Multiparticle entanglement and its applications to cryptography

Julia Kempe*
Department of Mathematics, University of California at Berkeley, Berkeley, California and École Nationale Superieure des Télécommunications, Paris, France
(Received 18 February 1999)

Entanglement between three or more parties exhibits a realm of properties unknown to two-party states. Bipartite states are easily classified using the *Schmidt decomposition*. The Schmidt coefficients of a bipartite pure state encompass all the nonlocal properties of the state and can be ''seen'' by looking at one party's density matrix only. Pure states of three and more parties, however, lack such a simple form. They have more invariants under local unitary transformations than any one party can ''see'' on their subsystem. These ''hidden nonlocalities'' will allow us to exhibit a class of multipartite states that cannot be distinguished from each other by any party. Generalizing a result of Bennett, Popescu, Rohrlich, Smolin, and Thapliyal, and using a recent result by Nielsen, we will show that these states cannot be transformed into each other by local actions and classical communication. Furthermore, we will use an orthogonal subset of such states to hint at applications to cryptography and illustrate an extension to quantum secret sharing [using recently suggested $((n,k))$-threshold schemes]. [S1050-2947(99)01408-0]

PACS number(s): 03.67.−a, 03.65.−w

I. INTRODUCTION

The entanglement properties of *bipartite pure states* have already been treated extensively. The analysis of entanglement and its properties for these states is much easier than for three or more party-shared states due to a particularly convenient form that captures all nonlocal parameters: the (unique) *Schmidt decomposition* [1].

An interesting question which arises in attempts to classify entanglement is which states can be obtained from a given state if we allow *local actions and classical communication* of the parties. By classical communication we mean an *a priori* unlimited amount of two-way classical communications. We will call these transformations of a k-party state k-LOCC (k-party local operations and classical communication). The crucial difference between pure local unitary action and LOCC is that each party may perform (generalized) measurements on its subsystem and broadcast the outcomes via classical channels between the parties. The other parties may choose their subsequent actions conditional on the outcomes of these measurements.

For *bipartite* pure states, Nielsen [2] has recently found necessary and sufficient conditions for the process of entanglement transformation via 2-LOCC to be possible. A key tool in this result is the Schmidt decomposition of bipartite states and the conditions involve the Schmidt coefficients of the states only.

So once we are given the density matrix of one party, a bipartite pure state no longer contains any secrets: The eigenvalues of one party's density matrix completely characterize the state (up to equivalence under local unitary operations) and give us complete knowledge about its entanglement transformation properties under local operations and classical communication between the parties. In other words, given a sufficient supply of copies of a certain state shared by two parties, each of the parties is able to determine (up to a certain precision) its equivalence class under local unitaries *and* which other states it can be transformed into via 2-LOCC.

The situation is drastically different for *multipartite* states involving more than two parties. No convenient (locally invariant) form—analogous to the Schmidt decomposition—can be given. The number of invariants of a state under local unitaries grows exponentially with the number of parties (see Sec. II). Attempts to find canonical points on the orbits of multipartite states have been made [3], but yield unwieldy outcomes. We will say that two multiparty states are *unitarily equivalent* ($|\Psi\rangle \sim |\Phi\rangle$) if they can be transformed into each other by local (single-party) unitary operations only (without classical communication). Linden and Popescu [4] have given a lower bound on the number of parameters needed to describe equivalence classes of multipartite states. To parametrize inequivalent states, they also exhibited an explicit polynomial form for invariants of a multipartite state under local unitaries (see Sec. III B). Some of these invariants are functions of the eigenvalues of the local density matrices of all parties. For three (and more) parties, however, the number of independent invariants under local unitaries is bigger than the number of independent eigenvalues of all local-density matrices. This means that if we get all possible information from each party's subsystem, there will be invariants under local unitaries that we cannot determine. We will call these parameters *hidden nonlocalities* of our quantum state. Complete knowledge of each local system thus does not give us complete information on the equivalence class of the multipartite state under local unitary operations.

Let us review Nielsen's result to make the difference between bipartite and multipartite states more precise: For bipartite pure states and 2-LOCC, there is a partial ordering on the states that characterizes their mutual entanglement transformation properties [2]:

*Visiting the California Institute of Technology, Pasadena, CA. Electronic address: kempe@math.berkeley.edu

$$|\Psi\rangle \overset{\text{2-LOCC}}{\rightarrow} |\Phi\rangle \text{ iff } \rho_A^\Psi \prec \rho_A^\Phi, \tag{1}$$

where ρ_A is the density matrix of one party and $\rho_A^\Psi \prec \rho_A^\Phi$ means that the eigenvalues $\lambda_1^\Psi, \ldots, \lambda_k^\Psi$ of ρ_A^Ψ are majorized by the eigenvalues $\lambda_1^\Phi, \ldots, \lambda_k^\Phi$ of ρ_A^Φ, i.e.,

$$\sum_{i=1}^{k} \lambda_i^{\Psi\downarrow} \leqslant \sum_{i=1}^{k} \lambda_i^{\Phi\downarrow}, \quad \forall k. \tag{2}$$

The arrow indicates that the eigenvalues have to be put into decreasing order.

This gives a partial ordering in the space of all nonlocal parameters of bipartite states (remember that the nonlocal parameters are the independent eigenvalues of the density matrix of one party). In the case of just two qubits shared by two parties, this even gives a *total ordering* on the states, meaning that given two states either the first can be transformed into the second or vice versa (there is only one independent Schmidt coefficient). Among *higher dimensional bipartite states*, however, we also find sets of states that cannot be transformed into each other either way by LOCC. These states have been termed *incommensurate*. The smallest system to provide us with two bipartite incommensurate pure states is the nine-dimensional space of two *qutrits* [2]. Also note that the commensurateness or incommensurateness of two bipartite states can be immediately identified by looking at the density matrix of one subsystem.

Two bipartite pure states whose one-party density matrices have the same eigenvalues are *always* mutually obtainable from each other via 2-LOCC. Also

$$\frac{1}{n} I \prec \rho_A^\Phi, \quad \forall |\Phi\rangle \tag{3}$$

implies that starting with an Einstein-Podolsky-Rosen (EPR)-type bipartite state (unique up to local unitaries with the property that its density matrix obtained by tracing out one party is proportional to the identity matrix), we can extract *every* given bipartite state $|\Phi\rangle$ with local operations and classical communication. The partially ordered set of states under 2-LOCC has just *one* maximal state (up to unitary equivalence).

We will show that this structure is very different for *multipartite states*. Bennett, Popescu, Rohrlich, Smolin, and Thapliyal (BPRST) [5,6] have found two three-party states—each party having two qubits—of dimension 2^6 that are incommensurate, although all of their subdensity matrices are identical. Following their argument, we will use Nielsen's result (1) to generalize their proof and show that even for the smallest three-partite state (of dimension 8) there are incommensurate states that have *identical or similar* local-density matrices. Their incommensurateness cannot be ''seen'' by looking at subsystems of the state (it is *hidden*). We connect *hidden nonlocalities* to *hidden incommensurateness* to see that two multipartite states with similar density matrices on each party are incommensurate if and only if they are not unitarily equivalent.

We give some examples of *locally equivalent k*-LOCC *incommensurate states*. We will suggest how to ''encode into hidden nonlocalities'' with the help of an orthogonal subset of such states. These states have the property that they are totally indistinguishable from each other for each party alone and cannot be transformed into each other by local operations and classical communication between the parties. Furthermore, we can find a set of such states that are *maximal* in the sense that they cannot be obtained from any other (unitarily not equivalent) state by *k*-LOCC. Only if the parties perform a collective (orthogonal) measurement will they be able to (perfectly) distinguish these states. This area needs further exploration.

We will analyze a recently suggested cryptographic protocol [7] for *quantum secret sharing* to identify a class of incommensurate and locally equivalent states in them. An $((n,k))$ threshold scheme $(k<n)$ is a method to encode and divide a secret quantum state between n parties such that from any k shares the state can be perfectly recovered and from any $k-1$ or fewer shares no information whatsoever about the state can be inferred.

The scheme as introduced in [7] assumes that all parties are honest when they participate in reconstructing the secret. Allowing for the possibility of some parties being dishonest in order to retrieve the secret alone, we will show how the scheme can be ''misused'' for cheating by one party if it is used to encode a ''classical'' bit and how this cheating can be prevented by using incommensurate locally identical states.

II. COUNTING HIDDEN NONLOCALITIES

Linden and Popescu [4] have classified the orbits of multipartite states under local unitary operations and determined the dimension of generic orbits and the number of parameters needed to describe the location of such an orbit in Hilbert space.

In the case of k parties each having one spin-$\frac{1}{2}$ particle (qubit), there are at least $2^{k+1}-2-3k$ real parameters that characterize nonlocal properties. [Initially each 2^k-dimensional state has 2^k complex parameters and the requirement of unit norm leaves $2^{k+1}-1$ real parameters. The group of equivalence transformations is $U(1)\times SU(2)\times SU(2)\times\cdots\times SU(2)$—each local unitary $U(2)\simeq U(1)\times SU(2)$ but each local phase can be factored out to one single global phase. The group (and the generic orbit) then has dimension $3k+1$ or less.]

Furthermore, an explicit form for polynomial invariants of an orbit has been given [4] (see Sec. III B). To get a picture of how the number of *hidden nonlocalities* grows, let us analyze the three-, four-, and five-party cases. We can easily count parameters in the three-party spin-$\frac{1}{2}$ case: We have five (independent) nonlocal parameters but only three (in general) different density matrices each characterized by one eigenvalue. So there are two nonlocal parameters that we cannot ''see'' by only looking at various subsystems of our entangled state. Now let us look at the four-party spin-$\frac{1}{2}$ case. Here we have at least 18 nonlocal parameters but at most seven independent subdensity matrices where two density matrices are *independent* if the eigenvalues of the first do not completely determine the eigenvalues of the second. The four one-party matrices each have one nonlocal parameter and the three independent density matrices of two joint parties have at most three parameters each thus leaving a total of at least $18-4*1-3*3=5$ hidden nonlocalities. Of

the 18 nonlocal parameters, 14 cannot be seen by only one party alone; they are *hidden* if we look at one-party subsystems only. For the five-party case, the number of nonlocal parameters that cannot be seen by looking only at each party locally is $\leqslant 58$. There are at least 18 nonlocal parameters that cannot be accessed by looking at any one- and two-party subdensity matrices of the system.

In general, the number of *hidden nonlocalities* grows exponentially with the number of parties.

III. CLASS OF 3-LOCC INCOMMENSURATE STATES

We now want to show that there are 3-LOCC incommensurate states for the three-spin-$\frac{1}{2}$ system. There are five independent invariants under local unitaries; three of them are of the form $\mathrm{tr}\,\rho_p^2$ $(p=A,B,C)$ and completely characterize the eigenvalues of ρ_p (see Sec. III B). Suppose that we have two states $|\Psi\rangle$ and $|\Phi\rangle$ that differ only in the last two *hidden* invariants, i.e., the three one-party density matrices of $|\Psi\rangle$ and $|\Phi\rangle$ have the same eigenvalues. For ease of argument, choose them such that ρ_A, ρ_B, and ρ_C have full rank 2.

Claim. $|\Psi\rangle$ and $|\Phi\rangle$ are 3-LOCC incommensurate.

Proof. What does a general 3-LOCC protocol look like? First one party, say Alice, will perform a generalized measurement and broadcast her outcome. Then Bob and Charlie will continue with generalized measurements on their subsystems conditional on Alice's outcome and broadcast their outcomes. At a certain point, Alice will continue, and so on. Let us for a moment (mentally) merge Bob's and Charlie's systems and look at the 3-LOCC protocol as a protocol between the systems A and BC. Everything that Bob and Charlie do after receiving Alice's outcome and before Alice's next action can be viewed as a generalized measurement on the BC subsystem. So the whole 3-LOCC protocol can be viewed as a specific case of a 2-LOCC protocol between A and BC. In particular, this means that if $|\Psi\rangle$ could be transformed into $|\Phi\rangle$ via 3-LOCC, it certainly could be transformed into $|\Phi\rangle$ via 2-LOCC on A and BC.

Assume there was a 3-LOCC protocol that transforms $|\Phi\rangle$ to $|\Psi\rangle$. We have chosen the states such that

$$\rho_A^{\Psi}\sim\rho_A^{\Phi}\sim\begin{pmatrix}\cos^2\alpha & 0\\ 0 & \sin^2\alpha\end{pmatrix}. \tag{4}$$

Let $|v_A\rangle$ and $|v_A^{\perp}\rangle$ be the two eigenvectors of ρ_A^{Ψ} and rewrite

$$|\Psi\rangle=\cos\alpha|v_A\rangle|v_{BC}\rangle+\sin\alpha|v_A^{\perp}\rangle|v_{BC}^{\perp}\rangle. \tag{5}$$

This is the Schmidt decomposition of $|\Psi\rangle$ as a bipartite A-BC state. In particular, $|v_{BC}\rangle$ and $|v_{BC}^{\perp}\rangle$ are orthogonal in the joint BC-Hilbert space. Alice performs the first generalized measurement $M=\{M_1,M_2,\ldots\}$ (with $\Sigma_i M_i^{\dagger}M_i=I$) and obtains the outcome i. Hereby she transforms the state $|\Psi\rangle$ to a state $|\Psi'\rangle$ with

$$|\Psi'\rangle=\frac{1}{N}[\cos\ \alpha(M_i|v_A\rangle)|v_{BC}\rangle+\sin\alpha(M_i|v_A^{\perp}\rangle)|v_{BC}^{\perp}\rangle]. \tag{6}$$

(N is the normalization factor.)

From here Bob and Charlie will continue $|\Psi'\rangle \xrightarrow[\text{on A,BC}]{3-\text{LOCC}} |\Phi\rangle$ so in particular we know that $|\Psi'\rangle \xrightarrow{2-\text{LOCC}} |\Phi\rangle$. From

$$|\Psi\rangle \xrightarrow{2-\text{LOCC}} |\Psi'\rangle \xrightarrow{2-\text{LOCC}} |\Phi\rangle. \tag{7}$$

Nielsen's criterion (1) tells us

$$\rho_A^{\Psi}\prec\rho_A^{\Psi'}\prec\rho_A^{\Phi}\sim\rho_A^{\Psi}, \tag{8}$$

so $\rho_A^{\Psi}=\cos^2\alpha|v\rangle\langle v|+\sin^2\alpha|v^{\perp}\rangle\langle v^{\perp}|$ has to have the same eigenvalues as

$$\begin{aligned}\rho_A^{\Psi'}&=\frac{1}{N^2}(\cos^2\alpha M_i|v\rangle\langle v|M_i^{\dagger}+\sin^2\alpha M_i|v^{\perp}\rangle\langle v^{\perp}|M_i^{\dagger})\\&=\frac{M_i}{N}\rho_A^{\Psi}\frac{M_i^{\dagger}}{N}.\end{aligned} \tag{9}$$

This implies that there is a unitary transformation U such that

$$U^{\dagger}\rho_A^{\Psi}U=\frac{M_i}{N}\rho_A^{\Psi}\left(\frac{M_i}{N}\right)^{\dagger}. \tag{10}$$

It follows that $U(M_i/N)$ has to be unitary and diagonal in the same basis as ρ_A^{Ψ} (just pick a basis where ρ_A^{Ψ} is diagonal and write out the matrix elements in their most general form using that ρ_A^{Ψ} has full rank). We see that $M_i|v_A\rangle$ and $M_i|v_A^{\perp}\rangle$ have to be orthogonal and that Alice's generalized measurement reduces to a local unitary operation on her qubit.

Continuing this argument for each subsequent step of the 3-LOCC protocol it follows that the whole protocol ends up to be a succession of local unitaries. But we have chosen our states to be nonequivalent under local unitaries. This completes the proof.

Note that the constraint to full-rank local-density matrices can be lifted if we only look at the restriction of M_i onto the support of ρ_A, ρ_B, ρ_C. We have thus shown that even in the simplest three-party case there are states that—having the same eigenvalues of all subdensity matrices—are 3-LOCC-incommensurate. Furthermore, once we fix the eigenvalues of ρ_A, ρ_B, ρ_C, we have two additional parameters to specify different classes of 3-LOCC-incommensurate states. In the five-dimensional space of unitarily nonequivalent states, we have found a two-dimensional subspace of mutually incommensurate states.

This proof generalizes trivially to more than two dimensions of each party's Hilbert space and to $k\geqslant 3$ parties. To see the latter, we note that at each step of a k-LOCC protocol we can divide the system into two parts—one party that performs a local operation and the other $k-1$ parties—and apply Nielsen's criterion as in the three-party case.

It follows from our proof that throughout each step of a k-LOCC transformation protocol each party's density matrices of the state obtained at a particular step have to majorize the corresponding density matrices of all states at previous steps. In particular, we have the following.

Corollary 1. If, say, Alice's density matrix at the beginning and at the end of a k-LOCC protocol are similar, then Alice's action is restricted to local unitaries.

Corollary 2. Two k-partite states $|\Psi\rangle$ and $|\Phi\rangle$ that have similar density matrices ($\rho_p^\Psi \sim \rho_p^\Phi$, $p=A,B,\ldots$) on each party's subsystem are k-LOCC *incommensurate* if and only if they are *not unitarily equivalent*. After having proved the existence of 3-LOCC incommensurate states, let us give some specific examples.

A. The 2-GHZ–3-EPR example

BPRST [5,6] originally showed that the following three-partite states are incommensurate:

$$\text{2-GHZ}=\frac{(|0_{A1}0_{B1}0_{C1}\rangle+|1_{A1}1_{B1}1_{C1}\rangle)}{\sqrt{2}} \otimes \frac{(|0_{A2}0_{B2}0_{C2}\rangle+|1_{A2}1_{B2}1_{C2}\rangle)}{\sqrt{2}} \tag{11}$$

and

$$\text{3-EPR}=\frac{(|0_{A1}0_{B1}\rangle+|1_{A1}1_{B1}\rangle)}{\sqrt{2}}\otimes\frac{(|0_{A2}0_{C1}\rangle+|1_{A2}1_{C1}\rangle)}{\sqrt{2}} \otimes \frac{(|0_{B2}0_{C2}\rangle+|1_{B2}1_{C2}\rangle)}{\sqrt{2}}. \tag{12}$$

In the 3-EPR state, the three parties Alice, Bob, and Charlie share three EPR pairs, one between A and B, one between A and C, and one between B and C. In the 2 Greenberger-Horne-Zeilinger (2GHZ) state, they share just share two GHZ states. In both cases the density matrices of Alice, Bob, and Charlie are identical:

$$\rho=\frac{1}{4}I. \tag{13}$$

So in any 3-LOCC transformation protocol from 2-GHZ to 3-EPR and vice versa, Alice, Bob, and Charlie are restricted to local unitaries. It is, however, impossible to transform 2-GHZ to 3-EPR via local unitaries. One simple way to see this is to observe that 2-GHZ is a triseparable state—it gives separable density matrices when tracing out any one party—whereas 3EPR is not triseparable. (Tracing out A in 3-EPR gives $\frac{1}{4}I\otimes|\text{EPR}_{B2C2}\rangle\langle\text{EPR}_{B2C2}|$, which is obviously not separable.)

Note that this proof generalizes trivially to k-partite states and k-LOCC: $(k-1)$GHZ and $\binom{k}{2}$EPR *are* k-LOCC *incommensurate*.

B. Two locally nondistinguishable 3-LOCC incommensurate states of dimension 8

Note that the smallest bipartite system that contains two incommensurate states has to have dimension 9 at least with each party possessing a qutrit. This is because two density matrices that are not majorized either way have to have rank 3 at least. But even for the smallest three-partite system of dimension 8, there are incommensurate states. We can find states with identical local-density matrices that cannot be transformed into each other via 3-LOCC. To keep calculations easier, we looked for particularly simple states of the following form:

$$|\Psi\rangle=\alpha_+|000\rangle+\alpha_-|vvv\rangle, \tag{14}$$

where $|v\rangle$ is a normalized state. The equivalence classes of these states are characterized by two parameters—say $\alpha_+\alpha_+^*$ and $|\langle 0|v\rangle|$—and have equivalent density matrices on all three subparties. So from the five independent invariants of (generic) states under local unitary transforms, in this case only (at most) two are algebraically independent.

Let us look at the invariants in the general case for states of the form $|\Psi\rangle=\Sigma_{i,j,k}\alpha_{ijk}|e_ie_je_k\rangle$. From the coefficients α_{ijk} we can form polynomials that are manifestly invariant under local unitaries, like the degree 2 polynomial:

$$I_1=\sum_{ijk}\alpha_{ijk}\alpha_{ijk}^*, \tag{15}$$

which is the norm of the state. To fourth degree we get three polynomials:

$$I_2=\sum_{ijkmpq}\alpha_{kij}\alpha_{mij}^*\alpha_{mpq}\alpha_{kpq}^*=\text{tr}\,\rho_A^2,$$

$$I_3=\sum_{ijkmpq}\alpha_{ikj}\alpha_{imj}^*\alpha_{pmq}\alpha_{pkq}^*=\text{tr}\,\rho_B^2, \tag{16}$$

$$I_4=\sum_{ijkmpq}\alpha_{ijk}\alpha_{ijm}^*\alpha_{pqm}\alpha_{pqk}^*=\text{tr}\,\rho_C^2,$$

which in general are algebraically independent. One of the higher degree invariants is

$$I_5=\sum_{ijklmnopq}\alpha_{ijk}\alpha_{ilm}^*\alpha_{nlo}\alpha_{pjo}^*\alpha_{pqm}\alpha_{nqk}^*, \tag{17}$$

which in general is not algebraically dependent of I_2, I_3, I_4. For the simple state in Eq. (14), we have $I_2=I_3=I_4$, and a symbolic calculation (Groebner basis) shows that I_5 and I_2 are algebraically independent. We now exhibit two states of the above simple form (14) which have similar one-party density matrices (and the same I_2) but different I_5, thus being 3-LOCC *incommensurate*:

$$|\Psi\rangle=2\sqrt{\frac{3}{37}}|000\rangle-\frac{5}{\sqrt{37}}|111\rangle \tag{18}$$

and

$$|\Phi\rangle=4\sqrt{\frac{2}{37}}|000\rangle-\frac{5}{\sqrt{37}}|vvv\rangle, \tag{19}$$

where $|v\rangle=(|0\rangle+|1\rangle)/\sqrt{2}$ is the state $|1\rangle$ rotated by 45°,

$$I_2^\Psi=I_2^\Phi=\frac{769}{1369} \tag{20}$$

and

$$I_5^{\Psi} \approx 0.343 \neq I_5^{\Phi} \approx 0.242. \tag{21}$$

So these two states are 3-LOCC incommensurate. We can apply a local unitary transformation on each subsystem to one of the states to make their density matrices diagonal in the same basis so that they are completely indistinguishable for each party.

C. The ((3,2))-threshold states

In a recent paper [7], an encoding of a *qutrit* into a tripartite state has been given (see Sec. IV A). The encoded state is of the following form:

$$|\Phi(\alpha,\beta,\gamma)\rangle = \alpha(|000\rangle + |111\rangle + |222\rangle) + \beta(|012\rangle + |120\rangle + |201\rangle) + \gamma(|021\rangle + |102\rangle + |210\rangle). \tag{22}$$

The density matrix of any one party is proportional to the identity matrix. So all of these states have the same one-party density matrices. Most of these states will differ in the hidden nonlocalities and be 3-LOCC incommensurate. Here we will give a set of three locally indistinguishable *orthogonal* states of the above form:

$$|\Phi_1\rangle = |\Phi(1,0,0)\rangle = (|000\rangle + |111\rangle + |222\rangle),$$

$$|\Phi_2\rangle = \left|\Phi\left(0,\frac{1}{\sqrt{2}},\frac{1}{\sqrt{2}}\right)\right\rangle = \frac{1}{\sqrt{2}}(|012\rangle + |120\rangle + |201\rangle) + \frac{1}{\sqrt{2}}(|021\rangle + |102\rangle + |210\rangle), \tag{23}$$

$$|\Phi_3\rangle = \left|\Phi\left(0,\frac{1}{\sqrt{2}},-\frac{1}{\sqrt{2}}\right)\right\rangle = \frac{1}{\sqrt{2}}(|012\rangle + |120\rangle + |201\rangle) - \frac{1}{\sqrt{2}}(|021\rangle + |102\rangle + |210\rangle).$$

These states differ in the value of I_5 (17), which takes on $\frac{1}{9}$, $\frac{1}{18}$, and 0 for the three states, respectively. They are thus 3-LOCC incommensurate.

IV. CRYPTOGRAPHY—ENCODING INTO HIDDEN NONLOCALITIES

We have exhibited states that cannot be transformed into each other by local operations and classical communication involving three parties and shown that there is a large number of them. We think that these states can have a fruitful application in (quantum)-cryptographic protocols like three-party quantum bit commitment schemes. We can produce states that for each subsystem are indistinguishable and yet have some hidden nonlocal property that makes them different.

How could we *encode information into the hidden nonlocalities* and how can we access them? One possibility is to find *orthogonal states* that have the same respective subparty density matrices and differ only in these hidden parameters. Encode a bit-string into each of those and give a part of the corresponding state to the three parties, *A*, *B*, and *C*, without telling them which specific state they share. While the parties are locally separated and only allowed to perform local actions and classical communication they have no way to transform the states into each other. Only when they get together (or send their share of the state through a quantum channel) can they perform an orthogonal measurement and determine the encoded bitstring. To ensure that there is no common state Ω from which *two different* states can be obtained via *k*-LOCC, we can choose states with local-density matrices proportional to the identity. Since the identity matrix on a subsystem majorizes every other density matrix, ρ_A^{Ω} would have to be proportional to the identity as well. We have shown that in this case each party is restricted to local unitaries in their attempt to change the state via LOCC.

Another example of two tripartite states [apart from Eq. (23)] that *have identical one-party density matrices, are 3-*LOCC*-incommensurate, and orthogonal* is the actual 2GHZ-3EPR example from Sec. III A if we use the singlet state

$$\mathrm{EPR}' = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \tag{24}$$

instead of the EPR states. 3EPR′ and 2GHZ are 3-LOCC incommensurate and orthogonal.

A detailed analysis of some cryptographic schemes for the potential use of incommensurate states should be done. Here we will restrict ourselves to a rather illustrative example involving quantum secret sharing.

A. How Bob can cheat using the ((3,2)) threshold scheme and how to prevent that

The ((3,2)) threshold scheme in [7] encodes a qutrit

$$|\Psi\rangle = \alpha|1\rangle + \beta|2\rangle + \gamma|3\rangle \tag{25}$$

into the state $|\Phi(\alpha,\beta,\gamma)\rangle$ (22). Each party obtains one qutrit of the encoded state: Alice the first, Bob the second, and Charlie the third. This scheme allows any two parties together to completely extract the secret state $|\Psi\rangle$ (25). But no party alone can infer *any* information about the secret state $|\Psi\rangle$: each party's local-density matrix is proportional to the identity. The procedure to retrieve $|\Psi\rangle$ from say the first two qutrits is the following [7]: First the first register is added to the second (modulo 3) and then the (resulting) second qutrit is added to the first (mod 3). These operations can be performed without any measurement. This changes an encoded state $|\Phi(\alpha,\beta,\gamma)\rangle$ to

$$\begin{aligned}&\alpha(|000\rangle + |111\rangle + |222\rangle) + \beta(|012\rangle + |120\rangle + |201\rangle) \\ &\quad + \gamma(|021\rangle + |102\rangle + |210\rangle) + \alpha(|000\rangle + |021\rangle + |012\rangle) \\ &\overset{AB}{\rightarrow} \beta(|112\rangle + |100\rangle + |121\rangle) + \gamma(|221\rangle + |212\rangle + |200\rangle) \\ &= (\alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle) \otimes (|00\rangle + |21\rangle + |12\rangle).\end{aligned} \tag{26}$$

The secret state is completely restored in the first register. Analogous decoding procedures apply for *AC* and *BC*.

In the original scheme [7] it is assumed that the parties are honest when they participate in reconstructing the secret quantum state. Now assume the president of the bank uses this procedure to encode one of three (classical) ''trits'' ($b=0$, 1, or 2). He may want to use three orthogonal states $|\Phi_0\rangle$, $|\Phi_1\rangle$, $|\Phi_2\rangle$ that can be completely distinguished by an orthogonal measurement. So he distributes one of three *known* orthogonal states to his three vice presidents. He does not want any of them *alone* to get knowledge about the encoded trit, only two of them together should be able to find out what the secret was. For illustration, let us suppose that he uses the states

$$|\Psi_0\rangle=|0\rangle, \quad |\Psi_1\rangle=|1\rangle, \quad |\Psi_2\rangle=|2\rangle \tag{27}$$

to encode $b=0$, 1, and 2, respectively, and creates and distributes one of the three encoded states $|\Phi(1,0,0)\rangle$, $|\Phi(0,1,0)\rangle$, and $|\Phi(0,0,1)\rangle$. The three parties know the set of encoded states but not the actual state they are sharing.

Now let us assume Bob decides to obtain the secret on his own without having to share his knowledge with Alice or Charlie. He thinks of the following strategy. He applies a unitary transformation U to his share of the encoded secret state

$$U:|0\rangle\rightarrow|1\rangle, \quad |1\rangle\rightarrow|2\rangle, \quad |2\rangle\rightarrow|0\rangle. \tag{28}$$

The set of encoded states after this transformation will have changed to

$$\begin{aligned} &|\Phi(1,0,0)\rangle\rightarrow(|010\rangle+|121\rangle+|202\rangle),\\ &|\Phi(0,1,0)\rangle\rightarrow(|022\rangle+|100\rangle+|211\rangle),\\ &|\Phi(0,0,1)\rangle\rightarrow(|001\rangle+|112\rangle+|220\rangle). \end{aligned} \tag{29}$$

Alice and Charlie have no way of detecting Bob's dishonest action. Suppose now that at the time for two parties to find out what the secret was, Alice and Bob were the two to jointly retrieve the state. If they apply Eq. (26) to the changed state, they obtain

$$\left.\begin{aligned} b=0:&|1\rangle,\\ b=1:&|2\rangle\\ b=2:&|0\rangle, \end{aligned}\right\}\otimes(|10\rangle+|01\rangle+|22\rangle),$$

At the end of this procedure, Alice and Bob are supposed to know the value of b. Assume $b=0$. Alice will think that $b=1$. Bob, however, having changed the state, knows that if jointly with Alice he gets the outcome ''$b=1$,'' the actual trit b is 0. So he has obtained the actual secret alone and misled Alice. Bob can apply U^{-1} afterwards to erase the traces of his cheating completely. Similar misleading happens if Bob and Charlie retrieve the secret. Of course, if Alice and Charlie were the two to recover the secret trit, Bob's action would not help and they will obtain $b=0$.

This type of cheating is possible, because the set of orthogonal states chosen to encode b is equivalent under local unitaries. Bob has applied a local unitary transformation U to change $\rho_{AB}^0\rightarrow\rho_{AB}^1$, etc. Hereby, he has changed the state corresponding to $b=0$ to a state $|\Psi\rangle$ with $\rho_{AB}^{\Psi}=\rho_{AB}^1$. $|\Psi\rangle$ and the actual state corresponding to $b=1$ are related by a local unitary on Charlie's system ($|\Psi\rangle$ is a purification of ρ_{AB}^1 and so is the state corresponding to $b=1$). This can only be possible if the states encoding $b=0$ and $b=1$ are unitarily equivalent.

To prevent this type of cheating by a dishonest misleading party, the president of the bank has to select a set of *incommensurate* orthogonal states like Eqs. (23). They are not transformable into each other by any local action (and classical communication). The class of incommensurate states has helped us to *choose a quantum secret*.

V. CONCLUSION

We have exhibited a class of locally equivalent multipartite states that belong to an essential different class of entanglement. Actually *almost all* locally similar multiparticle states cannot be transformed into each other either way by local operations and classical communication; *they are incommensurate*. The partial order induced on multipartite states by transformation via k-LOCC is different from the bipartite case: There is a multidimensional manifold of unitarily nonequivalent states that are maximal in the sense that there is no other state from which they can be obtained by k-LOCC. The number of parameters to characterize different classes of entanglement grows exponentially with the number of parties involved. This space of locally indistinguishable and yet incommensurate states suggests itself for cryptographic applications involving several parties. We have shown that a set of incommensurate orthogonal and locally indistinguishable states can improve an $((n,k))$-threshold scheme against a form of cheating by a party.

Other possible applications in cryptography should be investigated. For instance, it is conceivable to find states $|\Omega\rangle$ shared between k parties such that any of them by choosing a local action could transform the whole state into either $|\Phi\rangle$ or $|\Psi\rangle$, where the last two states have the same local-density matrices for each party. This shared state can then be used to share a secret between multiple users that none of them can reveal to an outsider. Only in getting together can they find out what the secret was. The partial order of multipartite states should be investigated beyond classes of locally equivalent states.

Another way to follow would be to suggest ''multipartite'' quantum bit commitment schemes involving sets of incommensurate states. Note that all proofs of the ''no-go'' theorem [8,9] for two-party quantum bit commitment schemes (like [10]) use the Schmidt-decomposition of a bipartite state (or in other words, the nonexistence of hidden parameters for two-party entanglement). Multiparty protocols do not obey their line of argument.

ACKNOWLEDGMENTS

Above all I would like to thank Michael Nielson for introducing me to the topic of multipartite entanglement, and

for very fruitful discussions and encouragement. Thanks are due to John Preskill for very helpful discussions and hospitality at Caltech, where this work was done, and to Alexei Kitaev for critical comments. Thanks are also due to Daniel Lidar and Markus Grassl for improvements on the manuscript. I wish to acknowledge continuing support by Issac Chuang. This work was partially supported by DARPA DAAG 55-97-1-0341, and through the Quantum Information and Computing Institute (QUIC) administered through the ARO.

[1] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer Academic, Dordrecht, 1993).
[2] M. Nielsen, e-print quant-ph/9811053.
[3] N. Linden, S. Popescu, and A. Sudbery, e-print quant-ph/9801076.
[4] N. Linden and S. Popescu, Fortschr. Phys. **46**, 567 (1998).
[5] C. Bennett, S. Popescu, D. Rohrlich, A. Smolin, and A. Thapliyal (unpublished).
[6] S. Popescu (unpublished).
[7] R. Cleve, D. Gottesman, and H.-K. Lo, e-print quant-ph/9901025.
[8] D. Mayers, e-print quant-ph/9603015.
[9] H.-K. Lo and H. F. Chau, Phys. Rev. Lett. **78**, 3410 (1997).
[10] G. Brassard, C. Crépeau, R. Jozsa, and D. Langlois, in *Proceedings of the 34th Annual IEEE Symposium on the Foundation of Computer Science* (IEEE Computer Society Press, Los Alamitos, CA, 1993), p. 362.