Broadcasting of three-qubit entanglement via local copying and entanglement swapping

Satyabrata Adhikari* and B. S. Choudhury
Department of Mathematics, Bengal Engineering and Science University, Howrah-711103, West Bengal, India

(Received 13 February 2006; published 19 September 2006)

In this work, we investigate the problem of a secretly broadcasting of a three-qubit entangled state between two distant partners. The interesting feature of this problem is that starting from two-particle entangle states shared between two distant partners we find that the action of a local cloner on the qubits and the measurement on the machine state vector generates three-qubit entanglement between them. The broadcasting of entanglement is made secret by sending the measurement result secretly using cryptographic scheme based on orthogonal states. Further we show that this idea can be extended to generate three-particle entangled states between three distant partners.

DOI: 10.1103/PhysRevA.74.032323 PACS number(s): 03.67.−a

I. INTRODUCTION

The No cloning theorem is one of the most fundamental theorems in quantum computation and quantum information[1]. The theorem states that there does not exist any process, which turns two distinct nonorthogonal quantum states ψ, ϕ into states $\psi\otimes\psi$, $\phi\otimes\phi$, respectively. These restrictions can be successfully utilized in quantum cryptography [2]. Although we cannot copy an unknown quantum state perfectly one can always do it approximately. Beyond the no-cloning theorem, one can clone an arbitrary quantum state perfectly with some nonzero probability [3]. In the past years, much progress has been made in designing a quantum cloning machine. A first step towards the construction of an approximate quantum cloning machine was taken by Buzek and Hillery (BH) in 1996 [4]. They showed that the quality of the copies produced by their machine remain the same for all input states. This machine is popularly known as the universal quantum cloning machine (UQCM). Later this UQCM was proved to be optimal [5]: After that the different sets of quantum cloning machines such as the set of universal quantum cloning machines, the set of state dependent quantum cloning machines (i.e. the quality of the copies depend on the input state), and the probabilistic quantum cloning machines were proposed. Entanglement [6], the heart of quantum-information theory, plays a crucial role in computational and communicational purposes. Therefore, as a valuable resource in quantum-information processing, quantum entanglement has been widely used in quantum cryptography [7,8], quantum superdense coding [9], and quantum teleportation [10]. An astonishing feature of quantum-information processing is that information can be "encoded" in nonlocal correlations between two separated particles. The more "pure" is the quantum entanglement, the more "valuable" is the given two-particle state. Therefore, to extract pure quantum entanglement from a partially entangled state, researchers have done a lot of work inthe past years on purification procedures [11]. In other words, it is possible to compress locally an amount of quantum information. Now generally a question arises: whether the opposite is true or not, i.e., can quantum correlations be "decompressed?" This question was tackled by several researchers [12,13] using the concept of "broadcasting of quantum inseparability." Broadcasting is nothing but a local copying of nonlocal quantum correlations. That is the entanglement originally shared by a single pair is transferred into two less entangled pairs using only local operations. Suppose two distant parties A and B share two-qubit entangled states

$$|\psi\rangle = \alpha|00\rangle_{AB} + \beta|11\rangle_{AB}, \tag{1}$$

where α is real and β complex and the parameters satisfying the relation $\alpha^2+|\beta|^2=1$. The first qubit belongs to A and the second belongs to B. Each of the two parties now perform local copiers on their own qubit and then it turns out that for some values of α, (1) nonlocal output states are inseparable, and (2) local output states are separable.

In a classical theory one can always broadcast information but in quantum theory, broadcasting is not always possible. Barnum *et al.* showed that noncommuting mixed states cannot be broadcasted [14]. However, for pure states broadcasting is equivalent to cloning.

Buzek *et al.* [12] were the first who showed that the decompression of initial quantum entanglement is possible, i.e., that from a pair of entangled particles, two less entangled pairs can be obtained by a local operation. That means that inseparability of quantum states can be partially broadcasted (cloned) with the help of local operation. They used optimal universal quantum cloners for local copying of the subsystems and showed that the nonlocal outputs are inseparable if

$$\frac{1}{2}-\frac{\sqrt{39}}{16}\leq\alpha^2\leq\frac{1}{2}+\frac{\sqrt{39}}{16}. \tag{2}$$

Further, Bandyopadhyay *et al.* [13] studied the broadcasting of entanglement and showed that only those universal quantum cloners whose fidelity is greater than $\frac{1}{2}\left(1+\sqrt{\frac{1}{3}}\right)$ are suitable because only then the nonlocal output states become inseparable for some values of the input parameter α. They proved that an entanglement is optimally broadcast only when optimal quantum cloners are used for local copying and also showed that broadcasting of entanglement into more than two entangled pairs is not possible using only local

*Corresponding author. E-Mail address: satyyabrata@yahoo.com

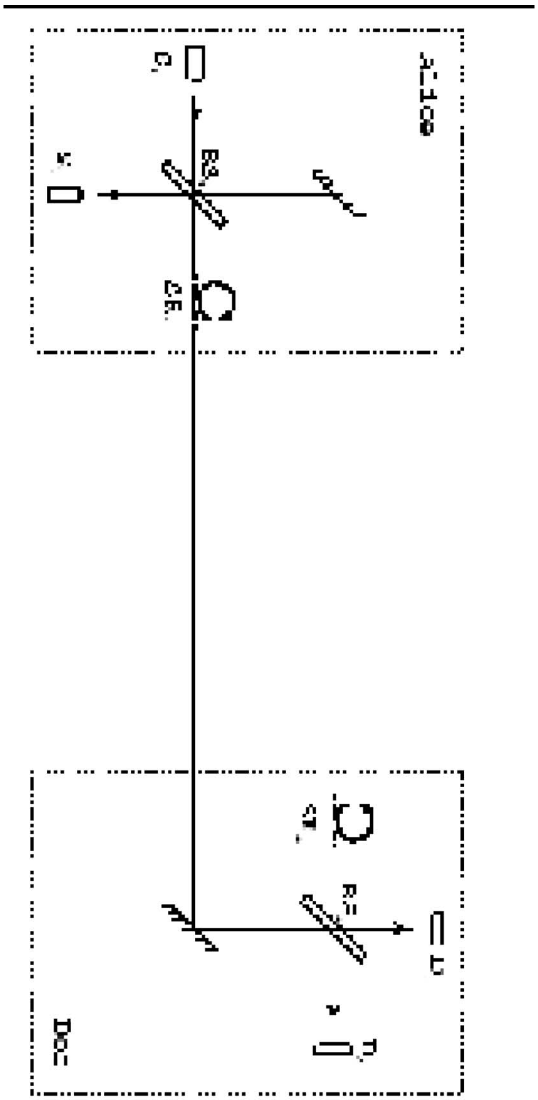

FIG. 1. Pictorial representation of the cryptographic scheme is shown in the given figure. The cryptographic scheme based on a Mach-Zehnder interferometer. The device consists of two-particle sources $S0$ and $S1$, a beam-splitter BS1, two mirrors, two storage rings SR1 and SR2, a beam-splitter BS2, and two detectors $D0$ and $D1$. The device is tuned in such a way that, if no eavesdropper is present, a particle emitted by $S0$ ($S1$) is finally detected by $D0$ ($D1$).

operations. Ghiu investigated the broadcasting of entanglement by using local $1 \rightarrow 2$ optimal universal asymmetric Pauli machines and showed that the inseparability is optimally broadcast when symmetric cloners are applied [15].

Motivated from the previous works on broadcasting of entanglement, we investigate the problem of the secretly broadcasting of a three-qubit entangled state between two distant partners with an universal quantum cloning machine and then the result is generalized to generate secret entanglement among three parties. Three-qubit entanglement between two distant partners can be generated as follows: Let us suppose that the two distant partners share an entangled state $|\psi\rangle_{12}=\alpha|00\rangle+\beta|11\rangle$. The two parties then apply the optimal universal quantum cloning machine on their respective qubits to produce a four-qubit state $|\chi\rangle_{1234}$. One party (say, Alice) then performs measurement on her quantum cloning machine state vectors. After that she informs Bob about her measurement results using Goldenberg and Vaidman's quantum cryptographic scheme based on orthogonal states. Getting measurement results from Alice, an other partner (say, Bob) also performs measurements on his quantum cloning machine state vectors and using the same cryptographic scheme, he sends his measurement outcomes to Alice. Since the measurement results are interchanged secretly so Alice and Bob share secretly a four-qubit state. They again apply the cloning machine on one of their respective qubits and generate a six-qubit state $|\phi\rangle_{125346}$. Therefore, each party has three-qubit states. Among six-qubit states, we interestingly find that there exists two three-qubit states shared by Alice and Bob which are entangled for some values of the input parameter α^2.

In the second part, we investigate the problem of secret entanglement broadcasting among three distant parties. To solve this problem, we start with the result of the first part, i.e., we assume that the two distant partners (say, Alice and Bob) shared a three-qubit entangled state. Without any loss of generality, we assume that among three qubits, two are with Alice and one with Bob. Then Alice teleports one of the qubits to the third distant partner (say, Carol). After the completion of the teleportation procedure, we find that the three distant partners shared a three-qubit entangled state for the same values of the input parameters α^2 as in the first part of the protocol. In broadcasting of inseparability, we generally use the Peres-Horodecki criteria to show the inseparability of nonlocal outputs and separability of local outputs.

Peres-Horodecki theorem. [16,17]: the necessary and sufficient condition for the state $\hat{\rho}$ of two spins $\frac{1}{2}$ to be inseparable is that at least one of the eigenvalues of the partially transposed operator defined as $\rho^{T}_{m,\mu,n\nu}=\rho_{m\nu,n\mu}$ is negative. This is equivalent to the condition that at least one of the two determinants

$$W_3 = \begin{vmatrix} \rho_{00,00} & \rho_{01,00} & \rho_{00,10} \\ \rho_{00,01} & \rho_{01,01} & \rho_{00,11} \\ \rho_{10,00} & \rho_{11,00} & \rho_{10,10} \end{vmatrix} \quad \text{and}$$

$$W_4 = \begin{vmatrix} \rho_{00,00} & \rho_{01,00} & \rho_{00,10} & \rho_{01,10} \\ \rho_{00,01} & \rho_{01,01} & \rho_{00,11} & \rho_{01,11} \\ \rho_{10,00} & \rho_{11,00} & \rho_{10,10} & \rho_{11,10} \\ \rho_{10,01} & \rho_{11,01} & \rho_{10,11} & \rho_{11,11} \end{vmatrix}$$

is negative. For the security of the broadcasting of entanglement, we use Goldenberg *et al.* quantum cryptographic scheme which was based on orthogonal states [18]. The cryptographic scheme is described in Fig. 1.

All the previous works on the broadcasting of entanglement deals with the generation of two two-qubit entangled states starting from a two-qubit entangled state using either an optimal universal symmetric cloner [4,5] or a asymmetric cloner [19,20]. The generated two-qubit entangled state can be used as a quantum channel in quantum cryptography, quantum teleportation, etc. The advantage of our protocol over other protocols of broadcasting is that we are able to provide a protocol which generates a secret quantum channel between distant partners. The introduced protocol generates two three-qubit entangled states between two distant partners starting from a two-qubit entangled state and also provides the security of the generated quantum channel; not only that, we also generalize our protocol from two parties to three parties and show that the generated three-qubit entangled states can serve as a secured quantum channel between three distant parties. Now to hack the quantum information, hackers have to do two things: First, they have to gather knowledge about the initially shared entangled state and secondly, they have to collect information about the measurement results performed by two distant partners. These two tasks are very difficult to implement in our protocol by the third party Eve. Therefore, the quantum channel generated by our protocol is more secured and hence can be used in various protocols viz. quantum key distribution protocols [21,22].

We then distribute our work in the remaining three sections. In sec. II, we present our idea with a specific example for the broadcasting of a three-qubit entangled state shared between two distant partners. In Sec. III, we generalize this idea to generate a three-qubit entangled state shared between three distant parties. To implement the idea, we use the concept of entanglement swapping. The last section is devoted to the conclusion.

II. SECRETLY BROADCASTING OF A THREE-QUBIT ENTANGLED STATE BETWEEN TWO DISTANT PARTNERS

In this section, first we define broadcasting of three-qubit entanglement, open entanglement, and closed entanglement. Let the previously shared entangled state (1) described by the two-qubit density operator be ρ_{13}. Using a BH quantum cloning machine twice by the distant partners (Alice and Bob) on their respective qubits, they generate a total six-qubit state ρ_{125346} between them. Therefore, Alice has three qubits 1, 2, and 5 and Bob possesses three qubits 3, 4, and 6.

Definition 1. The three-qubit entanglement is said to be broadcast if (i) any of the two local outputs [say (ρ_{12},ρ_{15}) in Alice's side and (ρ_{34},ρ_{36}) in Bob's side] are separable and (ii) one local output (say, ρ_{25} in Alice's side and ρ_{46} in Bob's side) is inseparable and associated with these local inseparable output; two nonlocal outputs [say (ρ_{23},ρ_{35}) and (ρ_{14},ρ_{16})] are inseparable.

Definition 2. An entanglement is said to be closed if each party has nonlocal correlation with other parties. For instance, any three-particle entangled state described by the density operator ρ_{325} is closed if ρ_{32}, ρ_{25}, and ρ_{35} are entangled states. Otherwise, it is said to be an open entanglement (see Fig. 2).

Now we are in a position to discuss our protocol for the secretly broadcasting of a three-qubit entangled state. We start the protocol with a two-qubit entangled state $|\psi\rangle_{13}$ shared between two distant partners popularly known as Alice and Bob (see Fig. 3). Particles 1 and 3 are possessed by Alice and Bob, respectively. Alice and Bob then operate the quantum cloning machine on their respective qubits. After the cloning procedure, Alice performs a measurement on the quantum cloning machine state vector and sends the measurements results to Bob. After getting measurement results from Alice Bob performs measurements on his quantum cloning marine state vector and sends the measurement results to Alice. Consequently, the two distant partners share a four-qubit state $|\zeta\rangle_{1234}$. Now Alice has two qubits 1 and 2 and Bob 3 and 4, respectively. Both of them again operates the quantum cloning machine on one of the qubits that they possess. As a result, the distant parties now share a six-qubit state $|\phi\rangle_{125346}$ in which three qubits 1, 2, and 5 possessed by Alice and the remaining three qubits 3, 4, and 6 possessed by Bob. Now if there exists two three-qubit entangled states between two distant partners for some values of the input parameter α^2, then only we can secretly broadcast a three-qubit entangled state using only the universal quantum cloning machine. The word "secretly" is justified by observing an important fact that the transmission of measurement results from Alice to Bob and Bob to Alice has been done by using Goldenberg and Vaidman's quantum cryptographic scheme. Therefore, the messages regarding measurement results can be transmitted secretly between two distant partners. Hence, the broadcasted three-qubit entangled state is only known to Alice and Bob and not to the third party "Eve." As a result, these newly generated three-qubit entangled states can be used as a secret quantum channel in various quantum cryptographic scheme.

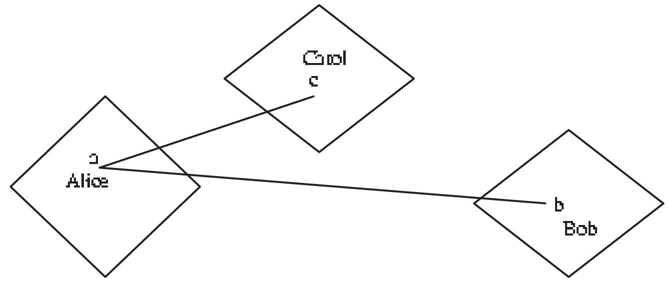

FIG. 2. In this figure, an open entanglement is shown. The entanglement is open in the sense that there is no direct entanglement between the qubits c and b.

Now to understand our protocol more clearly, we again discuss the whole protocol below by considering a specific example.

Step 1. Let the two-particle entangled state shared by two distant partners Alice and Bob be given by

$$|\psi\rangle_{13} = \alpha|00\rangle + \beta|11\rangle, \quad (3)$$

where α is real and β is complex with $\alpha^2+|\beta|^2=1$.

Step 2. The BH quantum copier is given by the transformation

FIG. 3. Alice and Bob initially share a two-particle entangled state $|\psi\rangle_{13}$.

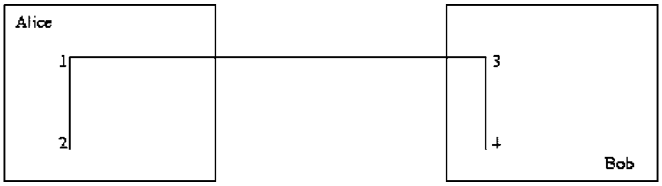

FIG. 4. Alice and Bob operate their local cloning machine on their respective qubits 1 and 3 to produce the copy qubits 2 and 4. Alice and Bob then perform measurements on the cloning machine state vectors and send their measurement results by using the cryptographic scheme shown in Fig. 1.

$$|0\rangle|\rangle|Q\rangle \to \sqrt{\tfrac{2}{3}}|00\rangle|Q_0\rangle + \frac{1}{\sqrt{3}}|\psi^+\rangle|Q_1\rangle, \tag{4}$$

$$|1\rangle|\rangle|Q\rangle \to \sqrt{\tfrac{2}{3}}|11\rangle|Q_1\rangle + \frac{1}{\sqrt{3}}|\psi^+\rangle|Q_0\rangle, \tag{5}$$

where $|\psi^+\rangle = 1/\sqrt{2}(|01\rangle + |10\rangle$ and $|Q_0\rangle$, $|Q_1\rangle$ are orthogonal quantum cloning machine state vectors.

Alice and Bob then operate the BH quantum cloning machine locally to copy the state of their respective particles (see Fig. 4). Therefore, after operating the quantum cloning machine, both Alice and Bob are able to approximately clone the state of the particle and consequently the combined system of four qubits is given by

$$\begin{aligned}|\chi\rangle_{1234} = {} & \Bigg[\left(\frac{2\alpha}{3}|0000\rangle + \frac{\beta}{3}|\psi^+\rangle|\psi^+\rangle\right)|Q_0\rangle^B + \left(\frac{\sqrt{2}\alpha}{3}|00\rangle|\psi^+\rangle\right. \\ & \left. + \frac{\sqrt{2}\beta}{3}|\psi^+\rangle|11\rangle\right) \quad |Q_1\rangle^B\Bigg]|Q_0\rangle^A \\ & + \Bigg[\left(\frac{\sqrt{2}\alpha}{3}|\psi^+\rangle|00\rangle + \frac{\sqrt{2}\beta}{3}|11\rangle|\psi^+\rangle\right)|Q_0\rangle^B \\ & + \left(\frac{\alpha}{3}|\psi^+\rangle|\psi^+\rangle + \frac{2\beta}{3}|1111\rangle\right)|Q_1\rangle^B\Bigg]|Q_1\rangle^A. \end{aligned} \tag{6}$$

The subscripts 1, 2, and 3, 4 refer to two approximate copy qubits in the Alice's and Bob's side, respectively. Also $|\rangle^A$ and $|\rangle^B$ denotes quantum cloning machine state vectors in Alice's and Bob's side, respectively.

Alice then performs measurements on the quantum cloning machine state vectors in the basis $\{|Q_0\rangle^A, |Q_1\rangle^A\}$. Thereafter, Alice informs Bob about her measurement results using Goldenberg and Vaidman's quantum cryptographic scheme based on orthogonal states which is discussed in the previous section. After getting measurement results from Alice, Bob also performs measurements on the quantum cloning machine state vectors in the basis $\{|Q_0\rangle^B, |Q_1\rangle^B\}$ and then using the same cryptographic scheme, he sends his measurement outcome to Alice. In this way Alice and Bob interchange their measurement results secretly.

Step 3. After measurements, let the state shared by Alice and Bob be given by

$$|\zeta_a\rangle_{1234} = \frac{1}{\sqrt{N}}\left[\frac{2\alpha}{3}|0000\rangle + \frac{\beta}{3}|\psi^+\rangle|\psi^+\rangle\right], \tag{7}$$

where $N = \frac{(3\alpha^2+1)}{9}$ represents the normalization factor.

Afterward, Alice and Bob again operate their respective cloners on the qubits 2 and 4, respectively, and therefore, the total state of six qubits is given by

$$\begin{aligned}|\phi\rangle_{125346} = {} & \frac{1}{\sqrt{N}}\Bigg[\frac{2\alpha}{3}\Bigg[|0\rangle_1 \otimes \left(\sqrt{\frac{2}{3}}|00\rangle|Q_0\rangle + \frac{1}{\sqrt{3}}|\psi^+\rangle|Q_1\rangle\right)_{25} \\ & \otimes |0\rangle_3 \otimes \left(\sqrt{\frac{2}{3}}|00\rangle|Q_0\rangle + \frac{1}{\sqrt{3}}|\psi^+\rangle|Q_1\rangle\right)_{46} \\ & + \frac{\beta}{6}\Bigg[|0\rangle_1 \otimes \left(\sqrt{\frac{2}{3}}|11\rangle|Q_1\rangle + \frac{1}{\sqrt{3}}|\psi^+\rangle|Q_0\rangle\right)_{25} \\ & \otimes |0\rangle_3 \otimes \left(\sqrt{\frac{2}{3}}|11\rangle|Q_1\rangle + \frac{1}{\sqrt{3}}|\psi^+\rangle|Q_0\rangle\right)_{46} + |0\rangle_1 \\ & \otimes \left(\sqrt{\frac{2}{3}}|11\rangle|Q_1\rangle + \frac{1}{\sqrt{3}}|\psi^+\rangle|Q_0\rangle\right)_{25} \otimes |1\rangle_3 \\ & \otimes \left(\sqrt{\frac{2}{3}}|00\rangle|Q_0\rangle + \frac{1}{\sqrt{3}}|\psi^+\rangle|Q_1\rangle\right)_{46} + |1\rangle_1 \\ & \otimes \left(\sqrt{\frac{2}{3}}|00\rangle|Q_0\rangle + \frac{1}{\sqrt{3}}|\psi^+\rangle|Q_1\rangle\right)_{25} \otimes |0\rangle_3 \\ & \otimes \left(\sqrt{\frac{2}{3}}|11\rangle|Q_1\rangle + \frac{1}{\sqrt{3}}|\psi^+\rangle|Q_0\rangle\right)_{46} + |1\rangle_1 \\ & \otimes \left(\sqrt{\frac{2}{3}}|00\rangle|Q_0\rangle + \frac{1}{\sqrt{3}}|\psi^+\rangle|Q_1\rangle\right)_{25} \otimes |1\rangle_3 \\ & \otimes \quad \left(\sqrt{\frac{2}{3}}|00\rangle|Q_0\rangle + \frac{1}{\sqrt{3}}|\psi^+\rangle|Q_1\rangle\right)_{46}\Bigg]. \end{aligned} \tag{8}$$

Now our task is to see whether we can generate two three-qubit entangled states from the above six-qubit state or not. To examine the above fact, we have to consider two three-qubit states described by the density operators ρ_{146} and ρ_{325}.

The density operator ρ_{146} is given by

$$\begin{aligned}\rho_{146} = {} & \frac{1}{N}\Bigg[\frac{4\alpha^2}{9}\left(\frac{2}{3}|000\rangle\langle 000| + \frac{1}{3}|0\psi^+\rangle\langle 0\psi^+|\right) \\ & + \frac{\alpha\beta^*}{9}\left(\frac{\sqrt{2}}{3}|000\rangle\langle 1\psi^+| + \frac{\sqrt{2}}{3}|0\psi^+\rangle\langle 111|\right) \\ & + \frac{\alpha\beta}{9}\left(\frac{\sqrt{2}}{3}|111\rangle\langle 0\psi^+| + \frac{\sqrt{2}}{3}|1\psi^+\rangle\langle 000|\right) \\ & + \frac{|\beta|^2}{36}\left(\frac{2}{3}|011\rangle\langle 011| + \frac{2}{3}|0\psi^+\rangle\langle 0\psi^+| + \frac{2}{3}|000\rangle\langle 000| \right. \\ & \left. + \frac{2}{3}|111\rangle\langle 111| + \frac{2}{3}|1\psi^+\rangle\langle 1\psi^+| + \frac{2}{3}|100\rangle\langle 100|\right)\Bigg]. \end{aligned} \tag{9}$$

The density operator ρ_{325} describes the other three-qubit state that looks exactly the same as ρ_{146}.

Now to show that the state described by the density operator ρ_{146} is entangled, we have to show that the two-qubit state described by the density operators ρ_{11}, ρ_{16}, and ρ_{46} is entangled, i.e., we have to show that there exist some values of the input state parameter α^2 for which the three-qubit state is a closed entangled state (see Fig. 5).

The reduced density operators ρ_{14}, ρ_{16}, and ρ_{46} are given by

$$\rho_{16}=\rho_{14}=\frac{1}{N}\left[\frac{4\alpha^2}{9}\left(\tfrac{5}{6}|00\rangle\langle 00|+\tfrac{1}{6}|01\rangle\langle 01|\right)+\frac{2\alpha\beta^*}{27}|00\rangle\langle 11|+\frac{2\alpha\beta}{27}|11\rangle\langle 00|+\frac{|\beta|^2}{36}(|00\rangle\langle 00|+|01\rangle\langle 01|+|10\rangle\langle 10|+|11\rangle\langle 11|)\right], \tag{10}$$

$$\rho_{46}=\frac{1}{N}\left[\frac{4\alpha^2}{9}\left[\tfrac{2}{3}|00\rangle\langle 00|+\tfrac{1}{6}(|01\rangle\langle 01|+|01\rangle\langle 10|+|10\rangle\langle 01|+|10\rangle\langle 10|)\right]+\frac{|\beta|^2}{36}\left[\tfrac{4}{3}|00\rangle\langle 00|+\tfrac{4}{3}|11\rangle\langle 11|+\tfrac{2}{3}(|01\rangle\langle 01|+|01\rangle\langle 10| + |10\rangle\langle 01|+|10\rangle\langle 10|)\right]\right]. \tag{11}$$

Now using the Peres-Horodecki theorem, we find that the state described by the density operators ρ_{16} and ρ_{14} are entangled if $0.18<\alpha^2<1$ and the state described by the density operator ρ_{46} is entangled if $0.61<\alpha^2<1$. Therefore, we can say that the state described by the density operator ρ_{146} is a closed three-qubit entangled state if $0.61<\alpha^2<1$. Similarly, the other reduced density operator ρ_{325} describes a closed entangled state if $0.61<\alpha^2<1$.

Also the other two-qubit state described by the density operators ρ_{12}, ρ_{15}, ρ_{34}, and ρ_{36} is given by

$$\begin{aligned}\rho_{12}=\rho_{15}=\rho_{34}=\rho_{36}=\frac{1}{N}\Bigg[&\frac{4\alpha^2}{9}\left(\tfrac{5}{6}|00\rangle\langle 00|+\tfrac{1}{6}|01\rangle\langle 01|\right)\\&+\frac{|\beta|^2}{36}\left(\tfrac{1}{3}|00\rangle\langle 00|+\tfrac{5}{3}|01\rangle\langle 01|+\tfrac{4}{3}|01\rangle\langle 10|+\tfrac{4}{3}|10\rangle\langle 01|\right.\\&\left.+\tfrac{5}{3}|10\rangle\langle 10|+\tfrac{1}{3}|11\rangle\langle 11|\right)\Bigg].\end{aligned} \tag{12}$$

These density operators are separable only when $0.27<\alpha^2<1$. Hence, broadcasting of a three-qubit entangled state is possible when $0.61<\alpha^2<1$.

Now, our task is to find out how is the entanglement distributed over the state, i.e., how much are the two-qubit density operators ρ_{16}, ρ_{14}, and ρ_{46} are entangled. To evaluate the amount of entanglement, we have to calculate the concurrence defined by Wootters [23] and hence entanglement of formation.

Wootters gave out, for the mixed state $\hat{\rho}$ of two qubits, the concurrence

$$C=\max(\lambda_1-\lambda_2-\lambda_3-\lambda_4,0), \tag{13}$$

where the λ_i, in decreasing order, are the square roots of the eigenvalues of the matrix $\rho^{\frac{1}{2}}(\sigma_y\otimes\sigma_y)\rho^*(\sigma_y\otimes\sigma_y)\rho^{\frac{1}{2}}$ and ρ^* denotes the complex conjugation of ρ in the computational basis $\{|00\rangle,|01\rangle,|10\rangle,|11\rangle\}$ and σ_y is the Pauli operator.

The entanglement of formation E_F can then be expressed as a function of C, namely

$$\begin{aligned}E_F=&-\frac{1+\sqrt{1-C^2}}{2}\log_2\frac{1+\sqrt{1-C^2}}{2}\\&-\frac{1-\sqrt{1-C^2}}{2}\log_2\frac{1-\sqrt{1-C^2}}{2}.\end{aligned} \tag{14}$$

After a little bit of calculation; we find that the concurrence and hence the entanglement of formation depends on the probability α^2. Therefore, we have to calculate the amount of entanglement in the two-qubit states described by the reduced density operators ρ_{16}, ρ_{14}, and ρ_{46} in the range $0.61<\alpha^2<1$ because the two-qubit reduced density operators are entangled in this range of the input state parameter α^2. Since concurrence depends on α^2 so it varies as α^2 varies. Therefore, when $0.61<\alpha^2<1$, the concurrences for the mixed states described by density operators ρ_{16}, ρ_{14} varies from 0.17 to 0.29 while the concurrence for the mixed states described by density operators ρ_{46} varies from 0.08 to 0.15, respectively. Using the relation (16) and the values of concurrence, we find that the entanglement of formation for the density operators ρ_{16}, ρ_{14}varies from 0.06 to 0.15 while the entanglement of formation for the density operator ρ_{46} varies from 0.01 to 0.03, respectively. Therefore, the generated three-qubit entangled state is a weak closed entangled state in the sense that the amount of entanglement in the two-qubit density operators are very low. Further, the above results show that the entanglement between qubits 1 and 6 (1 and 4) is higher than between the qubits 4 and 6.

Furthermore, if the measurement results are either $\sqrt{2}\alpha/3|00\rangle|\psi^+\rangle+\sqrt{2}\beta/3|\psi^+\rangle|11\rangle$ or $\sqrt{2}\alpha/3|\psi^+\rangle|00\rangle+\sqrt{2}\beta/3|11\rangle|\psi^+\rangle$, then the two three-qubit states described by the density operators ρ_{146} and ρ_{325} are different and the broadcasting is possible for $0.6<\alpha^2<1$ or $0.14<\alpha^2<0.4$ according to the outcomes. Also if the outcome of the mea-

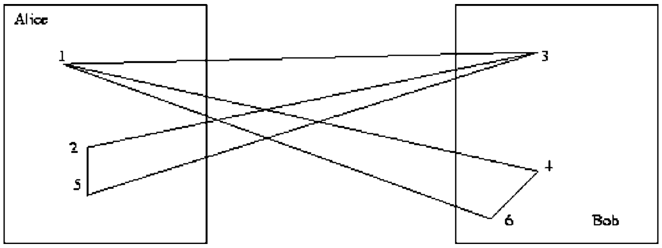

FIG. 5. Alice and Bob then again apply their cloning machine on one of their qubits to produce copy qubits 5 and 6, respectively. Finally we are able to broadcast two three-qubit entanglement between two distant partners Alice and Bob for some values of the parameter α^2.

surement is $\alpha/3|\psi^+\rangle|\psi^+\rangle+2\beta/3|1111\rangle$, then the state described by the density operators ρ_{146} and ρ_{325} are identical and the broadcasting is possible for $0.38<\alpha^2<0.73$.

III. SECRETLY GENERATION OF TWO THREE-QUBIT ENTANGLED STATES BETWEEN THREE DISTANT PARTNERS

In this section, we attempt to answer a question: can we secretly generate two three-qubit entangled states shared between three distant partners using LOCC? The answer is an affirmative. Now we show below that the three-qubit entangled state shared between three distant partners can be generated by a different process. To generate a three-qubit entangled state between three distant partners, we require only two well-known concepts: (i) quantum cloning and (ii) entanglement swapping.

Entanglement swapping [24,25] is a method that enables one to entangle two quantum systems that do not have direct interaction with one another. Bose *et al.* [24] generalized the procedure of entanglement swapping and obtained a scheme for manipulating entanglement in multiparticle systems. They showed that this scheme can be regarded as a method of generating entangled states of many particles. An explicit scheme that generalizes entanglement swapping to the case of generating a three-particle GHz state from three Bell pairs has been presented by Zukowski *et al.* [25]. The standard entanglement swapping helps to save a significant amount of time when one wants to supply two distant users with a pair of atoms or electrons (or any particle possessing mass) in a Bell state from some central source. The entanglement swapping can be used, with some probability which we quantify, to correct amplitude errors that might develop in maximally entangled states during propagation. In this work, we use the concept of entanglement swapping in the generation of a three-qubit entanglement between three distant partners. Now we are in a position to discuss the protocol for a secret generation of two three-qubit entangled states between three distant partners via quantum cloning and entanglement swapping.

Let us suppose for the implementation of any particular cryptographic scheme, three distant partners Alice, Bob, and Carol want to generate two three-qubit entangled states between them. To do the same task, let us assume that initially Alice-Bob and Carol-Alice share two-qubit entangled states described by the density operators ρ_{13}, ρ_{78}, where Alice has qubits 1 and 8, Bob and Carol possess qubits 3 and 7, respectively. Then Alice and Bob are adopting the broadcasting process described in the previous section to generate two three-qubit entangled states in between them. Therefore, Alice and Bob now have two three-qubit entangled states described by the density operators ρ_{146} and ρ_{325} where Alice has qubits 1, 2, and 5 and Bob possesses 3, 4, and 6. Now we are in a position for the illustration of the generation of a three-qubit entangled between three parties at distant places by using the concept of entanglement swapping.

Without any loss of generality, we take a three-qubit entangled state between two distant parties described by the density operator ρ_{325}. The density operator ρ_{325} can be rewritten as

$$\rho_{325}=\frac{1}{N}\Bigg[\frac{4\alpha^2}{9}\left(\tfrac{2}{3}|000\rangle\langle 001|+\tfrac{1}{3}|0\psi^+\rangle\langle 0\psi^+|\right)+\frac{\alpha\beta^*}{9}\left(\frac{\sqrt{2}}{3}|000\rangle\times\langle 1\psi^+|+\frac{\sqrt{2}}{3}|0\psi^+\rangle\langle 111|\right)+\frac{\alpha\beta}{9}\left(\frac{\sqrt{2}}{3}|111\rangle\langle 0\psi^+|+\frac{\sqrt{2}}{3}|1\psi^+\rangle\langle 000|\right)+\frac{|\beta|^2}{36}\left(\tfrac{2}{3}|011\rangle\langle 011|+\tfrac{2}{3}|0\psi^+\rangle\langle 0\psi^+|+\tfrac{2}{3}|000\rangle\langle 000|+\tfrac{2}{3}|111\rangle\langle 111|+\tfrac{2}{3}|1\psi^+\rangle\langle 1\psi^+|+\tfrac{2}{3}|100\rangle\times\langle 100|\right)\Bigg], \tag{15}$$

where qubits 2 and 5 are possessed by Alice and qubit 3 is possessed by Bob, respectively. To achieve the goal of the generation of a three-qubit entangled state between three distant partners, we proceed in the following way.

Let Alice and Carol share a singlet state

$$|\psi^-\rangle_{87}=\left(\frac{1}{\sqrt{2}}\right)(|01\rangle-|10\rangle), \tag{16}$$

where particles 8 and 7 are possessed by Alice and Carol, respectively.

The combined state between Alice, Bob, and Carol is given by the

$$\rho_{32587}=\rho_{325}\otimes|\psi^-\rangle_{78}\langle\psi^-|. \tag{17}$$

Alice then performs Bell state measurements on the particles 2 and 8 in the basis $\{|B_1^\pm\rangle,|B_2^\pm\rangle\}$, where $|B_1^\pm\rangle=(1/\sqrt{2})\times(|00\rangle\pm|11\rangle)$, $|B_2^\pm\rangle=(1/\sqrt{2})(|01\rangle\pm|10\rangle)$. If the measurement result is $|B_1^+\rangle$, then the three-qubit density operator is given by

$$\rho_{357}=\frac{1}{N}\Bigg[\frac{4\alpha^2}{9}\left[\tfrac{2}{3}|001\rangle\langle 001|+\tfrac{1}{6}(|011\rangle\langle 011|-|011\rangle\langle 000|-|000\rangle\langle 011|+|000\rangle\langle 000|)\right]+\frac{\alpha\beta^*}{27}(|001\rangle\langle 111|-|001\rangle\langle 100|+|000\rangle\langle 110|-|011\rangle\times\langle 110|)+\frac{\alpha\beta}{27}(-|110\rangle\langle 011|+|110\rangle\langle 000|+|111\rangle\langle 001|$$

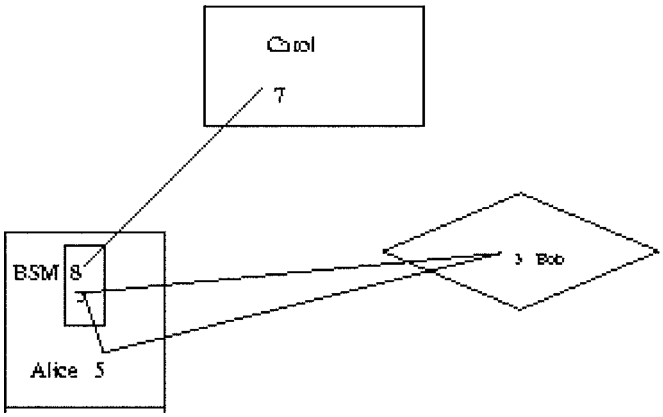

FIG. 6. Alice and Bob share a three-qubit entangled state described by the density operator ρ_{325}. Alice and Carol share a singlet state described by the density operator $\rho_{78}=|\psi^{-}\rangle_{78}\langle\psi^{-}|$. Then Alice performs Bell-state measurements (BSM) on particles 2 and 8 of the joint state described by the density operator $\rho_{325}\otimes\rho_{78}$.

$$-|100\rangle\langle 001|) + \frac{|\beta|^2}{36}\Big[\tfrac{2}{3}(|010\rangle\langle 010| + |001\rangle\langle 001| + |110\rangle \times\langle\times\times 110| + |101\rangle\langle 101|) + \tfrac{1}{3}(|011\rangle\langle 011| - |011\rangle\langle 000| - |000\rangle\langle 011| + |000\rangle\langle 000| + |111\rangle\langle 111| - |111\rangle\langle 100| - |100\rangle\langle 111| + |100\rangle\langle 100|)\Big]. \quad (18)$$

After the Bell-state measurement, Alice announces publicly the measurement result. Thereafter, Alice, Bob, and Carol operate a unitary operator $U_1=I_3\otimes(\sigma_z)_5(\sigma_x)_7$ on their respective particles to retrieve the state described by the density operator ρ_{325}.

If the measurement result is $|B_1^{-}\rangle$ or $|B_2^{+}\rangle$ or $|B_2^{-}\rangle$ then accordingly they operate an unitary operator $U_2=I_3\otimes(I_5)\otimes(\sigma_x)_7$ or $U_3=I_3\otimes(I_5)\otimes(\sigma_z)_7$ or $U_4=I_3\otimes(I_3)\otimes(I_7)$ on their respective particles to retrieve the state described by the density operator ρ_{325}. Hence, we find that after getting the measurement results, each party (Alice, Bob, and Carol) applies the suitable unitary operator on their respective particles to share the three-qubit entangled state in between them, which is previously shared between only two distant partners Alice and Bob.

Also we note an important fact that the generated three-qubit entangled state is totally secret between three distant partners because the outcome of the measurement on the machine state vector is totally unknown to the eavesdropper. Furthermore, the reduced density operator describing a three-qubit state between two distant partners and the reduced density operator describing a three-qubit state between three distant partners are entangled for the same range of α^2. The above protocol is described pictorially in Figs. 6 and 7.

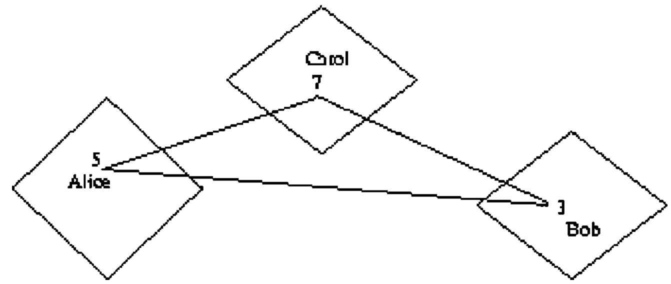

FIG. 7. Finally, after applying suitable unitary operators, a three-qubit entangled state described by the density operator ρ_{325} is generated between three distant partners Alice, Carol, and Bob.

Therefore, in this section we describe the secretly generation of a three-qubit entangled state between three distant partners starting from a three-qubit entangled state shared between two distant partners using quantum cloning and entanglement swapping. This quantum channel generated by the above procedures can be regarded as a secret quantum channel because the result of the measurement on the machine state vectors transmitted secretly by the quantum cryptographic scheme.

IV. CONCLUSION

In this work, we present a protocol for the secret broadcasting of a three-qubit entangled state between two distant partners. Here we should note an important fact that the two copies of a three-qubit entangled state is not generated from a previously shared three-qubit entangled state but from a previously shared two-qubit entangled state using the quantum cloning machine. They send their measurement results secretly using the cryptographic scheme so that the produced copies of the three-qubit entangled state shared between two distant parties can serve as a secret quantum channel. We also extend this idea to create the three-particle entangled state secretly between three distant partners using quantum cloning and the entanglement swapping procedure.

ACKNOWLEDGMENTS

S.A wishes to acknowledge the support given by CSIR Project F.No.8/3(38)/2003-EMR-1, New Delhi. S.A would like to thank Samir Kunkri for useful discussion with him.

[1] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982).
[2] A. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[3] L. M. Duan and G. C. Guo, Phys. Rev. Lett. **80**, 4999 (1998).
[4] V. Buzek and M. Hillery, Phys. Rev. A **54**, 1844 (1996).
[5] D. Bruss, P. D. DiVincenzo, A. Ekert, C. A. Fuchs, C. Macchiavello, and J. A. Smolin, Phys. Rev. A **57**, 2368 (1998).
[6] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).
[7] C. H. Bennett and G. Brassard, *Proceedings of the IEEE International Conference on Computers, System and Signal Pro-*

cessing, Bangalore, India, (IEEE, New York, 1984), pp. 175–179.
[8] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[9] C. H. Bennett and S. J. Weisner, Phys. Rev. Lett. **69**, 2881 (1992).
[10] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1985 (1993).
[11] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, Phys. Rev. A **53**, 2046 (1996); D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).
[12] V. Buzek, V. Vedral, M. B. Plenio, P. L. Knight, and M. Hillery, Phys. Rev. A **55**, 3327 (1997).
[13] S. Bandyopadhyay and G. Kar, Phys. Rev. A **60**, 3296 (1999).
[14] H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, and B. Schumacher, Phys. Rev. Lett. **76**, 2818 (1996).
[15] I. Ghiu, Phys. Rev. A **67**, 012323 (2003).
[16] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).
[17] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).
[18] L. Goldenberg and L. Vaidman, Phys. Rev. Lett. **75**, 1239 (1995).
[19] N. J. Cerf, Phys. Rev. Lett. **84**, 4497 (2000).
[20] N. J. Cerf, J. Mod. Opt. **47**, 187 (2000).
[21] A. Cabello, Phys. Rev. A **61**, 052312 (2000).
[22] C. Li, H.-S. Song, and L. Zhou, J. Opt. B: Quantum Semiclassical Opt. **5**, 155 (2003).
[23] W. K. Wootters, Phys. Rev. Lett. **80**, 2245 (1998).
[24] S. Bose, V. Vedral, and P. L. Knight, Phys. Rev. A **57**, 822 (1998).
[25] M. Zukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, Phys. Rev. Lett. **71**, 4287 (1993).