The state can be described by a density matrix ρ, which is a positive semidefinite operator with trace 1. The state is entangled if ρ cannot be expressed as a convex combination of product states, i.e., if there exist states ρ1, ρ2, ..., ρn such that

\[ \rho = \sum_i c_i \rho_i \]

where the ci are non-negative and \( \sum_i c_i = 1 \).

An entangled state cannot be factorized into a product of states from separate subsystems. This is a fundamental property of quantum mechanics, which is responsible for the non-local correlations observed in quantum experiments.

The study of entanglement, the so-called "spooky action at a distance" phenomenon, has led to the heart of quantum information theory and can be traced back to the work of Einstein, Podolsky, and Rosen in 1935.
where the $\sigma$’s are the members of the set of rotation matrices $\sigma = \{ I_2, (\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}), (\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}) \}$. The Rotations $\sigma$ are simply the identity and the three Pauli spin operators, leaving aside imaginary parts which contribute only to the overall phase. The single singlet obtained between $A$ and $B$ by this procedure is all that can be distilled. This is a simple consequence of $A$ and $B$ each possessing only one qubit in the original state $\rho$.

Because entanglement between $A$ and $B$ can be distilled from it, $\rho$ must be entangled. If it were not it could be written in the biseparable form

$$\rho = \sum \alpha_i |\psi_i^A \rangle \langle \psi_i^A| \otimes |\phi_i^{BCD} \rangle \langle \phi_i^{BCD}| .$$

It was proven in [3] that if two parties are on opposite sides of a separable cut, then local quantum operations and classical communication will always leave them in a separable form, which implies immediately that no pure entanglement can be distilled between them. So if $\rho$ is of the form (5) there would be no way to distill any entanglement between $A$ and any of the other parties, including $B$, even if all three other parties $B$, $C$ and $D$ join together. Since it actually is possible to distill entanglement under these conditions (having $B$ in the same laboratory with $C$ and $D$ can only help) $\rho$ must have been entangled all along.

On the other hand, if all four parties remain in separate labs the state is not distillable. The proof of this will be based on looking at various cuts across which $\rho$ is separable, despite the fact that it is an entangled state. To demonstrate the nondistillability of $\rho$ it will be sufficient to show that, despite being entangled, $\rho$ is separable across the three bipartite cuts $AB : CD, AC : BD$ and $AD : BC$. This will separate every party from every other party, and every pair of parties from every pair, across at least one separable boundary. This requires that no entanglement can be distilled between any two parties or any two pairs, leaving only the possibility of distilling some three- or four-party entanglement. This is ruled out by noting that any such entanglement would span a separable bipartite cut. For example, if there were some distilled $A : BC$ entanglement it would still have to be separable across the $AB : CD$ boundary, leaving only the possibility of some entanglement of $A$ with $B$ and/or some entanglement of $C$ with $D$, each of which has already been excluded.

The state $\rho$ is separable across the $AB : CD$ boundary as it is written in separable form (2). One way to show the state is separable across the $AC : BD$ cut is to rewrite the state with $B$ and $C$ interchanged and consider the original $AB : CD$ cut. After interchanging indices it is easy to show that $\rho$ is invariant under the interchange of $B$ and $C$ and is therefore separable across the $AC : BD$ cut. Writing out each vector in the mixture (leaving out the 1/2 normalization for clarity):

$$|\Phi^+\rangle_{AB} \otimes |\Phi^+\rangle_{CD} = (|00\rangle + |11\rangle) \otimes (|00\rangle + |11\rangle) = |0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle$$

$$|\Phi^-\rangle_{AB} \otimes |\Phi^-\rangle_{CD} = (|00\rangle - |11\rangle) \otimes (|00\rangle - |11\rangle) = |0000\rangle - |0011\rangle - |1100\rangle + |1111\rangle$$

$$|\Psi^+\rangle_{AB} \otimes |\Psi^+\rangle_{CD} = (|01\rangle + |10\rangle) \otimes (|01\rangle + |10\rangle) = |0101\rangle + |0110\rangle + |1001\rangle + |1010\rangle \right.$$ (6)

$$|\Psi^-\rangle_{AB} \otimes |\Psi^-\rangle_{CD} = (|01\rangle - |10\rangle) \otimes (|01\rangle - |10\rangle) = |0101\rangle - |0110\rangle - |1001\rangle + |1010\rangle$$

Now, by interchanging the $B$ and $C$ index we have

$$|\Phi^+\rangle_{AC} \otimes |\Phi^+\rangle_{BD} = |0000\rangle + |0101\rangle + |1010\rangle + |1111\rangle$$

$$|\Phi^-\rangle_{AC} \otimes |\Phi^-\rangle_{BD} = |0000\rangle - |0101\rangle - |1010\rangle + |1111\rangle$$

$$|\Psi^+\rangle_{AC} \otimes |\Psi^+\rangle_{BD} = |0111\rangle + |0110\rangle + |1001\rangle + |1100\rangle \right.$$ (7)

First note that in both cases when the outer product is taken and the projectors corresponding to these vectors are mixed together, all the minus signs will vanish. Terms with minus signs combined with each other will have the sign cancel. Negative terms combined with positive terms will be cancelled since all the negative terms appear elsewhere as positive terms. So either the signs or the cross-terms having them all cancel, and we can ignore sign hereafter. It is then simple to check that every term in (6) also appears in (7), just in a different place. When the projectors are added up they will result in the same final density matrix. The same property will hold for the $AD : BC$ cut which is symmetric with the $AC : BD$ case. Thus, $\rho$ has been shown to be not distillable and therefore its entanglement is bound.

If $\rho$ is separable across the $AC : BD$ cut, for instance, how is it possible that $B$ and $D$ coming together can enable $A$ and $B$ to become entangled? The answer is that when $C$ and $D$ join together in the same laboratory, they have crossed the line of the cut and can create obviously entangled across it. The surprising thing is that this entanglement is not only shared by $C$ and $D$ but by $A$ and $B$. It would not have been possible for $A$ and $B$ to become entangled without themselves getting together in the same laboratory were $\rho$ entirely four-way separable (1) to begin with, so the whole process depends on $\rho$’s having some four-way entanglement.
The invariance under interchange of particles noted above also makes it clear that $\rho$ has the property that if any two of the parties come together they can perform the Bell measurement and pass classical information to the other two parties giving them a distilled Bell state. Since it is not immediately obvious why this distillation works when, for example, $B$ and $D$ get together, since they don’t as clearly share a Bell state containing information about which Bell state the others share as when $A$ and $B$ or $C$ and $D$ get together, it is instructive to look at an alternative explanation for what is going on.

Since the $\sigma_i$’s are, up to a phase, self-inverse, and since Eq. (4) works whichever party applies the rotation, it must be that the $\sigma_i$’s can be used in reverse, to create one of the other Bell states out of a $|\Psi^+\rangle$. This is illustrated in Figure 1. The Bell measurement is just a rotation to the Bell basis (made up of a matrix whose rows are the Bell states) followed by a measurement in the standard basis. If we now think of the $\sigma_i$’s as multiplying the rows of the Bell measurement on the right rather than the original $|\Psi^+\rangle$’s on the left, we can see that they cancel each other out, up to a phase, and the resulting measurement inside the dashed box is the same as the original Bell measurement. We can then think of the whole procedure as $B$ and $D$ getting together to teleport [10] half of a $|\Psi^+\rangle$ belonging to $A$ and $B'$ to $C$ using the $|\Psi^-\rangle$ shared by $C$ and $D'$. The measurement will result in two bits of classical data $j$ which will be used at $C$ to complete the teleportation by performing a $\sigma_j$ rotation in exactly the same way as in Eq. (4).

Thus we may think of the whole process as either two parties measuring which Bell state they have (determining the unknown $\sigma_i$) or as their teleporting half of a $|\Psi^+\rangle$ they share with one party to the remaining party, with an implicit cancellation of the $\sigma_i$’s.

The “unlocking” feature, that two parties can assist the other two in getting some entanglement, is reminiscent of the unlocking of hidden entanglement discussed by Cohen [11] also known as the entanglement of assistance [12]. The new feature here is that the unlockable four-party state is bound entangled—the entanglement is not available if none of the parties can perform joint quantum operations. The earlier examples explicitly allow one of three parties, say $C$, to give the other two parties $A$ and $B$ some classical information which they can use to obtain some pure entanglement even though the joint state of $A$ and $B$ ignoring $C$ is separable, thus these are examples of three-party distillable states. These are two distinct types of unlocking: In one case $C$ can unlock the hidden entanglement shared by $A$ and $B$; in the other the ability of $C$ and $D$ to unlock the entanglement of $A$ and $B$ is itself unlocked by their coming together.

In [13], Dür, Cirac and Tarrach give a three-qubit state with the property that it is $A : BC$ and $B : AC$ separable, but not separable $AB : C$ (what they call a class 3 state). These separability conditions are sufficient to show using arguments similar to the above that their state is not distillable when all the parties are isolated. They further point out that their state has negative partial transpose with respect to $C$ and that the state is therefore $AB : C$ distillable because any state in $2 \otimes n$ with negative partial transpose is distillable [14]. Thus, they have provided the first example of an unlockable bound-entangled state, though it will require many copies of the state to perform the distillation, lacking the direct distillability in one copy of $\rho$.

The type of unlocking exhibited by Dür, Cirac and Tarrach state differs subtly from that of $\rho$ presented here. In their state, when $A$ and $B$ get together it is they who gain distillable entanglement with $C$. On the other hand, in the case of the four-party state, when two of the parties get together they gain nothing themselves, merely the ability to give the other two parties distillable entanglement. If three of the four parties of $\rho$ get together, the situation will be that of the Dür, Cirac and Tarrach state. This suggests the following categorization of states:

- **Altruistic states**: States where one party can help the others distill some entanglement, but gets none in return.
  - Examples of these are the states with hidden entanglement studied by Cohen [11] and DiVincenzo et. al. [12]. In particular the Greenberger, Horne and Zeilinger (GHZ) state [15] has this property.
  - **Unlockable bound-entangled states**: States that are bound unless some parties come together, after which some entanglement can be distilled between remaining separated parties. These include the Dür, Cirac and Tarrach state, as well as $\rho$.
  - **Unlockable bound-altruistic states**: Bound-entangled states that when some parties come together are reduced to altruistic states, $\rho$ being the first example.

Other states that have some multi-party entanglement, but are separable across various cuts, have been studied in [13,16-20]. The state $\rho$ has $A : B : C : D$ bound entanglement, when grouped $AB : C : D$ has distillable $C : D$ entanglement, and is separable $AB : CD$, and similarly for all permutations of the parties. A three-party state given in [17] has $A : B : C$ bound entanglement and is separable $A : BC$, $AB : C$ and $AC : B$.

There are several obvious generalizations of unlockable states to higher dimensions and more parties. For example, a four-party state of the same form as $\rho$ (Eq. (2)) but using the $n^2$ orthogonal maximally entangled states in $n \otimes n$ will
have the same properties. The unlocking measurement performed by C and D is just a measurement in the basis of the maximally entangled states, the separability across the \( AB : CD \) cut is again by construction, and the symmetry is easy to see using the teleportation argument with the \( \sigma_i \)'s being the members of Heisenberg group in \( n \) dimensions.

One could also look for states where if \( n \) parties come together they can cause the remaining \( m \) to have entanglement, or some subset of the remaining \( m' \), or where when some of the parties come together they can cause the remaining parties to still have an unlockable bound entangled state. Some such states may be constructed by distributing the parts of several copies of \( \rho \) among several (more than four) different parties. Some surprises await, however: The tensor product of two copies of \( \rho \), one shared by the four parties \( A, B, C \) and \( D \) and another shared by \( A, B, C \) and a fifth party \( E \) can be distilled into an EPR pair shared by \( D \) and \( E \), even though the individual copies of \( \rho \) are not distillable at all, providing an example of superadditivity of distillable entanglement [21]. The many variations of such states and their applications to the cryptographic “web of trust” are beyond the scope of this letter, but will the subject of future work.

A particular related question is whether there is an example of an unlockable bound entangled state of rank lower than four. It was shown in [22] that there exist no rank two bipartite bound entangled states. If a multi-partite bound entangled state were to exist, it would have to be that when enough parties join together the remaining bipartite state is always either separable or distillable. Since we now see that there do exist states that become distillable as parties join up, the search for a lower rank multi-party bound entangled state may prove fruitful.

The author would like to thank Charles Bennett, Ignacio Cirac, David DiVincenzo, Wolfgang Dürr, Oliver Cohen, Barbara Terhal, and Ashish Thapliyal for helpful discussions, and the Army Research Office for support under contract number DAAG55-98-C-0041.

FIG. 1. A and B (and C and D) share a \( |\Psi^-\rangle \) which has been turned into one of the four possible Bell states by \( \sigma_i \). When the \( \sigma_i \)'s are merged into the Bell measurement, we have teleportation from \( B' \) to \( C \).