Noncommuting Mixed States Cannot Be Broadcast

Howard Barnum, Carlton M. Caves, Christopher A. Fuchs, Richard Jozsa,* and Benjamin Schumacher†
Center for Advanced Studies, Department of Physics and Astronomy, University of New Mexico, Albuquerque, New Mexico 87131-1156
(Received 8 November 1995)

We show that, given a general mixed state for a quantum system, there are no physical means for *broadcasting* that state onto two separate quantum systems, even when the state need only be reproduced marginally on the separate systems. This result extends the standard no-cloning theorem for pure states.

PACS numbers: 89.70.+c, 02.50.–r, 03.65.Bz

The fledgling field of quantum information theory [1] draws attention to fundamental questions about what is physically possible and what is not. An example is the theorem [2,3] that there are no physical means by which an *unknown pure* quantum state can be reproduced or copied—a result summarized by the phrase "quantum states cannot be cloned." In this paper we formulate and prove an impossibility theorem that extends the pure-state no-cloning theorem to (invertible) mixed quantum states. The theorem answers the question: Are there any physical means for *broadcasting* an unknown quantum state onto two separate quantum systems? By broadcasting we mean that the marginal density operator of each of the separate systems is the same as the state to be broadcast.

The pure-state "no-cloning" theorem [2,3] prohibits broadcasting pure states, for the only way to broadcast a pure state $|\psi\rangle$ is to put the two systems in the product state $|\psi\rangle \otimes |\psi\rangle$, i.e., to clone $|\psi\rangle$. Things are more complicated when the states are mixed. A mixed-state no-cloning theorem is not sufficient to demonstrate no broadcasting, for there are many conceivable ways to broadcast a mixed state ρ without the joint state being in the product form $\rho \otimes \rho$, the mixed-state analog of cloning; the systems might be correlated or entangled in such a way as to give the right marginal density operators. For instance, if the density operator has the spectral decomposition $\rho = \sum_b \lambda_b |b\rangle\langle b|$, a potential broadcasting state is the highly correlated joint state $\tilde{\rho} = \sum_b \lambda_b |b\rangle|b\rangle\langle b|\langle b|$, which, though not of the product form $\rho \otimes \rho$, reproduces the correct marginal density operators.

The general problem, posed formally, is this. A quantum system AB is composed of two parts, A and B, each having an N-dimensional Hilbert space. System A is secretly prepared in one state from a set $\mathcal{A} = \{\rho_0, \rho_1\}$ of two quantum states. System B, slated to receive the unknown state, is in a standard quantum state Σ. The initial state of the composite system AB is the product state $\rho_s \otimes \Sigma$, where $s = 0$ or 1 specifies which state is to be broadcast. We ask whether there is any physical process $\mathcal{E}$, consistent with the laws of quantum theory, that leads to an evolution of the form $\rho_s \otimes \Sigma \rightarrow \mathcal{E}(\rho_s \otimes \Sigma) = \tilde{\rho}_s$, where $\tilde{\rho}_s$ is *any* state on the N^2-dimensional Hilbert space AB such that

$$\mathrm{tr}_A(\tilde{\rho}_s) = \rho_s \quad \text{and} \quad \mathrm{tr}_B(\tilde{\rho}_s) = \rho_s\,. \tag{1}$$

Here tr_A and tr_B denote partial traces over A and B. If there is an $\mathcal{E}$ that satisfies Eq. (1) for both ρ_0 and ρ_1, then the set $\mathcal{A}$ can be *broadcast*. A special case of broadcasting is the evolution specified by $\mathcal{E}(\rho_s \otimes \Sigma) = \rho_s \otimes \rho_s$; we reserve the word *cloning* for this strong form of broadcasting.

The most general action $\mathcal{E}$ on AB consistent with quantum theory is to allow AB to interact unitarily with an auxiliary quantum system C in some standard state and thereafter to ignore the auxiliary system [4]; that is,

$$\mathcal{E}(\rho_s \otimes \Sigma) = \mathrm{tr}_C[U(\rho_s \otimes \Sigma \otimes \Upsilon)U^\dagger]\,, \tag{2}$$

for some auxiliary system C, some standard state Υ on C, and some unitary operator U on ABC. We show that such an evolution can lead to broadcasting if and only if ρ_0 and ρ_1 commute. This result strikes close to the heart of the difference between the classical and quantum theories, because it provides another physical distinction between *commuting* and *noncommuting* states. We further show that $\mathcal{A}$ is clonable if and only if ρ_0 and ρ_1 are identical or orthogonal ($\rho_0\rho_1 = 0$).

To see that the set $\mathcal{A}$ can be broadcast when the states commute, we do not need to attach an auxiliary system. Since orthogonal pure states can be cloned, broadcasting can be obtained by cloning the simultaneous eigenstates of ρ_0 and ρ_1. Let $|b\rangle$, $b = 1, \ldots, N$, be an orthonormal basis for A in which both ρ_0 and ρ_1 are diagonal, and let their spectral decompositions be $\rho_s = \sum_b \lambda_{sb}|b\rangle\langle b|$. Consider any unitary operator U on AB consistent with $U|b\rangle|1\rangle = |b\rangle|b\rangle$. If we choose $\Sigma = |1\rangle\langle 1|$ and let

$$\tilde{\rho}_s = U(\rho_s \otimes \Sigma)U^\dagger = \sum_b \lambda_{sb}|b\rangle|b\rangle\langle b|\langle b|\,, \tag{3}$$

we immediately have that $\tilde{\rho}_0$ and $\tilde{\rho}_1$ satisfy Eq. (1).

The converse of this statement—that if $\mathcal{A}$ can be broadcast, ρ_0 and ρ_1 commute—is more difficult to prove. Our proof is couched in terms of the concept of *fidelity* between two density operators. The fidelity $F(\rho_0, \rho_1)$ is defined by

$$F(\rho_0, \rho_1) = \mathrm{tr}\sqrt{\rho_0^{1/2}\rho_1\rho_0^{1/2}}\,, \tag{4}$$

where for any positive operator O, i.e., any Hermitian operator with *non-negative* eigenvalues, $O^{1/2}$ denotes its

 0031-9007/96/76(15)/2818(4)$10.00

unique positive square root. (Note that Ref. [5] defines fidelity to be the square of the present quantity.) Fidelity is an analog of the modulus of the inner product for pure states [5,6] and can be interpreted as a measure of distinguishability for quantum states: it ranges between 0 and 1, reaching 0 if and only if the states are orthogonal and reaching 1 if and only if $\rho_0 = \rho_1$. It is invariant under the interchange $0 \to 1$ and under the transformation $\rho_0 \to U\rho_0 U^\dagger$, $\rho_1 \to U\rho_1 U^\dagger$ for any unitary operator U [5,7]. Also, from the properties of the direct product, one has that $F(\rho_0 \otimes \sigma_0, \rho_1 \otimes \sigma_1) = F(\rho_0,\rho_1)F(\sigma_0,\sigma_1)$.

Another reason $F(\rho_0,\rho_1)$ defines a good notion of distinguishability [8] is that it equals the minimal overlap between the probability distributions $p_0(b) = \mathrm{tr}(\rho_0 E_b)$ and $p_1(b) = \mathrm{tr}(\rho_1 E_b)$ generated by a generalized measurement or *positive operator-valued measure* (POVM) $\{E_b\}$ [4]. That is [7],

$$F(\rho_0,\rho_1) = \min_{\{E_b\}} \sum_b \sqrt{\mathrm{tr}(\rho_0 E_b)}\sqrt{\mathrm{tr}(\rho_1 E_b)}\,, \tag{5}$$

where the minimum is taken over all sets of positive operators $\{E_b\}$ such that $\sum_b E_b = \mathbb{1}$. This representation of fidelity has the advantage of being defined operationally in terms of measurements. We call a POVM that achieves the minimum in Eq. (5) an *optimal* POVM.

One way to see the equivalence of Eqs. (5) and (4) is through the Schwarz inequality for the operator inner product $\mathrm{tr}(AB^\dagger)$: $\mathrm{tr}(AA^\dagger)\,\mathrm{tr}(BB^\dagger) \ge |\mathrm{tr}(AB^\dagger)|^2$, with equality if and only if $A = \alpha B$ for some constant α. Going through this exercise is useful because it leads directly to the proof of the no-broadcasting theorem. Let $\{E_b\}$ be any POVM and let U be any unitary operator. Using the cyclic property of the trace and the Schwarz inequality, we have that

$$\sum_b \sqrt{\mathrm{tr}(\rho_0 E_b)}\sqrt{\mathrm{tr}(\rho_1 E_b)} = \sum_b \sqrt{\mathrm{tr}(U\rho_0^{1/2} E_b\, \rho_0^{1/2} U^\dagger)}\sqrt{\mathrm{tr}(\rho_1^{1/2} E_b\, \rho_1^{1/2})} \ge \sum_b |\mathrm{tr}(U\rho_0^{1/2} E_b^{1/2} E_b^{1/2} \rho_1^{1/2})| \tag{6}$$

$$\ge \left| \sum_b \mathrm{tr}(U\rho_0^{1/2} E_b \rho_1^{1/2}) \right| = |\mathrm{tr}(U\rho_0^{1/2}\rho_1^{1/2})|\,. \tag{7}$$

We can use the freedom in U to make the inequality as tight as possible. To do this, we recall [5,9] that $\max|\mathrm{tr}(VO)| = \mathrm{tr}\sqrt{O^\dagger O}$, where O is any operator and the maximum is taken over all unitary operators V. The maximum is achieved only by those V such that $VO = e^{i\phi}\sqrt{O^\dagger O}$, ϕ being arbitrary; that there exists at least one such V is ensured by the operator polar decomposition theorem [9]. Therefore, by choosing

$$U\rho_0^{1/2}\rho_1^{1/2} = \sqrt{\rho_1^{1/2}\rho_0\rho_1^{1/2}}\,, \tag{8}$$

we get that $\sum_b \sqrt{\mathrm{tr}(\rho_0 E_b)}\sqrt{\mathrm{tr}(\rho_1 E_b)} \ge F(\rho_0,\rho_1)$.

Consulting the conditions for equality in steps (6) and (7), we find that a POVM is optimal if and only if

$$U\rho_0^{1/2} E_b^{1/2} = \mu_b \rho_1^{1/2} E_b^{1/2} \tag{9}$$

and the terms in the sum (7) have a common phase. By absorbing this phase into U by virtue of its phase freedom, this second condition becomes

$$\mathrm{tr}(U\rho_0^{1/2} E_b \rho_1^{1/2}) = \mu_b\, \mathrm{tr}(\rho_1 E_b) \ge 0 \Leftrightarrow \mu_b \ge 0\,. \tag{10}$$

When ρ_1 is invertible, Eq. (9) becomes

$$M E_b^{1/2} = \mu_b E_b^{1/2}, \tag{11}$$

where

$$M = \rho_1^{-1/2} U \rho_0^{1/2} = \rho_1^{-1/2}\sqrt{\rho_1^{1/2}\rho_0\rho_1^{1/2}}\,\rho_1^{-1/2} \tag{12}$$

is a positive operator. Therefore one way to satisfy Eq. (9) with $\mu_b \ge 0$ is to take $E_b = |b\rangle\langle b|$, where the vectors $|b\rangle$ are an orthonormal eigenbasis for M, with μ_b the eigenvalue of $|b\rangle$. When ρ_1 is noninvertible, there are still optimal POVMs. One can choose the first E_b to be the projector onto the null space of ρ_1. In the support of ρ_1 (the orthocomplement of its null space), ρ_1 is invertible, so we may construct the analog of M restricted to the support and choose the remaining E_b's to project onto its eigenvectors. Note that if both ρ_0 and ρ_1 are invertible, M is invertible.

We begin the proof of the no-broadcasting theorem by using Eq. (5) to show that fidelity cannot decrease under the operation of partial trace; this gives rise to an elementary constraint on all potential broadcasting processes $\mathcal{E}$. Suppose Eq. (1) is satisfied for the process $\mathcal{E}$ of Eq. (2), and let $\{E_b\}$ denote an optimal POVM for distinguishing ρ_0 and ρ_1. Then, for each s, $\mathrm{tr}[\tilde\rho_s(E_b \otimes \mathbb{1})] = \mathrm{tr}_A[\mathrm{tr}_B(\tilde\rho_s)E_b] = \mathrm{tr}_A(\rho_s E_b)$; it follows that

$$\begin{aligned} F_A(\rho_0,\rho_1) &\equiv \sum_b \sqrt{\mathrm{tr}[\tilde\rho_0(E_b\otimes\mathbb{1})]}\sqrt{\mathrm{tr}[\tilde\rho_1(E_b\otimes\mathbb{1})]} \\ &\ge \min_{\{\tilde E_c\}} \sum_c \sqrt{\mathrm{tr}(\tilde\rho_0 \tilde E_c)}\sqrt{\mathrm{tr}(\tilde\rho_1 \tilde E_c)} \\ &= F(\tilde\rho_0,\tilde\rho_1)\,. \end{aligned} \tag{13}$$

Here $F_A(\rho_0,\rho_1)$ denotes the fidelity $F(\rho_0,\rho_1)$; the subscript A emphasizes that $F_A(\rho_0,\rho_1)$ stands for the particular representation on the first line. The inequality in Eq. (13) comes from the fact that $\{E_b \otimes \mathbb{1}\}$ might not be an optimal POVM for distinguishing $\tilde\rho_0$ and $\tilde\rho_1$; this demonstrates the said partial-trace property. Similarly

$$\begin{aligned} F_B(\rho_0,\rho_1) &\equiv \sum_b \sqrt{\mathrm{tr}[\tilde\rho_0(\mathbb{1}\otimes E_b)]}\sqrt{\mathrm{tr}[\tilde\rho_1(\mathbb{1}\otimes E_b)]} \\ &\ge F(\tilde\rho_0,\tilde\rho_1)\,, \end{aligned} \tag{14}$$

where the subscript B emphasizes that $F_B(\rho_0, \rho_1)$ stands for the representation on the first line.

On the other hand, we can just as easily derive an inequality that is opposite to Eqs. (13) and (14). By the direct product formula and the invariance of fidelity under unitary transformations,

$$F(\rho_0, \rho_1) = F(\rho_0 \otimes \Sigma \otimes \Upsilon, \rho_1 \otimes \Sigma \otimes \Upsilon) = F\big(U(\rho_0 \otimes \Sigma \otimes \Upsilon)U^\dagger, U(\rho_1 \otimes \Sigma \otimes \Upsilon)U^\dagger\big). \quad (15)$$

Therefore, by the partial-trace property,

$$F(\rho_0, \rho_1) \le F\big(\mathrm{tr}_C[U(\rho_0 \otimes \Sigma \otimes \Upsilon)U^\dagger], \mathrm{tr}_C[U(\rho_1 \otimes \Sigma \otimes \Upsilon)U^\dagger]\big), \quad (16)$$

or, more succinctly,

$$F(\rho_0, \rho_1) \le F\big(\mathcal{E}(\rho_0 \otimes \Sigma), \mathcal{E}(\rho_1 \otimes \Sigma)\big) = F(\tilde{\rho}_0, \tilde{\rho}_1). \quad (17)$$

The elementary constraint now follows, for the only way to maintain Eqs. (13), (14), *and* (17) is with strict equality. In other words, we have that if the set $\mathcal{A}$ can be broadcast, then there are density operators $\tilde{\rho}_0$ and $\tilde{\rho}_1$ on AB satisfying Eq. (1) *and*

$$F_A(\rho_0, \rho_1) = F(\tilde{\rho}_0, \tilde{\rho}_1) = F_B(\rho_0, \rho_1). \quad (18)$$

Let us pause at this point to consider the restricted question of cloning. If $\mathcal{A}$ is to be clonable, there must exist a process $\mathcal{E}$ such that $\tilde{\rho}_s = \rho_s \otimes \rho_s$ for $s = 0, 1$. But then, by Eq. (18), we must have

$$F(\rho_0, \rho_1) = F(\rho_0 \otimes \rho_0, \rho_1 \otimes \rho_1) = F(\rho_0, \rho_1)^2, \quad (19)$$

which means that $F(\rho_0, \rho_1) = 1$ or 0; i.e., ρ_0 and ρ_1 are identical or orthogonal. There can be no cloning for density operators with nontrivial fidelity. The converse, that orthogonal and identical density operators can be cloned, follows, in the first case, from the fact that they can be distinguished by measurement and, in the second case, because they need not be distinguished at all.

Like the pure-state no-cloning theorem [2,3], this no-cloning result for mixed states is a consistency requirement for the axiom that quantum measurements cannot distinguish nonorthogonal states with perfect reliability. If nonorthogonal quantum states could be cloned, there would exist a measurement procedure for distinguishing those states with arbitrarily high reliability: one could make measurements on enough copies of the quantum state to make the probability of a correct inference of its identity arbitrarily high. That this consistency requirement, as expressed in Eq. (18), should also exclude more general kinds of broadcasting is not immediately obvious. Nevertheless, this is the content of our claim that Eq. (18) generally cannot be satisfied; any broadcasting process can be viewed as creating distinguishability *ex nihilo* with respect to measurements on the larger Hilbert space AB. Only for commuting density operators does broadcasting not create any extra distinguishability.

We now show that Eq. (18) implies that ρ_0 and ρ_1 commute. We assume that ρ_0 and ρ_1 are invertible. We proceed by studying the conditions necessary for the representations $F_A(\rho_0, \rho_1)$ and $F_B(\rho_0, \rho_1)$ in Eqs. (13) and (14) to equal $F(\tilde{\rho}_0, \tilde{\rho}_1)$. Recall that the optimal POVM $\{E_b\}$ for distinguishing ρ_0 and ρ_1 can be chosen so that the POVM elements $E_b = |b\rangle\langle b|$ are a complete set of orthogonal one-dimensional projectors onto orthonormal eigenstates of M. Then, repeating the steps leading from Eqs. (7) to (10), one finds that the necessary conditions for equality in Eq. (18) are that each $E_b \otimes \mathbb{1} = (E_b \otimes \mathbb{1})^{1/2}$ and each $\mathbb{1} \otimes E_b = (\mathbb{1} \otimes E_b)^{1/2}$ satisfy

$$\tilde{U}\tilde{\rho}_0^{1/2}(\mathbb{1} \otimes E_b) = \alpha_b\, \tilde{\rho}_1^{1/2}(\mathbb{1} \otimes E_b), \quad (20)$$

$$\tilde{V}\tilde{\rho}_0^{1/2}(E_b \otimes \mathbb{1}) = \beta_b\, \tilde{\rho}_1^{1/2}(E_b \otimes \mathbb{1}), \quad (21)$$

where α_b and β_b are non-negative numbers and $\tilde{U}$ and $\tilde{V}$ are unitary operators satisfying

$$\tilde{U}\tilde{\rho}_0^{1/2}\tilde{\rho}_1^{1/2} = \tilde{V}\tilde{\rho}_0^{1/2}\tilde{\rho}_1^{1/2} = \sqrt{\tilde{\rho}_1^{1/2}\tilde{\rho}_0\tilde{\rho}_1^{1/2}}\,. \quad (22)$$

Although ρ_0 and ρ_1 are assumed invertible, one cannot demand that $\tilde{\rho}_0$ and $\tilde{\rho}_1$ be invertible—a glance at Eq. (3) shows that to be too restrictive. This means that $\tilde{U}$ and $\tilde{V}$ need not be the same. Also we cannot assume that there is any relation between α_b and β_b.

The remainder of the proof consists in showing that Eqs. (20)–(22), which are necessary (though perhaps not sufficient) for broadcasting, are nevertheless restrictive enough to imply that ρ_0 and ρ_1 commute. The first step is to sum over b in Eqs. (20) and (21). Defining the positive operators

$$G = \sum_b \alpha_b |b\rangle\langle b| \quad \text{and} \quad H = \sum_b \beta_b |b\rangle\langle b|, \quad (23)$$

we obtain

$$\tilde{U}\tilde{\rho}_0^{1/2} = \tilde{\rho}_1^{1/2}(\mathbb{1} \otimes G) \quad \text{and} \quad \tilde{V}\tilde{\rho}_0^{1/2} = \tilde{\rho}_1^{1/2}(H \otimes \mathbb{1}). \quad (24)$$

The next step is to demonstrate that G and H are invertible and, in fact, equal to each other. Multiplying the two equations in Eq. (24) from the left by $\tilde{\rho}_0^{1/2}\tilde{U}^\dagger$ and

$\tilde{\rho}_0^{1/2}\tilde{V}^\dagger$, respectively, and tracing the first over A and the second over B, we get

$$\rho_0 = \mathrm{tr}_A(\tilde{\rho}_0^{1/2}\tilde{U}^\dagger\tilde{\rho}_1^{1/2})G \quad \text{and} \quad \rho_0 = \mathrm{tr}_B(\tilde{\rho}_0^{1/2}\tilde{V}^\dagger\tilde{\rho}_1^{1/2})H\,. \tag{25}$$

Since, by assumption, ρ_0 is invertible, it follows that G and H are invertible. Returning to Eq. (24), multiplying both parts from the left by $\tilde{\rho}_1^{1/2}$, and tracing over A and B, respectively, we obtain

$$\mathrm{tr}_A(\tilde{\rho}_1^{1/2}\tilde{U}\tilde{\rho}_0^{1/2}) = \rho_1 G \quad \text{and} \quad \mathrm{tr}_B(\tilde{\rho}_1^{1/2}\tilde{V}\tilde{\rho}_0^{1/2}) = \rho_1 H\,. \tag{26}$$

Conjugating the two parts of Eq. (26) and inserting the results into the two parts of Eq. (25) yields

$$\rho_0 = G\rho_1 G \quad \text{and} \quad \rho_0 = H\rho_1 H\,. \tag{27}$$

This shows that $G = H$, because these equations have a unique positive solution, namely, the operator M of Eq. (12). This can be seen by multiplying Eq. (27) from the left and right by $\rho_1^{1/2}$ to get $\rho_1^{1/2}\rho_0\rho_1^{1/2} = (\rho_1^{1/2}G\rho_1^{1/2})^2$. The positive operator $\rho_1^{1/2}G\rho_1^{1/2}$ is thus the unique positive square root of $\rho_1^{1/2}\rho_0\rho_1^{1/2}$.

Knowing that $G = H = M$, we return to Eq. (24). The two parts, taken together, imply that

$$\tilde{V}^\dagger\tilde{U}\tilde{\rho}_0^{1/2} = \tilde{\rho}_0^{1/2}(M^{-1}\otimes M)\,. \tag{28}$$

If $|b\rangle$ and $|c\rangle$ are eigenvectors of M, with eigenvalues μ_b and μ_c, Eq. (28) implies that

$$\tilde{V}^\dagger\tilde{U}(\tilde{\rho}_0^{1/2}|b\rangle|c\rangle) = \frac{\mu_c}{\mu_b}(\tilde{\rho}_0^{1/2}|b\rangle|c\rangle)\,. \tag{29}$$

This means that $\tilde{\rho}_0^{1/2}|b\rangle|c\rangle$ is zero or it is an eigenvector of the unitary operator $\tilde{V}^\dagger\tilde{U}$. In the latter case, since the eigenvalues of a unitary operator have modulus 1, it must be true that $\mu_b = \mu_c$. Hence we can conclude that

$$\tilde{\rho}_0^{1/2}|b\rangle|c\rangle = 0 \quad \text{when} \quad \mu_b \neq \mu_c\,. \tag{30}$$

This is enough to show that M and ρ_0 commute and hence $[\rho_0, \rho_1] = 0$. Consider the matrix element

$$\langle b'|(M\rho_0 - \rho_0 M)|b\rangle = (\mu_{b'} - \mu_b)\langle b'|\rho_0|b\rangle = (\mu_{b'} - \mu_b)\sum_c \langle b'|\langle c|\tilde{\rho}_0|c\rangle|b\rangle\,. \tag{31}$$

If $\mu_b = \mu_{b'}$, this is automatically zero. If, on the other hand, $\mu_b \neq \mu_{b'}$, then the sum over c must vanish by Eq. (30). It follows that ρ_0 and M commute. Hence, using Eq. (27),

$$\rho_1\rho_0 = M^{-1}\rho_0 M^{-1}\rho_0 = \rho_0 M^{-1}\rho_0 M^{-1} = \rho_0\rho_1\,. \tag{32}$$

This completes the proof that noncommuting quantum states cannot be broadcast.

Note that, by the same method as above, $\tilde{\rho}_1^{1/2}|b\rangle|c\rangle = 0$ when $\mu_b \neq \mu_c$. This condition, along with Eq. (30), determines the conceivable broadcasting states, in which the correlations between the systems A and B range from purely classical to purely quantum. For example, since ρ_0 and ρ_1 commute, the states of Eq. (3) satisfy these conditions, but so do the perfectly entangled pure states $\sum_b \sqrt{\lambda_{sb}}\,|b\rangle|b\rangle$. Not all such broadcasting states can be realized by a physical process $\mathcal{E}$, but sufficient conditions for realizability are not known.

In closing, we mention an application of this result. In some versions of quantum cryptography [10], the legitimate users of a communication channel encode the bits 0 and 1 into nonorthogonal pure states. This is done to ensure that any eavesdropping is detectable, since eavesdropping necessarily disturbs the states sent to the legitimate receiver [11]. If the channel is noisy, however, causing the bits to evolve to noncommuting mixed states, the detectability of eavesdropping is no longer a given. The result presented here shows that there are no means available for an eavesdropper to obtain the signal, noise and all, intended for the legitimate receiver without in some way changing the states sent to the receiver.

We thank Richard Hughes for useful discussions. This work was supported in part by the Office of Naval Research (Grant No. N00014-93-1-0116).

*Permanent address: School of Mathematics and Statistics, University of Plymouth, Drake Circus, Plymouth, Devon PL4 8AA, England.

†Permanent address: Department of Physics, Kenyon College, Gambier, OH 43022.

[1] C. H. Bennett, Phys. Today **48**, No. 10, 24 (1995).
[2] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982).
[3] D. Dieks, Phys. Lett. **92A**, 271 (1982).
[4] K. Kraus, *States, Effects, and Operations: Fundamental Notions of Quantum Theory* (Springer, Berlin, 1983).
[5] R. Jozsa, J. Mod. Opt. **41**, 2315 (1994).
[6] A. Uhlmann, Rep. Math. Phys. **9**, 273 (1976).
[7] C. A. Fuchs and C. M. Caves, Open Sys. Inf. Dyn. **3**, 1 (1995).
[8] W. K. Wootters, Phys. Rev. D **23**, 357 (1981).
[9] R. Schatten, *Norm Ideals of Completely Continuous Operators* (Springer, Berlin, 1960).
[10] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[11] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).