Multiparty quantum secret sharing of classical messages based on entanglement swapping

Zhan-jun Zhang[1,2,*] and Zhong-xiao Man[2]
[1]*School of Physics and Material Science, Anhui University, Hefei 230039, China*
[2]*Wuhan Institute of Physics and Mathematics, Chinese Academy of Sciences, Wuhan 430071, China*

(Received 20 December 2004; published 4 August 2005)

A multiparty quantum secret sharing (QSS) protocol of classical messages (i.e., classical bits) is proposed by using swapping quantum entanglement of Bell states. The secret messages are imposed on Bell states by local unitary operations. The secret messages are split into several parts, and each part is distributed to a separate party so that no action of a subset of all the parties without the cooperation of the entire group is able to read out the secret messages. In addition, dense coding is used in this protocol to achieve a high efficiency. The security of the present multiparty QSS against eavesdropping has been analyzed and confirmed even in a noisy quantum channel.

DOI: 10.1103/PhysRevA.72.022303 PACS number(s): 03.67.Dd, 03.65.Ta, 89.70.+c

Suppose that Alice wants to send a secret message to two distant parties, Bob and Charlie. One of them, Bob or Charlie, is not entirely trusted by Alice, but she knows that if the two of them coexist, the honest one will keep the dishonest one from doing any damage. Instead of giving entire secret messages to either of them, it may be desirable for Alice to split the secret messages into two encrypted parts and send each one a part so that neither individual is able to obtain all of the original information unless they collaborate. To achieve this end, classical cryptography can use a technique called secret sharing [1,2], where secret messages are distributed among N users in such a way that only by combining their pieces of information can the N users recover the secret messages. Recently this concept has been generalized to quantum scenario [3]. However, it should be remembered, as was stressed in Ref. [3], that for practical purposes it is possible to combine quantum cryptography with classical secret sharing to achieve secret sharing in an very simple manner. That is, as stated in Ref. [3], "the most obvious way of doing this is simply for Alice to use quantum cryptographic protocols to send each of the bit strings that result from the classical secret sharing procedure. This method will work; it is, however, awkward. One first must establish mutual keys among different pairs of parties, in this case, one for Alice and Bob and another for Alice and Charlie, and then implement the classical procedure. The classical procedure, it should be pointed out, becomes more and more complicated the larger the number of pieces into which one wants to split the message." Due to the obvious disadvantages, in Ref. [3] an alternative is employed. In fact, since quantum secret sharing (QSS) is likely to play a key role in protecting secret quantum information, e.g., in secure operations of distributed quantum computation, sharing difficult-to-construct ancilla states, joint sharing of quantum money [4], and so on, after the pioneering QSS work proposed by using three-particle and four-particle GHZ (Greenberger-Horne-Zeilinger) states [3], this kind of work on QSS attracted a great deal of attention in both the theoretical and experimental aspects [4–20], and various methods were proposed to realize QSS. Entanglement swapping [21–23] is a method that enables one to entangle two quantum systems that do not have direct interaction with one another. Based on entanglement swapping, a number of applications in quantum information [24] have been found, such as constructing a quantum telephone exchange, speeding up the distribution of entanglement, correcting errors in Bell states, preparing entangled states of a higher number of particles, and secret sharing of classical information. Entanglement swapping is also used in QSS protocols [7,12]; however, in those multiparty QSS protocols [3,5,11,12] the identification of multiqubit GHZ states are required and should be achieved. In fact, according to the present-day technologies, an identification of a Bell state is much easier than an identification of a GHZ state. In this paper, we propose a multiparty QSS protocol based completely on the entanglement swapping and identification of Bell states.

Before giving our protocol, let us briefly introduce the local unitary operations which can impose secret messages on Bell states and the entanglement swapping of Bell states. We define the four Bell states as

$$|\Psi^{+}\rangle=\frac{1}{\sqrt{2}}(|0\rangle|1\rangle+|1\rangle|0\rangle)=\frac{1}{\sqrt{2}}(|+\rangle|+\rangle-|-\rangle|-\rangle), \quad (1)$$

$$|\Psi^{-}\rangle=\frac{1}{\sqrt{2}}(|0\rangle|1\rangle-|1\rangle|0\rangle)=\frac{1}{\sqrt{2}}(|+\rangle|-\rangle-|-\rangle|+\rangle), \quad (2)$$

$$|\Phi^{+}\rangle=\frac{1}{\sqrt{2}}(|0\rangle|0\rangle+|1\rangle|1\rangle)=\frac{1}{\sqrt{2}}(|+\rangle|+\rangle+|-\rangle|-\rangle), \quad (3)$$

$$|\Phi^{-}\rangle=\frac{1}{\sqrt{2}}(|0\rangle|0\rangle-|1\rangle|1\rangle)=\frac{1}{\sqrt{2}}(|+\rangle|-\rangle+|-\rangle|+\rangle), \quad (4)$$

where $|+\rangle=(1/\sqrt{2})(|0\rangle+|1\rangle)$ and $|-\rangle=(1/\sqrt{2})(|0\rangle-|1\rangle)$. Let $u_1=|0\rangle\langle 0|+|1\rangle\langle 1|$, $u_2=|0\rangle\langle 0|-|1\rangle\langle 1|$, $u_3=|1\rangle\langle 0|+|0\rangle\langle 1|$, and $u_4=|0\rangle\langle 1|-|1\rangle\langle 0|$ be four local unitary operators acting on one qubit of the qubit pair in a Bell state. One can then see that $u_1|\Psi^{-}\rangle=|\Psi^{-}\rangle$, $u_2|\Psi^{-}\rangle=|\Psi^{+}\rangle$, $u_3|\Psi^{-}\rangle=|\Phi^{+}\rangle$, and $u_4|\Psi^{-}\rangle$

[*] Corresponding author. Email address: zjzhang@ahu.edu.cn

$=|\Phi^-\rangle$. Assume that each of the preceding four unitary operations corresponds to two classical bits, respectively, i.e., u_0 to "00," u_1 to "01," u_2 to "10," and u_3 to "11." The encodings of the secret messages can then be imposed on the Bell states by using the local unitary operations. Since the following equations hold:

$$(u_1|\Psi^-_{ab}\rangle)\otimes|\Psi^-_{cd}\rangle=|\Psi^-_{ab}\rangle\otimes|\Psi^-_{cd}\rangle=\frac{1}{2}(|\Psi^-_{ac}\rangle|\Psi^-_{bd}\rangle+|\Phi^+_{ac}\rangle\times|\Phi^+_{bd}\rangle-|\Psi^+_{ac}\rangle|\Psi^+_{bd}\rangle-|\Phi^-_{ac}\rangle|\Phi^-_{bd}\rangle),\quad(5)$$

$$(u_2|\Psi^-_{ab}\rangle)\otimes|\Psi^-_{cd}\rangle=|\Psi^+_{ab}\rangle\otimes|\Psi^-_{cd}\rangle=\frac{1}{2}(|\Psi^+_{ac}\rangle|\Psi^-_{bd}\rangle-|\Psi^-_{ac}\rangle\times|\Psi^+_{bd}\rangle-|\Phi^+_{ac}\rangle|\Phi^-_{bd}\rangle+|\Phi^-_{ac}\rangle|\Phi^+_{bd}\rangle),\quad(6)$$

$$(u_3|\Psi^-_{ab}\rangle)\otimes|\Psi^-_{cd}\rangle=|\Phi^+_{ab}\rangle\otimes|\Psi^-_{cd}\rangle=\frac{1}{2}(|\Phi^-_{ac}\rangle|\Psi^+_{bd}\rangle-|\Psi^+_{ac}\rangle\times|\Phi^-_{bd}\rangle-|\Psi^-_{ac}\rangle|\Phi^+_{bd}\rangle+|\Phi^+_{ac}\rangle|\Psi^-_{bd}\rangle),\quad(7)$$

$$(u_4|\Psi^-_{ab}\rangle)\otimes|\Psi^-_{cd}\rangle=|\Phi^-_{ab}\rangle\otimes|\Psi^-_{cd}\rangle=\frac{1}{2}(|\Phi^+_{ac}\rangle|\Psi^+_{bd}\rangle+|\Phi^-_{ac}\rangle\times|\Psi^-_{bd}\rangle-|\Psi^+_{ac}\rangle|\Phi^+_{bd}\rangle-|\Psi^-_{ac}\rangle|\Phi^-_{bd}\rangle),\quad(8)$$

obviously, one can see that there is an explicit correspondence between a known initial state of two qubit pairs (secret encoding has been imposed on one pair via a local unitary operation) and its Bell-state measurement outcomes after the quantum entanglement swapping.

For convenience, let us first describe a three-party QSS protocol. Suppose that there are three parties, Alice, Bob, and Charlie. The sender, Alice, wants to distribute secret messages between two parties, Bob and Charlie. To achieve this goal, the parties act as follows:

(i) Alice prepares three qubit pairs, all in the same Bell state, say, $|\Psi^-\rangle$'s; that is, Alice prepares $|\Psi^-_{12}\rangle\otimes|\Psi^-_{34}\rangle\otimes|\Psi^-_{56}\rangle$ [see Fig. 1(a)]. Then Alice stores qubits 1 and 6 in her own site, sends to Bob qubits 2 and 3 via the Alice-Bob quantum channel, and sends to Charlie qubits 4 and 5 via the Alice-Charlie quantum channel [see Figs. 1(a) and 1(b)]. They should publicly confirm whether the qubit distributions have been successful. If successful, Alice can select one of two possible options. With probability c, Alice selects the first option, called *detecting mode*. The goal of this option is to check the security of qubit-transmission quantum channels. If this mode is selected, the procedure continues at (ii). In contrast, Alice can select the second option with probability $r=1-c$. The goal of the second option is to impose the secret message and implement QSS. We call this option *message mode*. If this mode is selected, the procedure continues at (iii).

(ii) Alice chooses randomly one of the two sets of measurement basis (MB), say, $\chi_z=\{|1\rangle,|0\rangle\}$ and $\chi_x=\{|+\rangle,|-\rangle\}$, to measure qubit 1. Then Alice tells Bob which MB she has chosen. Bob uses the same MB as Alice to measure qubit 2 and tells Alice his measurement outcome on qubit 2. Alice compares her measurement outcome on qubit 1 with Bob's measurement outcome on qubit 2 [see Fig. 1(c)]. If no eavesdropping exits, their outcomes should be completely opposite, i.e., if Alice gets $|0\rangle$ ($|1\rangle$), then Bob gets $|1\rangle$ ($|0\rangle$) and if Alice gets $|+\rangle$ ($|-\rangle$), then Bob gets $|-\rangle$ ($|+\rangle$). This method is sufficient to check whether the Alice-Bob channel is secure. In fact, in the present protocol there are two qubit-transmission quantum channels, the Alice-Bob quantum channel and the Alice-Charlie quantum channel. Here we only consider the security of the Alice-Bob channel. Due to symmetry, the security considerations for the Alice-Charlie quantum channel are the same, and so for simplicity, we do not discuss it here. Only when they ascertain that there is no eavesdropper, Eve, in each channel, as they proceed to (i). Otherwise, QSS is aborted.

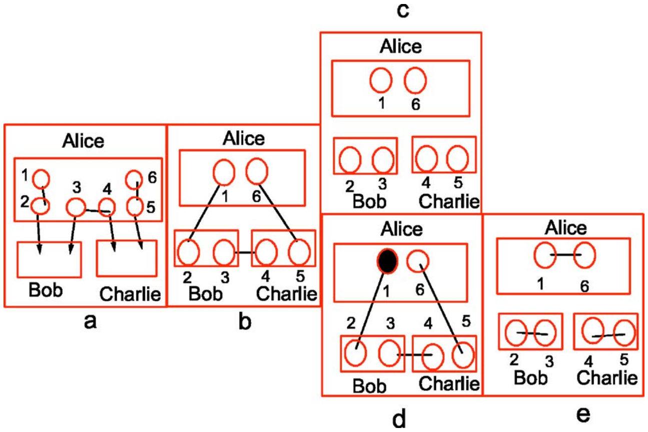

FIG. 1. (Color online) The detecting mode (*a-b-c*) and the message mode (*a-b-d-e*) of the present quantum secret sharing protocol. The hollow circle represents a qubit. The line between two qubits represents their entanglement. The solid circle in (d) indicates that a unitary operation has been performed on the qubit.

(iii) First, Alice performs a local unitary operation randomly on one of her two qubits 1 and 6, say, on qubit 1 [see Fig. 1(d)]. Then she performs a Bell-state measurement on qubits 1 and 6 and announces publicly her measurement outcome. After this, Bob and Charlie perform Bell-state measurements on their own qubits, respectively, and record the measurement outcomes. In fact, after Alice's Bell-state measurement, qubits 2 and 5 should project to one of the four Bell states [see Fig. 1(e)]. If Bob and Charlie collaborate, according to their Bell-state measurement outcomes and Alice's public announcement of the Bell-state measurement on qubits 1 and 6, they can deduce the exact local unitary operation that Alice performed on qubit 1 in terms of Eqs. (5)–(8) in a recursion way. For an example, if Bob's and Charlie's outcomes are respectively $|\Psi^-_{23}\rangle$ and $|\Phi^+_{45}\rangle$, since the state Alice prepared initially in qubits 3 and 4 is $|\Psi^-_{34}\rangle$, then from Eq. (7) they can know that qubits 2 and 5 have projected to $|\Phi^+_{25}\rangle$ after Alice's Bell-state measurement on qubits 1 and 6. Since both the initial states of the qubit pair (1, 2) and the initial states of the qubit pair (5, 6) are $|\Psi^-\rangle$, respectively, and Bob and Charlie know Alice's Bell-state measurement outcome on qubits 1 and 6 (say, $|\Psi^+_{16}\rangle$) and they have already deduced the state $|\Phi^+_{25}\rangle$ of qubits 2 and 5, then from Eq. (8) they can determine that the local unitary operation performed by Alice is u_4, that is, the secret message that Alice distributed is the two classical bits "11."

So far, we have presented a three-party QSS protocol completely based on the quantum entanglement swapping and identification of Bell states. Now let us analyze the security of the protocol. In order to acquire Alice's transmitted information, efficient eavesdroppers word capture the traveling qubits and replace them with their own qubits prepared in advance. But this eavesdropping can be detected in the detecting mode by using randomly chosen MB and comparing the measurement outcomes. Even if in the serious case of an insider, say, Charlie (Charlie*), cooperating with an outside eavesdropper, Eve, the eavesdropping can also be detected in the detecting mode. Our protocol is based on Einstein-Podolsky-Rosen (EPR) pairs, so the proof of the security is same in essence as those in Refs. [25–29]. Hence, the present protocol is secure against eavesdropping.

We have presented a three-party QSS protocol based on entanglement swapping. In fact, this is easily generalized to a multiparty case. Suppose that there are N parties. At first, each party prepares two qubits in the Bell state $|\Psi^-\rangle$. Then each of them sends one qubit to a specific partner and retains another in his or her own site, that is, the nth party prepares a qubit pair in $|\Psi^-\rangle$, then he or she sends one qubit to the $(n+1)$th party and stores one in his or her own site. (The Nth party sends one qubit to the first party.) After this procedure is successfully finished, they also have two options. One is to detect eavesdropping. This procedure is the same of essence as that of the three-party QSS protocol. Hence, the security of the generalized version can be confirmed. The other is to distribute the secret messages among the other parties. The sender (say, Alice, whose n order is assumed to be either the smallest or the largest one) performs a local unitary operation on one of her two qubits. Then Alice measures these two qubits on the basis of Bell state and announces the measurement outcome. After this, because the order of n is always increased (or decreased), each of the other parties performs in turn the Bell-state measurement on the two qubits in its own site. If they collaborate, they can successfully extract Alice's secret messages in a recursive way. Incidentally, in the generalized protocol, the order of measurement is very important. Once such an order is destroyed, then the secret message cannot be correctly extracted by the other parties even if they collaborate.

It should be pointed out that the preceding protocol seems to be designed only for ideal quantum channels. In this protocol the reliable sharing of an entangled qubit pair between two parties is very important and necessary. It is known that when a qubit of an entangled pair travels in a noisy quantum channel, the initial entanglement might be lost. Hence, a security problem for this protocol in a noisy channel seems to arise. Fortunately, it has been proven that over any long distance, two parties can reliably share an entangled pair by using the quantum-repeater technique, containing the entanglement purification and teleportation [30–34]. Once two parties have shared an entangled qubit pair, then in the detecting mode any eavesdropping can be detected by using the method of two MBs. Hence, even in a noisy channel the present protocol works securely also.

Now let us make some comparisons between the present protocol and other protocols [3,7]. First, we discuss three-party secret sharing protocols. In Ref. [3], GHZ states must be prepared for use. It is known that according to the present-day technologies a GHZ state might be synthesized from two Bell states, while the synthesization efficiency is lower (not greater that 50%). In order to send a shared key containing N bits [3], it is necessary to use on average $2N$ GHZ triplets because the three parties can successfully establish a joint key only half of the time. Hence, at least $4N$ Bell states must be employed to synthesize the $2N$ GHZ triplets. Once the joint key is established, Alice needs to send N classical bits to transmit her secret messages. Therefore, considering the $6N$ classical bits published by the three parties when establishing their joint key (all three parties must announce the direction of their measurements so that they can decide whether to keep or to discard the result from a given triplet), $7N$ classical bits in total need to be published in the protocol in Ref. [3]. In Ref. [7], only Bell states are employed and the protocol allows direct transmission of the sender's secret messages. In order to send N shared secret bits, [7], it is necessary to use on average $2N$ Bell states because of the success probability of $1/2$. Moreover, the $6N$ classical bits in total must be published by the three parties, because in each run, three-classical bits need to be publicly announced. Obviously, as far as the the three-party protocols are concerned, the protocol in Ref. [7] is better than that in Ref. [3]. Incidentally, the three-party protocol in Ref. [3] can be easily generalized to a $M(M\geqslant 4)$–party case, while that in Ref. [7] cannot.

In the present three-party protocol, classical secret bits can also be directly transmitted. To send N classical secret bits, due to the employment of dense coding, Alice needs to prepare $3N/2$ Bell states in message mode, and only she must publish N classical bits to enable Bob and Charlie to infer her secret bits. Because the possibility of message mode is $r=1-c$, in message mode, the total Bell states needed are $3N/[2(1-c)]$ and the total classical bits published are $N/(1-c)$. In fact, in the protocols in Refs. [3,7], something like message authentification must be used to detect possible attacks. In this case, more initial states and more public classical bits are needed. In the present protocol, to check the security of the two quantum channels, detecting mode is necessary. In detecting mode, to check the security of the two quantum channels, two Bell states are needed and four classical bits must be published in each run. Considering that the possibility of detecting mode is c, in detecting mode, $2/c$ Bell states and $4/c$ public classical bits are needed. If the estimations on both the resource and the public bits are simplified by eliminating both the message authentification procedure and detecting mode, one finds that the present protocol is best if the c value is small enough. By the way, in Ref. [35], the security related to c has been explicitly demonstrated. When the number n of transmitted bits is not too small, the security can be assured.

As mentioned, only the three-party protocol in Ref. [3] and the present one can be generalized to the $M(M\geqslant 4)$ case. Compared with the $M(M\geqslant 4)$–party protocol in Ref. [3], our protocol has distinct advantages. In the present protocol, only Bell states are used and need to be identified, and the parties can apply the entanglement purification protocol to reliably share a qubit pair in a Bell state [36,37]. However, for the protocol using $M(M \geqslant 4)$–qubit GHZ states, when the number M of all the parties is large, how to prepare a $M(M \geqslant 4)$–qubit GHZ state and how to reliably share the GHZ states among M parties warrant further study [38]. Moreover, when the secret sharing protocol is applied to secret message splitting, the advantage is also clear. For instance, as far as a 10-party protocol is concerned, if 10-particle GHZ states are used, one should prepare a 10-particle GHZ state in advance and perform 511 difficult multiparticle GHZ-state measurements (see Ref. [12]) for secret splitting. However, in the present protocol, we only need 10 Bell states as well as the complete Bell-state identification. This means that in the present protocol the experimental difficulties in preparing initial states and in discriminating some entangled states are greatly reduced. As for the public classical bits, when one party is increased, in the present protocol no public classical bits are increased, while in the protocol in Ref. [3] additional seven public classical bits are needed. Obviously, the present multiparty secret sharing protocol supersedes the counterpart protocol in Ref. [3]. Incidentally, we realize that the experimental realization of full Bell measurement represents an unsolved problem, which affects the advantage over some GHZ-based protocols. Hillery *et al.* [3] have clearly shown that their protocol supersedes the standard quantum cryptography and classical secret sharing protocols, and hence, the present protocol obviously supersedes them.

To summarize, we have presented a multiparty QSS protocol based on entanglement swapping of Bell states. The security of the protocol has been confirmed, even in a noisy quantum channel. The advantages of the present protocol are revealed.

This work is supported by the National Natural Science Foundation of China under Grant No. 10304022.

[1] B. Schneier, *Applied Cryptography* (Wiley, New York, 1996), p. 70.
[2] J. Gruska, *Foundations of Computing* (Thomson Computer Press, London, 1997), p. 504.
[3] M. Hillery, V. Buzek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).
[4] D. Gottesman, Phys. Rev. A **61**, 042311 (1999).
[5] M. K. Stephen Yeung and S. H. Strogatz, Phys. Rev. Lett. **82**, 648 (1999).
[6] S. Bandyopadhyay, Phys. Rev. A **62**, 012308 (2000).
[7] A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A **59**, 162 (1999).
[8] H. F. Chau, Phys. Rev. A **66**, 060302(R) (2002).
[9] S. Bagherinezhad and V. Karimipour, Phys. Rev. A **67**, 044302 (2003).
[10] G. P. Guo and G. C. Guo, Phys. Lett. A **310**, 247 (2003).
[11] L. Xiao, G. L. Long, F. G. Deng, and J. W. Pan, Phys. Rev. A **69**, 052307 (2004).
[12] Y. M. Li, K. S. Zhang, and K. C. Peng, Phys. Lett. A **324**, 420 (2004).
[13] W. Tittel, H. Zbinden, and N. Gisin, Phys. Rev. A **63**, 042301 (2001).
[14] V. Scarani and N. Gisin, Phys. Rev. Lett. **87**, 117901 (2001).
[15] W. Tittel, H. Zbinden, and N. Gisin, Phys. Rev. A **63**, 042301 (2001).
[16] A. M. Lance, T. Symul, W. P. Bowen, B. C. Sanders, and P. K. Lam, Phys. Rev. Lett. **92**, 177903 (2004).
[17] Z. J. Zhang, J. Yang, Z. X. Man, and Y. Li, Eur. Phys. J. D **33**, 133 (2005).
[18] Z. J. Zhang, Phys. Lett. A **342**, 60 (2005).
[19] Z. J. Zhang and Z. X. Man, Phys. Lett. A **341**, 55 (2005).
[20] Z. J. Zhang, Y. Li, and Z. X. Man, Phys. Rev. A **71**, 044301 (2005).
[21] M. Zukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, Phys. Rev. Lett. **71**, 4287 (1993).
[22] J. W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **80**, 3891 (1998).
[23] J. Lee, S. Lee, J. Kim, and S. D. Oh, Phys. Rev. A **70**, 032305 (2004).
[24] S. Bose, V. Vedral, and P. L. Knight, Phys. Rev. A **57**, 822 (1998).
[25] F. G. Deng, G. L. Long, and X. S. Liu, Phys. Rev. A **68**, 042317 (2003).
[26] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
[27] H. Inamori, L. Rallan, and V. Verdral, J. Phys. A **34**, 6913 (2001).
[28] G. L. Long and X. S. Liu, Phys. Rev. A **65**, 032302 (2002).
[29] E. Waks, A. Zeevi, and Y. Yamamoto, Phys. Rev. A **65**, 052310 (2002).
[30] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[31] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[32] H. J. Briegel, W. Dur, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).
[33] W. Dur, H. J. Briegel, J. I. Cirac, and P. Zoller, Phys. Rev. A **59**, 169 (1998).
[34] H. K. Lo and H. F. Chau, Science **283**, 2050 (1999).
[35] K. Bostroem and T. Felbinger, Phys. Rev. Lett. **89**, 187902 (2002).
[36] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sampera, Phys. Rev. Lett. **77**, 2818 (1996).
[37] B. S. Shi, Y. K. Jiang, and G. C. Guo, Phys. Rev. A **62**, 054301 (2000).
[38] Z. Zhao, Y. A. Chen, A. N. Zhang, T. Yang, H. J. Briegel, and J. W. Pan, Nature (London) **430**, 54 (2004).