportation. The comparison between this scheme and the previous ones shows that it is more economical and efficient.

Keywords: controlled, teleportation, Bell state

PACS: 03.67.Hk, 03.67.Dd, 03.65.Ud **DOI:** 10.1088/1674-1056/20/4/040307

1. Introduction

The principles of quantum mechanics have supplied many interesting applications in the field of quantum information in the past years, such as quantum computation, quantum key distribution, quantum secret sharing, quantum teleportation (QT), etc.[1,2] Especially, QT is an important branch of quantum information which allows the two remote parties, the sender Alice and the receiver Bob, to teleport an unknown quantum state $\alpha|0\rangle+\beta|1\rangle$, utilizing the nonlocal correlation of quantum channels.[3] QT has attracted much attention in both theoretical and the experimental aspects[4−17] since Bennett *et al.*[3] first introduced the concept of QT in 1993.

Controlled quantum teleportation (CQT), first introduced by Karlsson and Bourennane[18] in 1999, is a variant of QT in which a teleportation of a quantum state is performed under the supervision of all controllers. The property of CQT can be used in some special occasions, such as networked quantum information processing, cryptographic conferencing,[19−21] opening a credit account on the agreement of all the managers in a network,[22] etc. Accordingly, lots of schemes for CQT have been presented,[22−39] which can be classified into two kinds: one uses qubits as keys distributed among controllers[22−36] and the other uses classical bits as keys distributed among controllers.[37−39] As mentioned in Refs. [37]–[40], the schemes using qubits as keys distributed among controllers are, however, not as economical as those using classical keys. In the present paper, using classical bits as keys distributed among controllers, we propose a new CQT scheme with Bell states, which can guarantee the security through using the method of decoy states.[41−44] This scheme is more efficient than other similar ones.[37−39]

2. Proposed scheme

Suppose that the sender Alice wants to teleport a string of message qubits labeled by $1,2,\ldots,l$, which is initially in the state $\otimes_{i=1}^{l}(\alpha_i|0\rangle+\beta_i|1\rangle)$, to a remote receiver Bob, but she requires that Bob can recover the qubits $\otimes_{i=1}^{l}(\alpha_i|0\rangle+\beta_i|1\rangle)$ if and only if all the controllers (Charlie_1, Charlie_2, …, Charlie_{n-1} and Charlie_n) approve.

Let s be the security parameter, this scheme can be detailed as follows.

(i) Alice prepares l Bell states $\otimes_{i=1}^{l}|\phi_i^+\rangle_{12}$, where $|\phi_i^+\rangle_{12}=\frac{\sqrt{2}}{2}(|00\rangle+|11\rangle)_{12}$ ($i\in\{1,2,\ldots,l\}$) and the subscripts 1 and 2 denote the two correlated qubits of the state $|\phi_i^+\rangle_{12}$, respectively. Then she takes the

*Project supported by the National Natural Science Foundation of China (Grant Nos. 60873191, 60903152, 61003286 and 60821001), the Specialized Research Fund for the Doctoral Program of Higher Education, China (Grant Nos. 200800131016 and 20090005110010), the Beijing Nova Program, China (Grant No. 2008B51), the Key Project of the Chinese Ministry of Education (Grant No. 109014) and the Natural Science Foundation of Educational Bureau of Henan Province, China (Grant No. 2010B120008).

†Corresponding author. E-mail: wangtianyin@yahoo.cn

© 2011 Chinese Physical Society and IOP Publishing Ltd

qubit 2 from each Bell state $|\phi_i^+\rangle_{12}$ to form an ordered qubit sequence P_2 and all the remaining qubits 1 form another qubit sequence P_1. At the same time, she prepares s single-qubit states and each of them is randomly in one of the four quantum states: $|0\rangle, |1\rangle, |+\rangle = \frac{\sqrt{2}}{2}(|0\rangle + |1\rangle)$, and $|-\rangle = \frac{\sqrt{2}}{2}(|0\rangle - |1\rangle)$. Finally, she randomly inserts the s decoy states into the sequence P_2 to generate a new photon sequence P_2' and sends it to Bob. Note that nobody knows the initial states and positions of these s decoy states in the P_2' sequence except Alice.

(ii) When confirming that Bob has received the P_2' sequence, Alice informs him of the positions and initial states of the s decoy states. According to Alice's notification, Bob chooses the proper basis to measure every decoy state, i.e., if the initial state of the decoy state is either $|0\rangle$ or $|1\rangle$, he performs a Z-basis measurement; otherwise, he conducts an x-basis measurement. By combining the initial states and the measurement results of the s decoy states, Bob can evaluate the error rate of the transmission. If the error rate exceeds the threshold they preset, they abort the protocol; otherwise, the protocol continues.

(iii) Similarly, as in step (i), Alice prepares another s decoy states and randomly inserts them into the sequence P_1 to generate a new qubit sequence P_1'. Then she sends it to the first controller Charlie_1.

(iv) When receiving the P_1' sequence, for each qubit: Charlie_1 first ascertains whether each quantum signal only contains a single photon using a similar method to that in Refs. [45]–[48]. If it is not, he aborts the protocol; otherwise, he randomly chooses a phase θ ($\theta \in \{0, \frac{2}{3}\pi, \frac{4}{3}\pi\}$) and performs the phase operation $U(\theta)$ on it, where

$$U(\theta) = \{|0\rangle \to |0\rangle; |1\rangle \to \mathrm{e}^{\mathrm{i}\,\theta}|1\rangle\}. \tag{1}$$

Then he sends the P_1' sequence to the next controller Charlie_2.

(v) After receiving the P_1' sequence, Charlie_2 does the same action as Charlie_1 in step (iv), then he sends it to the next controller Charlie_3. Similar procedures are repeated until the last controller Charlie_n sends the P_1' sequence back to Alice after his encryption.

(vi) When receiving the P_1' sequence encrypted by all controllers, Alice also first ascertains whether each quantum signal contains only a single photon. If it does not, she aborts the protocol; otherwise, she performs an eavesdropping check by measuring the s decoy states prepared by herself in step (iii). Specifically, if the initial state of the decoy state is either $|0\rangle$ or $|1\rangle$, she performs a Z-basis measurement on it directly; otherwise, she randomly selects a controller Charlie_i one by one and lets him inform her of his phase θ_i until she obtains all the phases $\theta_1, \theta_2, \ldots, \theta_n$, then she performs the phase operation $U(-\sum_{i=1}^{n}\theta_i)$ on it. After that, the decoy state should be recovered into its original state if it is not disturbed during the transmission and Alice measures it with x-basis. Accordingly, Alice can determine the error rate and judge whether the P_1 sequence is disturbed by comparing the initial states and the measurement outcomes of the s decoy states. If the error rate exceeds an acceptable threshold, the process is aborted. Otherwise, Alice performs a Bell measurement on the message qubit $\alpha_i|0\rangle + \beta_i|1\rangle$ and the qubit 1 of the Bell state $|\phi_i^+\rangle_{12}$, $i = 1, 2, \ldots, l$, then she informs Bob of her measurement outcome.

(vii) When all the controllers approve that Bob recovers the message qubits $\otimes_{i=1}^{l}(\alpha_i|0\rangle + \beta_i|1\rangle)$ teleported by Alice, they inform him of their phase operations on each qubit 2 of the l Bell state $\otimes_{i=1}^{l}|\phi_i^+\rangle_{12}$.

(viii) According to Alice's measurement outcomes and the controllers' phase operations, Bob can successfully recover the message qubits $\otimes_{i=1}^{l}(\alpha_i|0\rangle+\beta_i|1\rangle)$ by performing a corresponding unitary operation on each qubit 2 of the l Bell states $\otimes_{i=1}^{l}|\phi_i^+\rangle_{12}$.

So far, using Bell states and phase encryption, we have completed the scheme for CQT. Now we show that Bob can recover the message qubits $\otimes_{i=1}^{l}(\alpha_i|0\rangle + \beta_i|1\rangle)$ when the controllers Charlie_1, Charlie_2, …, Charlie_{n-1} and Charlie_n approve. It can be seen that the Bell state $|\phi_i^+\rangle_{12}$ will evolve into the state $I\otimes U(\theta^i)|\phi_i^+\rangle_{12} = \frac{\sqrt{2}}{2}(|00\rangle+\mathrm{e}^{\mathrm{i}\,\theta^i}|11\rangle)_{12}$ after the n controllers' phase operations: $U(\theta_1^i), U(\theta_2^i), \ldots, U(\theta_n^i)$, where $U(\theta^i) = U(\theta_1^i)U(\theta_2^i)\cdots U(\theta_n^i)$. Combining the states $\alpha_i|0\rangle + \beta_i|1\rangle$ and $\frac{\sqrt{2}}{2}(|00\rangle + \mathrm{e}^{\mathrm{i}\,\theta^i}|11\rangle)_{12}$, we can have

$$\begin{aligned}
&(\alpha_i|0\rangle + \beta_i|1\rangle)_0 \otimes \frac{\sqrt{2}}{2}(|00\rangle + \mathrm{e}^{\mathrm{i}\,\theta^i}|11\rangle)_{12} \\
&= |\phi^+\rangle_{01} \otimes IU(\theta^i)(\alpha_i|0\rangle + \beta_i|1\rangle)_2 \\
&\quad +|\phi^-\rangle_{01} \otimes \sigma_z U(\theta^i)(\alpha_i|0\rangle + \beta_i|1\rangle)_2 \\
&\quad +|\psi^+\rangle_{01} \otimes \sigma_x U(\theta^i)(\alpha_i|0\rangle + \beta_i|1\rangle)_2 \\
&\quad +|\psi^-\rangle_{01} \otimes \mathrm{i}\,\sigma_y U(\theta^i)(\alpha_i|0\rangle + \beta_i|1\rangle)_2,
\end{aligned} \tag{2}$$

where $|\phi^\pm\rangle_{01} = \frac{\sqrt{2}}{2}(|00\rangle \pm |11\rangle)_{01}$, $|\psi^\pm\rangle_{01} = \frac{\sqrt{2}}{2}(|01\rangle \pm |10\rangle)_{01}$, $I = |0\rangle\langle 0| + |1\rangle\langle 1|$, $\sigma_x = |1\rangle\langle 0| + |0\rangle\langle 1|$, $\mathrm{i}\,\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|$, $\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$ and the subscript 0 denotes the message qubit $\alpha_i|0\rangle + \beta_i|1\rangle$. From Eq. (2), we can see that when Alice performs a Bell measurement on qubits 0 and

1, the state of qubit 2 will collapse into one of the four states: $IU(\theta^i)(\alpha_i|0\rangle + \beta_i|1\rangle), \sigma_z U(\theta^i)(\alpha_i|0\rangle + \beta_i|1\rangle), \sigma_x U(\theta^i)(\alpha_i|0\rangle + \beta_i|1\rangle)$, and $\mathrm{i}\sigma_y U(\theta^i)(\alpha_i|0\rangle + \beta_i|1\rangle)$. Accordingly, Bob can recover the message qubits $\otimes_{i=1}^{l}(\alpha_i|0\rangle + \beta_i|1\rangle)$ by performing one of the four operations $U(-\theta^i)I, U(-\theta^i)\sigma_z, U(-\theta^i)\sigma_x$, or $U(-\theta^i)\,\mathrm{i}\sigma_y$ on qubit 2 according to Alice's measurement outcome and the phase θ^i.

3. Security analysis

Now we analyse the security of the proposed scheme for CQT. For CQT, the security requires that nobody can recover the message qubits $\otimes_{i=1}^{l}(\alpha_i|0\rangle + \beta_i|1\rangle)$ except the receiver and the receiver can recover them if and only if all the controllers approve. In the following, we show that the proposed scheme can satisfy the requirement.

First, we show that nobody can learn any controller Charlie$_i$'s ($i \in \{1, 2, \ldots, n\}$) encryption operation $U(\theta_i)$ before he publishes it. The controller Charlie$_i$'s encryption operation $U(\theta_i)$ is randomly chosen from $U(0), U(\frac{2}{3}\pi)$ and $U(\frac{4}{3}\pi)$. If we perform the three operations on a single-qubit state $\alpha|0\rangle+\beta|1\rangle$, separately, where $|\alpha|^2+|\beta|^2=1$, we will have the following three quantum states:

$$\alpha|0\rangle + \beta|1\rangle, \alpha|0\rangle + \mathrm{e}^{\mathrm{i}\frac{2}{3}\pi}\beta|1\rangle, \alpha|0\rangle + \mathrm{e}^{\mathrm{i}\frac{4}{3}\pi}\beta|1\rangle. \quad (3)$$

Obviously, the three states cannot be completely orthogonal. If we perform the three operations on one qubit of any entangled state $|\phi\rangle$, separately, we will have three nonorthogonal entangled states. Without loss of generality, suppose that we perform the three operations on the first qubit of the entangled state $|\phi\rangle=|0\rangle|\phi_1\rangle+|1\rangle|\phi_2\rangle$, separately, we will obtain the three entangled states:

$$\begin{aligned}&|0\rangle|\phi_1\rangle + |1\rangle|\phi_2\rangle, |0\rangle|\phi_1\rangle \\ &\quad + \mathrm{e}^{\mathrm{i}\frac{2}{3}\pi}|1\rangle|\phi_2\rangle, |0\rangle|\phi_1\rangle + \mathrm{e}^{\mathrm{i}\frac{4}{3}\pi}|1\rangle|\phi_2\rangle. \quad (4)\end{aligned}$$

We can prove that these entangled states cannot be completely orthogonal by simple computation either. By the quantum no-distinguishing theorem, nonorthogonal states cannot be perfectly distinguished. Therefore, nobody can learn the controller Charlie$_i$'s encryption operation $U(\theta_i)$ before he publishes it.

Secondly, we show that nobody can recover the message qubits $\otimes_{i=1}^{l}(\alpha_i|0\rangle + \beta_i|1\rangle)$ transmitted by Alice except Bob. It is evident that if the CQT scheme is secure to the dishonest controllers, then it is secure to any adversary. In the following, we show that they cannot recover the message qubits $\otimes_{i=1}^{l}(\alpha_i|0\rangle + \beta_i|1\rangle)$ even if all the controllers Charlie$_1$, Charlie$_2$, ..., Charlie$_{n-1}$ and Charlie$_n$ are in collaboration. In step (i), Alice sends the P_2 sequence to Bob by using the method of inserting decoy states, which is similar to the quantum key distribution[49] whose security has been proven in Refs. [50] and [51]. Accordingly, the n controllers cannot recover the message qubits $\otimes_{i=1}^{l}(\alpha_i|0\rangle + \beta_i|1\rangle)$ by stealing the P_2 sequence. Another possible strategy to recover the message qubits $\otimes_{i=1}^{l}(\alpha_i|0\rangle + \beta_i|1\rangle)$ for the n controllers is that they send false qubits to Alice in step (v), i.e., for each qubit in the P_1' sequence, they send a false qubit (one qubit of a maximal entangled state) to Alice instead of the true one. In step (vi), Alice performs the teleportation measurement and informs Bob of the measurement outcome if and only if she confirms that the P_1 sequence is not disturbed, so this attack must evade Alice's detection in step (vi). Nevertheless, it is impossible for the n controllers. There are two reasons: one is that they do not know the positions and initial states of the s decoy qubits in the P_1' sequence and the other is that this scheme involves only three phase operations to encrypt the qubit in the P_1' sequence. Accordingly, the n controllers cannot evade Alice's detection in step (vi) by taking a teleportation attack in Refs. [52]–[55] since the number of the corresponding unitary operations on the teleportation measurement is at least four.

Finally, we show that Bob cannot recover the message qubits $\otimes_{i=1}^{l}(\alpha_i|0\rangle + \beta_i|1\rangle)$ even if arbitrary $n-1$ controllers approve. As shown above, after Alice's Bell measurement in step (vi), the qubit 2 in the P_2 sequence collapses into the following four states: $IU(\theta^i)(\alpha_i|0\rangle + \beta_i|1\rangle), \sigma_z U(\theta^i)(\alpha_i|0\rangle + \beta_i|1\rangle), \sigma_x U(\theta^i)(\alpha_i|0\rangle + \beta_i|1\rangle)$, and $\mathrm{i}\sigma_y U(\theta^i)(\alpha_i|0\rangle + \beta_i|1\rangle)$. Therefore, if Bob does not know the remaining controller Charlie$_i$'s encryption operation $U(\theta_i^i)$ on the qubit 2 of the Bell state $|\phi_i^+\rangle_{12}$, he cannot choose the right unitary operation $U(-\theta^i)I$, $U(-\theta^i)\sigma_z$, $U(-\theta^i)\sigma_x$, or $U(-\theta^i)\,\mathrm{i}\sigma_y$ to recover the message qubit $\alpha_i|0\rangle + \beta_i|1\rangle$, but he can obtain the state $\alpha|0\rangle + \mathrm{e}^{\mathrm{i}\,\theta_i^i}\beta|1\rangle$.

It is noted that we do not consider the invisible photon attack and Trojan horse attack strategy in the above analyses. It is evident that these attack strategies are also invalid to this scheme since the similar ways proposed in Refs. [45]–[48] to resist them are

employed in this scheme.

From the above analyses, we can say that nobody can recover the message qubits $\otimes_{i=1}^{l}(\alpha_i|0\rangle+\beta_i|1\rangle)$ except the receiver Bob and Bob can recover them if and only if all the controllers approve.

4. Discussion and conclusion

With present technology, the transmission distance of qubits is very limited and the channel loss and error in transmission are inevitable. In the proposed scheme, qubits 2 must be transmitted sequently among the n controllers: Charlie_1, Charlie_2, ..., Charlie_{n-1} and Charlie_n, which makes the channel loss and the error rate in transmission become large. These restrict the application of the scheme. Nevertheless, with the progress of experimental technology, these will not be problems before long.

The main contribution of this article is to give a new way for CQT in theory, without considering the experiment realization with the present technology.

In the proposed scheme we use classical bits as keys distributed among the n controllers and require only two-qubit entangled states, which makes it the economically as other similar schemes.[37−39] As mentioned in Refs. [37]–[39], the controlled parameters of controllers can be achieved by using quantum key distribution, quantum secure direct communication, quantum secret sharing or the combinations. Nevertheless, for any method of them up to no less than $O(2l)$ quantum qubits will be used additionally. In the proposed scheme, the controlled parameters of the n controllers are encrypted on the qubit 2 of the Bell states $\otimes_{i=1}^{l}|\phi_i^+\rangle_{12}$ and additional quantum resources are not necessary except the s decoy states used for eavesdropping check. Therefore, the proposed scheme is more efficient than previous ones.[37−39]

In conclusion, we presented a new CQT scheme with Bell states. We also analysed the security of the proposed scheme and showed that it can resist all the possible attack strategies in theory. This scheme can be used in some special scenarios.

References

[1] Wang T Y, Wen Q Y and Zhu F C 2009 *Chin. Phys.* B **18** 3189

[2] Wang T Y and Wen Q Y 2010 *Chin. Phys.* B **19** 060307

[3] Bennett C H, Brassard G, Crepeau C, Jozsa R, Peres A and Wootters W K *Phys. Rev. Lett.* **70** 1895

[4] Bouwmeester D, Pan J W, Mattle K, Eibl M, Weinfurter H and Zeilinger A 1997 *Nature* **390** 575

[5] Nielsen M A, Knill E and Laflamme R 1998 *Nature* **396** 52

[6] Furusawa A, Sorensen J L, Braunstein S L, Fuchs C A, Kimble H J and Polzik E S 1998 *Science* **282** 706

[7] Li W L, Li C F and Guo G C 2000 *Phys. Rev.* A **61** 034301

[8] Pan J W, Gasparoni S, Aspelmeyer M, Jennewein T and Zeilinger A 2003 *Nature* **421** 721

[9] Riebe M, Haffner H, Roos C F, Hansel W, Benhelm J, Lancaster G P T, Korber T W, Becher C, Schmidt-Kaler F, James D F V and Blatt R 2004 *Nature* **429** 734

[10] Barret M D, Chiaverini J, Schaetz T, Britton J, Itano W M, Jost J D, Knill E, Langer C, Leibfried D, Ozeri R and Wineland D J 2004 *Nature* **429** 737

[11] Zhao Z, Chen Y A, Zhang A N, Yang T, Briegel H J and Pan J W 2004 *Nature* **430** 54

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

[13] Modlawska J and Grudka A *Phys. Rev.* A **79** 064302

[14] Ren J G, Yang B, Yi Z H, Zhou F, Chen K, Peng C Z and Pan J W 2009 *Chin. Phys.* B **18** 3605

[15] Giampaolo S M and Illuminati F 2009 *Phys. Rev.* A **80** 050301

[16] Noh C, Chia A, Nha H, Collett M J and Carmichael H J 2009 *Phys. Rev. Lett.* **102** 230501

[17] Chen X B, Wen Q Y, Sun Z X, Shangguan L Y and Yang Y X 2010 *Chin. Phys.* B **19** 010303

[18] Karlsson A and Bourennane M 1998 *Phys. Rev.* A **58** 4394

[19] Biham E, Huttner B and Mor T 1996 *Phys. Rev.* A **54** 2651

[20] Townsend P D 1997 *Nature* **385** 47

[21] Bose S, Vedral V and Knight P L 1998 *Phys. Rev.* A **57** 822

[22] Yang C P and Han S Y 2005 *Phys. Lett.* A **343** 267

[23] An N B 2003 *Phys. Rev.* A **68** 022321

[24] Yan F L and Wang D 2003 *Phys. Lett.* A **316** 297

[25] Yang C P, Chu S I and Han S Y 2004 *Phys. Rev.* A **70** 022329

[26] Gao T, Yan F L and Wang Z X 2005 *Chin. Phys.* **14** 893

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

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

[29] Zhou P, Li X H and Deng F G 2007 *J. Phys.* A **40** 13121

[30] Man Z X, Xia Y J and An N B 2007 *J. Phys.* B **40** 1767

[31] Dong J and Teng J F 2008 *Euro. Phys. J.* D **49** 129

[32] Wang Y H and Song H S 2008 *Opt. Commun.* **281** 489

[33] Chen X B, Zhang N, Lin S, Wen Q Y and Zhu F C 2008 *Opt. Commun.* **281** 2331

[34] Nie D, He G Q and Zeng G H 2008 *J. Phys.* B **41** 175504

[35] Wang J, Hou K, Yuan H and Shi S H 2009 *Phys. Scr.* **80** 015004

[36] Wang X W, Su Y H and Yang G J 2009 *Quantum Information Proce.* **8** 319

[37] Zhang Z J, Liu Y M and Man Z X 2005 *Commun. Theor. Phys.* **44** 847

[38] Zhang Z J and Man Z X 2005 *Phys. Lett.* A **341** 55

[39] Zhang Z J 2006 *Phys. Lett.* A **352** 55

[40] SaiToh A, Rahimi R and Nakahara M 2009 *Phys. Rev.* A **79** 062313

[41] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503

[42] Lo H K, Ma X F and Chen K 2005 *Phys. Rev. Lett.* **94** 230504

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

[44] Li C Y, Deng F G, Zhou P, Liang Y J and Zhou H Y 2006 *Chin. Phys. Lett.* **23** 2896

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

[46] Deng F G, Li X H, Zhou H Y and Zhang Z J 2006 *Phys. Rev.* A **73** 049901(E)

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

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

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

[50] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441

[51] Lo H K and Chau H F 1999 *Science* **283** 2050

[52] He G P 2007 *Phys. Rev. Lett.* **98** 028901

[53] Wang T Y, Qin S J, Wen Q Y and Zhu F C 2008 *Acta Phys. Sin.* **57** 7452 (in Chinese)

[54] Wang T Y, Wen Q Y, Gao F, Lin S and Zhu F C 2008 *Phys. Lett.* A **373** 65

[55] Gao F, Wen Q Y and Zhu F C 2008 *Chin. Phys.* B **17** 3189