Teleportation and secret sharing with pure entangled states

Somshubhro Bandyopadhyay*
Department of Physics, Bose Institute, 93/1 Acharya Prafulla Chandra Road, Calcutta 700009, India
(Received 5 November 1999; revised manuscript received 11 February 2000; published 15 June 2000)

We present two optimal methods of teleporting an unknown qubit using any pure entangled state. We also discuss how such methods can also have successful application in quantum secret sharing with pure multipartite entangled states.

PACS number(s): 03.67.Hk, 03.65.Bz

I. INTRODUCTION

In recent years quantum entanglement [1] has found many exciting applications that have considerable bearing on the emerging fields of quantum information [2] and quantum computing [3]. Two such key applications are quantum teleportation [4] and quantum secret sharing [9]. Quantum teleportation involves secure transfer of an unknown qubit from one place to another and in quantum secret sharing, quantum information encoded in a qubit is split among several parties such that only one of them is able to recover the qubit exactly provided all the other parties agree to cooperate.

In quantum teleportation two parties (Alice and Bob) initially share a maximally entangled state (for example, an EPR pair). Alice also holds another qubit unknown to her that she wants to teleport to Bob. For this purpose she performs a certain joint two particle measurement on her two qubits and communicates her result to Bob. Bob now applies appropriate unitary transformations on his qubit to bring it to the desired state. However faithful teleportation [4] (and also secure key distribution [5]) is not possible if the entangled state used as the quantum channel is not maximally entangled. In fact staying within the standard teleportation scheme it is no longer possible for Bob to reconstruct the unknown qubit exactly, with a nonzero (however small) probability. Recently, the issue of teleportation with pure entangled states has been considered by Mor and Horodecki [6] (originally in an earlier work of Tal Mor [7]) where they observed that teleportation can also be understood from a more general approach based on ''generating ρ-ensembles at space-time separation'' by exploiting the Hughston, Jozsa, and Wooters (HJW) result [8]. They introduced the concept of ''conclusive'' teleportation and showed how perfect teleportation having a finite probability of success is made possible with pure entangled states. By conclusive teleportation it is meant that for certain conclusive outcomes of some generalized measurement, perfect teleportation with fidelity one is achieved. Of course this cannot take place with certainty unless the state is maximally entangled. We note that the success probability of conclusive teleportation, which is twice the modulus square of the smaller Schmidt coefficient, as obtained by Mor and Horodecki (henceforth MH) is also optimal.

Quantum secret sharing [9] protocol allows for splitting the quantum information among several parties such that any one can recover the information but not without the assistance of the remaining parties. For simplicity all the discussions will be with three partite systems, although generalization to four or more parties is always possible. In this case three parties (say, Alice, Bob, and Charlie) initially share a maximally entangled state, for example, a Greenberger, Horne, Zeilinger (GHZ) state [11]. Besides Alice also holds another qubit carrying some information (in quantum information we know that a message is encoded in a qubit) and by performing a Bell measurement on her two qubits she succeeds in splitting the quantum information among Bob and Charlie. Observe that neither Bob nor Charlie can recover the qubit in its exact form only by themselves performing whatever local operations they wish to. If and only if they agree to act in concert, then performing certain local measurements and communicating among themselves, any one of them can recover the desired state. It is not possible for both to get hold of the state as it is forbidden by the no-cloning theorem. We note that the protocol of secret sharing is very similar to that of teleportation and in a situation where Alice, Bob, and Charlie share a nonmaximal entangled state, the protocol as it is will not be successful.

In this paper we consider the issue of teleportation and secret sharing with a pure entangled state (a pure entangled state will always be taken to be nonmaximal unless stated otherwise). We suggest two more methods for conclusive teleportation that are optimal. We refer to them as qubit-assisted conclusive teleportation processes, since in both the methods either Alice or Bob needs to prepare an ancillary qubit in some specified state for carrying out the protocol. The motivation behind suggesting two more methods are twofold. First, one is to obtain a possible improvement over MH's suggestion from an operational point of view with an eye towards future experiments. Second, exploring various explicit local strategies can also provide some insight that can be fruitful, considering their possible application in various other manipulations of quantum entanglement. We also show using the methods developed for teleportation how successful secret sharing can be implemented using pure entangled states. We will refer to this type of secret sharing as conclusive secret sharing.

The present paper is organized as follows. In Sec. II, we discuss the standard teleportation scheme of Bennett, Brassard, Crepeau, Jozsa, Peres and Wootters [(BBCJPW) protocol] [4] and see why it is not successful when the shared quantum channel is a nonmaximally entangled pure state.

*Electronic address: dhom@bosemain.boseinst.ernet.in

Section III introduces the concept of conclusive teleportation and the protocol of MH [6] is discussed in some detail. In Sec. IV we present two new proposals of conclusive teleportation and discuss relative merits of the suggested and the existing ones. In Sec. V we describe the quantum secret sharing protocol [9]. In Sec. VI we discuss what we call conclusive secret sharing, i.e., quantum secret sharing with pure entangled states. There we show how the methods developed in the preceding sections in the context of quantum teleporation have applications in quantum secret sharing. Finally in Sec. VII we summarize and conclude.

II. QUANTUM TELEPORTATION: BBCJPW PROTOCOL

Quantum teleportation [4] allows for sending quantum information encoded in a qubit (a spin-1/2 particle or any quantum two-level system) from one place to another without any material transfer of the particle itself. The two parties involved in this process initially share a maximally entangled state. The protocol is carried out only using local measurements (Bell measurement) and classical communication.

Let us suppose that Alice and Bob share a maximally entangled state, say,

$$|\psi\rangle_{AB}=\frac{1}{\sqrt{2}}(|00\rangle_{AB}+|11\rangle_{AB}) \tag{1}$$

and the state of the unknown qubit that Alice is supposed to send to Bob is

$$|\phi\rangle_1=a|0\rangle+b|1\rangle=\begin{pmatrix}a\\b\end{pmatrix}_1. \tag{2}$$

The combined state of the three qubits can be written as

$$|\Phi\rangle_{1AB}=\frac{1}{2}\left[|\Phi^+\rangle_{1A}\begin{pmatrix}a\\b\end{pmatrix}_B+|\Phi^-\rangle_{1A}\begin{pmatrix}a\\-b\end{pmatrix}_B+|\Psi^+\rangle_{1A}\begin{pmatrix}b\\a\end{pmatrix}_B+|\Psi^-\rangle_{1A}\begin{pmatrix}b\\-a\end{pmatrix}_B\right] \tag{3}$$

where the states, $|\Phi^\pm\rangle,|\Psi^\pm\rangle$ are defined by

$$|\Phi^\pm\rangle=\frac{1}{\sqrt{2}}(|00\rangle\pm|11\rangle);|\Psi^\pm\rangle=\frac{1}{\sqrt{2}}(|01\rangle\pm|10\rangle)$$

and form a basis (Bell basis) in the composite Hilbert space of Alice's two qubits.

At this stage Alice performs a measurement in the Bell basis on her two qubits and therefore obtains any one of the four Bell states randomly and with equal probability. She then communicates her result to Bob (which requires two classical bits), who in turn rotates his quibit accordingly to reconstruct the unknown state in its exact form.

However, in a situation where Alice and Bob share a nonmaximal but pure entangled state of the form, say,

$$|\psi\rangle_{AB}=\alpha|00\rangle_{AB}+\beta|11\rangle_{AB}\rangle \tag{4}$$

(where, $\alpha^2+\beta^2=1$, and we assume without any loss of generality that α, β is real with $\alpha\geqslant\beta$) and following the standard method for teleportation, Bob ends up with the state $\binom{a\alpha}{b\beta}$, which cannot be rotated back to the desired state $\binom{a}{b}$ without having any knowledge of the state parameters a and b. Since the state that is teleported is supposed to be unknown, the Bennett protocol fails to reproduce the state exactly on Bob's side.

III. CONCLUSIVE TELEPORTATION: PROPOSAL OF MOR AND HORODECKI

Quite recently in a very interesting paper, Mor and Horodecki [6] suggested a protocol for teleportation when Alice and Bob share a nonmaximal pure entangled state. They obtained the optimal probability for successful teleportation, which is given by twice the modulus square of the smaller Schmidt coefficient of the state in question. The method succeeds sometimes and when it succeeds the fidelity is one, implying that the unknown state is exactly reproduced on Bob's side. Following Mor and Horodecki we will continue to refer to teleportation with pure entangled states as conclusive teleportation.

We begin with the fact that Alice and Bob share the pure entangled state (4) and the unknown state that Alice wishes to send to Bob is given by (2). The central feature of the scheme is to write down the combined three qubit state in the following way:

$$|\Psi\rangle=|\phi\rangle|\psi\rangle=\frac{1}{2}\Bigg[(\alpha|00\rangle+\beta|11\rangle)_A\begin{pmatrix}a\\b\end{pmatrix}_B+(\alpha|00\rangle-\beta|11\rangle)_A\begin{pmatrix}a\\-b\end{pmatrix}_B+(\beta|01\rangle+\alpha|10_A\begin{pmatrix}b\\a\end{pmatrix}_B+(\beta|01\rangle-\alpha|10_A\begin{pmatrix}-b\\a\end{pmatrix}_B\Bigg]. \tag{5}$$

Now measurement on Alice's side takes place in two steps. The first measurement projects the state onto either of the subspaces spanned by $\{|00\rangle, |11\rangle\}$ or $\{|01\rangle, |10\rangle\}$. Thus this measurement has two possible outcomes that occur with equal probability. Suppose the result is the subspace spanned by $\{|00\rangle, |11\rangle\}$. Alice now performs an optimal positive operator value measure [10] (POVM) that distinguishes conclusively between the two nonorthogonal states $\binom{\alpha}{\beta}_{\{00,11\}}$ and $\binom{\alpha}{-\beta}_{\{00,11\}}$. The probability of obtaining a conclusive result is $2\beta^2$ (β is the smaller of the Schmidt coefficients). Thus this is the probability of successful teleportation with fidelity one. The number of classical bits required in the above method is three. One bit is required for Alice to inform Bob whether she is successful in discriminating between the nonorthogonal states and two more bits are required so that Bob performs the required rotations to reconstruct the unknown state. Note that the above proposal cannot succeed always. This is because there is always a possibility of an inconclusive result in the state discrimination procedure. But when it succeeds, the probability of success being $2\beta^2$, the fidelity of teleportation is one. Also note that for $\beta=1/\sqrt{2}$, which corresponds to a maximally entangled state, the proposal is always successful with certainty as there need not be any inconclusive result since in this case one discriminates between two orthogonal states.

IV. QUBIT-ASSISTED CONCLUSIVE TELEPORTATION

We now discuss two methods for conclusive teleportation that are optimal. We will see that both these methods can appropriately be referred to as qubit-assisted processes, since in both schemes either Alice or Bob are required to prepare a qubit in some specified state to implement the respective protocol. Since the process of teleportation involves two parties, modifications, as far as measurement and other operations are concerned, may be suggested for any one of the parties without introducing any new operations for the other side. By this we mean that we can either modify the measurement part of Alice keeping the Bob part the same, i.e., he only has to do the standard rotations (proposal 1) or we can also suggest some further operations to be carried out by Bob once the original protocol of teleportation gets completed (proposal 2), which implies the measurement part of Alice remains unchanged.

A. Proposal I

The basic idea is as follows. Alice first prepares an ancilla qubit in a state, say $|\chi\rangle$, besides her usual possession of two qubits. She now performs a certain joint three particle measurement on her three qubits. It will be shown that for some of her results, Bob needs to perform only the standard rotations $(\sigma_z, \sigma_x, \sigma_z\sigma_x)$ to exactly reconstruct the unknown state, after he gets some information from Alice. However, for any of the remaining possible set of outcomes, the method works exactly the same way as that of Mor and Horodecki, discussed in the previous section. The method that we propose fails sometimes, but when successful, the fidelity of teleportation is one.
Suppose Alice and Bob share a pure entangled state given by (4) and the state that Alice wants to teleport to Bob is given by (2).
Alice now prepares an ancilla qubit in the state,

$$|\chi\rangle_2 = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}_2. \tag{6}$$

Observe that the state parameters of this ancillary qubit that Alice prepares are the Schmidt coefficients of the pure entangled state.

Now, the combined state of the four qubits is given by

$$|\Psi\rangle_{12AB} = |\phi\rangle_1 \otimes |\chi\rangle_2 \otimes |\psi\rangle_{AB} = \begin{pmatrix} a \\ b \end{pmatrix}_1 \otimes \begin{pmatrix} \alpha \\ \beta \end{pmatrix}_2 \otimes (\alpha|00\rangle + \beta|11\rangle)_{AB} \tag{7}$$

and we observe that the state $|\Psi\rangle_{12AB}$ can also be written as (we omit the tensor product sign henceforth)

$$\begin{aligned}|\Psi\rangle_{12AB} = \frac{\sqrt{\alpha^4+\beta^4}}{2}\Bigg[\Bigg(&(\alpha'|\Phi_1\rangle_{12A} + \beta'|\Phi_2\rangle_{12A})\begin{pmatrix} a \\ b \end{pmatrix}_B \\ &+ (\alpha'|\Phi_1\rangle_{12A} - \beta'|\Phi_2\rangle_{12A})\begin{pmatrix} a \\ -b \end{pmatrix}_B \\ &+ (\beta'|\Phi_3\rangle_{12A} + \alpha'|\Phi_4\rangle_{12A})\begin{pmatrix} b \\ a \end{pmatrix}_B \\ &+ (\beta'|\Phi_3\rangle_{12A} - \alpha'|\Phi_4\rangle_{12A})\begin{pmatrix} -b \\ a \end{pmatrix}_B \\ &+ \frac{\alpha\beta}{hJ}\Bigg[|\Phi_5\rangle_{12A}\begin{pmatrix} a \\ b \end{pmatrix}_B + |\Phi_6\rangle_{12A}\begin{pmatrix} a \\ -b \end{pmatrix}_B \\ &+ |\Phi_7\rangle_{12A}\begin{pmatrix} b \\ a \end{pmatrix}_B + |\Phi_8\rangle_{12A}\begin{pmatrix} -b \\ a \end{pmatrix}_B\Bigg],\end{aligned} \tag{8}$$

where $\alpha' = \alpha^2/\sqrt{\alpha^4+\beta^4}$ and $\beta' = \beta^2/\sqrt{\alpha^4+\beta^4}$.

The important thing to note from Eq. (8) is that we have succeeded in writing down the combined state in a way such that one part clearly resembles the one in the BBCJPW protocol (see Sec. I), whereas the other part resembles that of Mor and Horodeckis' (see Sec. II). This is turn implies that for a suitable measurement by Alice, there are some outcomes where only standard rotations by Bob are sufficient to construct the unknown state after he receives the result of Alice's measurement. If this is not the case then, of course, one has to resort to the POVM for state discrimination. The task is now to specify the kind of measurement that Alice should perform on her three qubits.

Observe that the following set $\{\Phi_i\}$, $i=1,2,\ldots,8$, forms a complete orthonormal basis of the combined Hilbert space of the three spin-1/2 particles (or two-level systems) that Alice holds and is defined by

$$\begin{gathered}|\Phi_1\rangle = |000\rangle, \quad |\Phi_2\rangle = |111\rangle, \quad |\Phi_3\rangle = |011\rangle, \\ |\Phi_4\rangle = |100\rangle, \\ |\Phi_5\rangle = \frac{1}{\sqrt{2}}[|010\rangle + |101\rangle], \quad |\Phi_6\rangle = \frac{1}{\sqrt{2}}[|010\rangle - |101\rangle], \\ |\Phi_7\rangle = \frac{1}{\sqrt{2}}[|001\rangle + |110\rangle], \quad |\Phi_8\rangle = \frac{1}{\sqrt{2}}[|001\rangle - |110\rangle].\end{gathered} \tag{9}$$

We now consider the following set of projection operators $\{P_1, P_2, P_3, P_4, P_5, P_6\}$ defined by

$$\begin{gathered}P_1 = P[\Phi_1] + P[\Phi_2], \quad P_2 = P[\Phi_3] + P[\Phi_4], \\ P_3 = P[\Phi_5]; \quad P_4 = P[\Phi_6], \quad P_5 = P[\Phi_7]; \quad P_6 = P[\Phi_8].\end{gathered} \tag{10}$$

In principle, the measurement of an observable O is always possible whose corresponding operator is represented by

$$O=\sum_{i=1}^{6} p_i P_i, \tag{11}$$

where Eq. (11) is the spectral decomposition of the operator O. The projectors involved in this spectral decomposition are not of the same nature. One essentially has in the set two types of projectors, both one-dimensional and two-dimensional ones. P_1 and P_2 are the two-dimensional projectors that project a state onto the subspaces spanned by $\{\Phi_1,\Phi_2\}$ and $\{\Phi_3,\Phi_4\}$, respectively, whereas the rest are all one-dimensional projectors.

Alice can now perform a joint three particle measurement in accordance with Eq. (11). The possible outcomes can broadly be divided into two types.

Type a: If she obtains any one of the states belonging to the set $\{|\Phi_5\rangle,|\Phi_6\rangle,|\Phi_7\rangle,|\Phi_8\rangle\}$, each of which occurs with probability $\alpha^2\beta^2/2$, the state of Bob's particle is projected onto one of the following states, $\binom{a}{b},\binom{a}{-b},\binom{b}{a},\binom{-b}{a}$. Qualitatively this set of outcomes resembles what we have seen in the standard teleportation scheme. So, Alice now informs Bob of the outcome of her measurement and that requires two classical bits. Thereafter Bob can appropriately rotate his qubit to bring it to the desired state.

Type b: But Alice's measurement may also project the state onto either of the subspaces spanned by $\{\Phi_1,\Phi_2\}$ and $\{\Phi_3,\Phi_4\}$, and each such result occurs with probability $(\alpha^4+\beta^4)/2$. Suppose the result is the subspace spanned by $\{\Phi_1,\Phi_2\}$. From (8) it follows that after such an outcome is obtained, the combined four qubit state is given by

$$|\Psi\rangle_{12AB}=(\alpha'|\Phi_1\rangle_{12A}+\beta'|\Phi_2\rangle_{12A})\begin{pmatrix} a\\ b\end{pmatrix}_B + (\alpha'|\Phi_1\rangle_{12A}-\beta'|\Phi_2\rangle_{12A}])\begin{pmatrix} a\\ -b\end{pmatrix}_B. \tag{12}$$

At this stage she performs an optimal POVM to conclusively distinguish between the two states, $\binom{\alpha'}{\beta'}_{\{\Phi_1;\Phi_2\}}$ and $\binom{\alpha'}{-\beta'}_{\{\Phi_1;\Phi_2\}}$ [the scalar product of these two nonorthogonal states is $(\alpha'^2-\beta'^2)$]. The respective positive operators that form an optimal POVM in this subspace are

$$A_1=\frac{1}{2\alpha'^2}\begin{pmatrix} \beta'^2 & \alpha'\beta' \\ \alpha'\beta' & \alpha'^2\end{pmatrix}; \quad A_2\begin{pmatrix} \beta'^2 & -\alpha'\beta' \\ -\alpha'\beta' & \alpha'^2\end{pmatrix};$$

$$A_3=\begin{pmatrix} 1-\dfrac{\beta'^2}{\alpha'^2} & 0 \\ 0 & 0\end{pmatrix}. \tag{13}$$

The optimal probability of obtaining a conclusive result from such a generalized measurement (POVM) is $2\beta'^2=2\beta^4/(\alpha^4+\beta^4)$.

Suppose Alice obtains a conclusive result and therefore concludes that the joint state of her two qubit is now $\binom{\alpha'}{\beta'}_{\{\Phi_1;\Phi_2\}}$. She now informs Bob that she had been successful in state discrimination and this requires one classical bit. Clearly this information alone is not sufficient for Bob because he does not have the information about the phase. So Alice needs to send two more classical bits of information to enable Bob to apply the necessary unitary transformation on his qubit. Thus a conclusive result followed by three bits of classical information results in perfect teleportation of the unknown qubit.

So, given our scheme what is the probability of successful teleportation with fidelity one? It is easy to obtain that the probability p of having perfect teleportation is

$$p=2\beta^4+2\alpha^2\beta^2=2\beta^2. \tag{14}$$

As noted earlier this probability is the optimal probability of perfect teleportation with a pure entangled state. We would like to mention that the number of classical bits required in this method depends on the outcome of Alice's measurement. If her result falls in the set when no POVM is required, then the number of classical bits required is two and if it is not, the number of classical bits required is three.

Although the above scheme may appear to be more complicated involving joint three particle measurement, still it simplifies the matter in other ways. For example, we have shown that there are possibilities when no POVM is required and for those outcomes the protocol runs exactly the same way as for a maximally entangled state. By introducing an extra qubit this partial dependence on POVM is achieved albeit at the cost of a joint three particle measurement. It is now clear that an outcome falling in the set ''type *a*'' greatly simplifies the remaining operations to be performed. But the probability of obtaining an outcome of ''type *a*'' being $2\alpha^2\beta^2$ is always less than $\alpha^4+\beta^4$, the probability that an outcome of ''type *b*'' has been realized. This implies that in more occasions Alice needs to undergo the state discrimination measurement to achieve perfect teleportation although realization of a ''type *a*'' result would have simplified her task considerably.

B. Proposal II

So far we have seen that the suggested methods actually modify the measurement part on Alice's side. But we can also think of local operations that may be carried out by Bob after Alice performs a Bell measurement on her two qubits and communicates her result, following the standard teleportation protocol [4]. This is what we do now. This proposal is carried out in two steps. In the first step the standard teleportation scheme is followed so that the state of Bob's qubit at the end of this is given by $\binom{a\alpha}{b\beta}$. The second step involves certain local operations to be performed by Bob.

We first briefly discuss the CNOT operation, which will be in use to carry out the protocol. A controlled-NOT gate (or quantum XOR) flips the second spin if and only if the first spin is ''up'' i.e., it changes the second bit if and only if the first bit is ''1.''[1] It is a unitary transformation, denoted by

[1]In our notation $|\uparrow\rangle=|1\rangle$ and $|\downarrow\rangle=|0\rangle$.

U_{XOR}, acting on pairs of spin-1/2 and defined by the following transformation rules:

$$|00\rangle \rightarrow |00\rangle;|01\rangle \rightarrow |01\rangle; \quad |10\rangle \rightarrow |11\rangle;|11\rangle \rightarrow |10\rangle, \tag{15}$$

or when written in matrix form

$$U_{\mathrm{XOR}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{16}$$

Note that the CNOT gate cannot be decomposed into a tensor product of two single bit transformation. The method that we propose now is as follows: Recall that following the Bennett protocol when Alice and Bob share a pure entangled state, Bob ends up with a state given by $\binom{a\alpha}{b\beta}$. Till this stage the number of classical bits required is two and no more bits will be required because all operations will now be carried out by Bob and there is no need to communicate any further with Alice.

We start from this stage when the state of Bob's qubit (we refer this qubit as ''qubit 1'' for convenience) is given by $\binom{a\alpha}{b\beta}_1$ and suggest the following local operations. Bob prepares an ancilla qubit (qubit 2) in a state $|0\rangle_2$. Thus the combined state of the two qubits that Bob holds is now given by

$$|\Psi\rangle_{12} = a\alpha|00\rangle_{12} + b\beta|10\rangle_{12}. \tag{17}$$

Bob now performs a CNOT operation on his two qubit state, thus transforming it into the state

$$|\Psi\rangle_{12} = a\alpha|00\rangle_{12} + b\beta|11\rangle_{12}. \tag{18}$$

Thus the two particles become entangled and this is absolutely necessary. The whole idea is to entangle the particle with an ancilla and then perform some measurement that serves the purpose. Now observe that the state given by (18) can also be written as,

$$|\Psi\rangle_{12} = \frac{1}{2}\left[(\alpha|0\rangle + \beta|1\rangle)_1 \begin{pmatrix} a \\ b \end{pmatrix}_2 + (\alpha|0\rangle - \beta|1\rangle)_1 \begin{pmatrix} a \\ -b \end{pmatrix}_2\right] \tag{19}$$

From (19) it is clear that a state discrimination measurement, which can conclusively distinguish between the two nonorthogonal states $\alpha|0\rangle + \beta|1\rangle$ and $\alpha|0\rangle - \beta|1\rangle$, will give the desired result.

In the last subsection we have discussed in some detail the formalism and the respective operators involved in such a measurement. So we do not give the explicit representation here. Now, this optimal state discrimination measurement, which is an optimal POVM, can be carried out on any one of the two qubits that Bob holds and let us assume that it is qubit 1 on which such a measurement is performed. As we have seen earlier the optimal probability of a conclusive result is $2\beta^2$. It is clear that this is also the probability of perfect teleportation with fidelity one, because a conclusive outcome implies that the state of qubit 2 is now given by either $\binom{a}{b}$ or $\binom{a}{-b}$ depending on the state of qubit 1. For example, suppose Bob concludes that the state of qubit 1 after his POVM is $\binom{\alpha}{\beta}$, then with certainty he also concludes that the state of qubit 2 is now what he desired. Thus this method also produces the optimal probability of successful teleportation.

V. QUANTUM SECRET SHARING

In quantum secret sharing [9] a person splits quantum information (encoded in qubits) among several other persons such that no individual can recover the whole information unless properly aided by the rest. This is another useful application of quantum entanglement and can play important roles in various diverse practical scenarios (see Ref. [9]). For simplicity we will be explicit only in three partite systems but the methods can nevertheless be generalized to any number of parties.

The protocol of quantum secret sharing is as follows. Three parties, say, Alice, Bob, and Charlie, initially share a maximally entangled state, for example, a GHZ state [11],

$$|\psi\rangle_{ABC} = \frac{1}{\sqrt{2}}(|000\rangle_{ABC} + \beta|111\rangle_{ABC}). \tag{20}$$

Alice also possesses another qubit, say, $\binom{a}{b}$. Alice performs a Bell measurement on her two qubits and communicates her result to Bob and Charlie, who in turn can perform appropriate rotations on their respective qubits so that the pure entangled state that they now share can be written as

$$|\Psi\rangle_{BC} = a|00\rangle_{BC} + b|11\rangle_{BC}. \tag{21}$$

Since information can be encoded in the state of a qubit, by performing the Bell measurement Alice actually splits the information that is now shared via the pure entangled state (21) between Bob and Charlie. The important thing to note is that neither Bob nor Charlie can recover the state $\binom{a}{b}$ by any general operations on their respective sides without communicating among themselves. They individually do not have any useful information whatsoever. Though they have the amplitude information, that is not sufficient since information about the phase is not available. So, in this situation only one of the parties (either Bob or Charlie) will be able to reconstruct the state, provided the other party agrees to cooperate. Assuming that they do agree to work in tandem and they also agree on the person (let us assume it is Charlie) who will have the state, the remaining part of the protocol now goes like this. First we rewrite the state given by (21) in the following way:

$$|\Psi\rangle_{BC} = \frac{1}{\sqrt{2}}\left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_B \begin{pmatrix} a \\ b \end{pmatrix}_C + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)_B \begin{pmatrix} a \\ -b \end{pmatrix}_C\right]. \tag{22}$$

Bob performs a measurement on his qubit in the x basis where the x eigenstates are defined by

$$|x\pm\rangle=\frac{1}{\sqrt{2}}(|0\rangle\pm|1\rangle) \tag{23}$$

and communicates his outcome to Charlie. This requires only one bit of information. Charlie now can appropriately rotate his qubit to reconstruct the unknown state. Note that the protocol is very similar to that of teleportation. Now, it is easy to see that instead of sharing a GHZ state, if Alice, Bob, and Charlie initially shared a nonmaximally entangled state of the form

$$|\psi\rangle_{ABC}=\alpha|000\rangle_{ABC}+\beta|111\rangle_{ABC}, \tag{24}$$

then following the protocol as it is Charlie ends up with the state $\binom{a\alpha}{b\beta}$. But this is not the state that Charlie wishes to have. Recall that we faced a similar situation in the case of quantum teleportation and the similarity between the nature of these two processes indicates the possibility of successful application of the methods developed for teleportation in this scenario. Indeed we will see that the methods discussed in the previous sections can be suitably applied so that secret sharing becomes ultimately successful with a nonzero probability. As we shall also see in this case the probability of successful secret sharing will turn out to be $2\beta^2$ and is conjectured to be optimal. This is the subject of the next section.

VI. QUANTUM SECRET SHARING WITH PURE ENTANGLED STATES: CONCLUSIVE QUANTUM SECRET SHARING

Note that we can broadly view the information splitting process as a method carried out in three stages.

First stage: Measurement by Alice and communication of her outcome to Bob and Charlie. Bob and Charlie rotate their respective qubits so that their state is given by (21).

Second stage: Measurement by Bob and communication of his result to Charlie.

Final stage: Charlie performs some unitary transformation on his qubit if necessary.

Since our goal is to implement secret sharing successfully with nonmaximal entangled states, we can suggest modifications at any one such stage. We propose three explicit schemes for this purpose. To be explicit, the first scheme changes the type of measurement by Alice only, keeping the remaining part of the original protocol intact. The second one keeps the measurement part of Alice intact but modifies that of Bob and the last method keeps the whole protocol intact till Charlie's end and suggests further local operations to be carried out by him. We will not describe the first and the last scheme in detail because the methods that have been developed (including that of Mor and Horodecki) will be used and there is no qualitative difference with teleportation as far as their application is concerned. The second proposal will be described in detail. As we shall see later, we can appropriately call such quantum secret sharing conclusive quantum secret sharing because the success of the protocol depends on conclusive outcomes of some generalized measurements. We begin with the fact that Alice, Bob, and Charlie share a pure entangled state of the form (24).

A. Proposal I

The goal of this proposal is to modify the measurement part of Alice so that after Alice carries out her specific measurement and communicates her result, the state of Bob and Charlie will be given by (21). If this is achieved, then the remaining part goes exactly as in the original protocol of Hillary *et al.* [9]. To achieve this purpose we note that two methods that have already been suggested for teleportation with pure entangled states may turn out to be useful. Indeed, when Alice performs a measurement on her qubits either following the MH protocol (Sec. II) or Proposal I of qubit-assisted conclusive teleportation (QACT) scheme, in either case after she communicates her outcome to Bob and Charlie, the state shared by Bob and Charlie is given by (21), which is precisely what we intended to achieve. It is easy to see that the probability of such conclusive secret sharing is $2\beta^2$.

B. Proposal II

The previous proposal suggested changes in the type of measurement by Alice. In this proposal we keep that part the same as that in [9], i.e., Alice first performs a Bell measurement on her two qubits and so on. Since now Alice, Bob, and Charlie initially shared a pure entangled state (24), then after completion of the first stage of the protocol [9], the entangled state shared by Bob and Charlie will be

$$|\Psi\rangle_{BC}=a\alpha|00\rangle_{BC}+b\beta|11\rangle_{BC} \tag{25}$$

instead of (21).

This state (25) can also be written as,

$$|\Psi\rangle_{BC}=\frac{1}{2}\left[(\alpha|0\rangle+\beta|1\rangle)_B\begin{pmatrix}a\\b\end{pmatrix}_C+(\alpha|0\rangle-\beta|1\rangle)_B\begin{pmatrix}a\\-b\end{pmatrix}_C\right]. \tag{26}$$

Now, a conclusive result of a POVM (discussed in Sec. IV A, for details see [10]) by Bob to discriminate between the two nonorthogonal states $\alpha|0\rangle+\beta|1\rangle$ and $\alpha|0\rangle-\beta|1\rangle$ is sufficient. It is clear from (26) that when Bob concludes that the state of his qubit is $\alpha|0\rangle+\beta|1\rangle$ (or $\alpha|0\rangle-\beta|1\rangle$), the state of Charlie's qubit is projected onto $a|0\rangle+b|1\rangle$ (or $a|0\rangle-b|1\rangle$). But for Charlie to have this information Bob needs to communicate with him and he needs to do that twice. First he informs if he is successful (requires one classical bit) and if he is, then he notifies his result (requiring 1 classical bit) so that Charlie can perform an appropriate rotation if necessary.

The probability of this being successful is nothing but the probability of obtaining a conclusive result from the state discrimination measurement. So the probability of being successful is $2\beta^2$.

C. Proposal III

This proposal follows the original secret sharing protocol to its fullest so that at the end the state of Charlie's qubit is $a\alpha|0\rangle + b\beta|1\rangle$. In fact in teleportation when the standard scheme was followed, the state of Bob's qubit resulted in the same state. So we can successfully apply here the proposal II of QACT to recover the desired state, which is discussed in detail in Sec. IV B. Again the probability of being successful is $2\beta^2$.

VII. SUMMARY AND CONCLUSION

In summary, we have described two optimal methods for teleporting an unknown quantum state using any pure entangled state. A positive implication of one of our strategies is in its partial dependence on POVM to achieve perfect teleportation where we have seen that for some of Alice's outcomes, only standard rotations are to be performed by Bob to get the unknown state. Nevertheless the cost one has to pay for it is a joint three particle measurement. The number of classical bits required is three if it is necessary to perform a POVM, otherwise it is two. The second strategy reduces the number of classical bits to two, since the local operations are carried out by Bob after following the standard teleportation scheme.

We have also discussed how the methods developed for conclusive teleportation can be successfully applied in quantum secret sharing in a situation where the parties share a pure nonmaximal entangled state among themselves. We call it conclusive secret sharing analogous to conclusive teleportation. Here we have exploited the qualitative similarity between the two processes of teleportation and secret sharing. The success probability of such conclusive secret sharing also happens to be twice the square of the smaller Schmidt coefficient (the three partite entangled state in consideration is Schmidt decomposable) and is conjectured to be optimal.

ACKNOWLEDGMENTS

I wish to acknowledge Guruprasad Kar and Anirban Roy for many stimulating discussions. I thank Ujjwal Sen for careful reading of the manuscript.

[1] E. Schrodinger, Naturwissenschaften **23**, 807 (1935); **23**, 823 (1935); **23**, 844 (1935); for a review see M. B. Plenio and V. Vedral, Contemp. Phys. **39**, 431 (1998); lecture notes of Lucien Hardy available at http://www.qubit.org.

[2] C. H. Bennett, Phys. Today **48**, 24 (1995); J. Preskill, Proc. R. Soc. A: Math. Phys. Eng. **454**, 469 (1998).

[3] A brief but excellent article is by R. Jozsa, e-print quant-ph/9707034; C. H. Bennett and D. DiVincenzo, Nature (London) **377**, 389 (1995).

[4] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).

[5] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[6] T. Mor and P. Horodecki, e-print quant-ph/9906039.

[7] T. Mor, e-print quant-ph/9608005.

[8] L. P. Hughston, R. Jozsa, and W. K. Wootters, Phys. Lett. A **183**, 14 (1993).

[9] M. Hillery, V. Buzek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).

[10] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer, Dordrecht, 1993), Chap. 9.

[11] D. M. Greenberger, M. A. Horne, and A. Zeilinger, Am. J. Phys. **58**, 1131 (1990).