Quantum Cryptography Based on Two Mixed States

Masato Koashi and Nobuyuki Imoto
NTT Basic Research Laboratories, 3-1 Morinosato Wakamiya, Atsugi, Kanagawa 243-01, Japan

(Received 12 April 1996)

Although it is known that any two nonorthogonal pure states can constitute a secure quantum cryptosystem, the generalization of this scheme to the use of two mixed states is not trivial. It is shown here that even if a condition corresponding to the nonorthogonality in the pure-state case is satisfied, the mixed-state cryptosystem is still vulnerable to attack by an eavesdropper. A necessary and sufficient condition for the secure communication is derived. It states that the two mixed states must be connected by a rotation operator with a nonorthogonal angle. [S0031-9007(96)01116-7]

PACS numbers: 89.70.+c, 03.65.−w

A typical aim of cryptography is to enable two parties, traditionally called Alice and Bob, to exchange messages without fearing that the information will leak to any other party. The only method known for this uses the so-called one-time pad, for which the coding and the decoding require a sequence of random bits (the "key") whose length is equal to that of the messages. The security of the communication depends on the secrecy of the key shared by the two parties, but none of the classical methods for distributing the key on a public channel has been proven to be secure. The methods are trusted simply because the computation required for breaking them would take too much time. Quantum cryptography, on the other hand, offers schemes in which the intervention of an eavesdropper, traditionally called Eve, inevitably introduces transmission errors, thereby revealing her presence to the legitimate parties. These schemes are secure as long as the laws of quantum mechanics are not violated.

The first scheme for quantum cryptography, presented by Bennett and Brassard [1], uses four states of single photons polarized along different directions, and various other types of quantum cryptosystems have since been suggested. There are proposed schemes utilizing Einstein-Podolsky-Rosen correlations [2,3], one based on two nonorthogonal states [4], a variant of the four-state scheme [5], and one based on orthogonal states [6]. Some have been demonstrated experimentally [7–10].

In all of these schemes the states prepared by Alice have been considered as pure states. In practical situations, however, the preparation of the states may not be precisely controlled by Alice, and some inherent noises may remain in the carriers of the bit information. In these cases the states used in the transmissions are mixed states and should be treated by density operators. It will also be of theoretical interest to find general requirements for the quantum states on which a secure key-distribution scheme can be built. In a first step to finding these requirements, in this Letter we generalize the two-state scheme [4], which is conceptually the simplest of the existing schemes, to the use of two mixed states. In the original scheme [4], Alice sends Bob a random binary sequence made of two states $|u_0\rangle$ and $|u_1\rangle$ representing the bits 0 and 1, respectively, and Bob subjects each state to a measurement randomly chosen from $P_0 \equiv 1 - |u_1\rangle\langle u_1|$ or $P_1 \equiv 1 - |u_0\rangle\langle u_0|$. Then Bob publicly tells Alice whether the result of each measurement was positive or negative. From the cases with positive results they can construct two copies of random bits that should be identical in the absence of eavesdropping. To certify this, they sacrifice some of the bits and compare them in a public channel. Any errors, if detected, indicate the presence of eavesdropping. It was proved that Eve cannot obtain the bit information without fear of introducing errors when $|u_0\rangle$ and $|u_1\rangle$ are nonorthogonal. Generalization of this scheme to two mixed states appears at first sight to be trivial, and one might think that any two "nonorthogonal" mixed states could be used for the secure transmissions. We will see, however, that this is not the case because Eve can choose among a greater variety of intervention strategies than are available to her in the pure-state case. As a result, additional conditions must be met if the key distribution is to be secure.

Suppose that Alice chooses two states with density operators $\rho^{(0)}$ and $\rho^{(1)}$, respectively, representing the bit values "0" and "1." In the following, we determine the requirements that must be met by these states if Alice is to transmit the bit values to Bob securely. First we represent $\rho^{(k)}$ $(k = 0, 1)$ in a diagonalized form,

$$\rho^{(k)} = \sum_{i=1}^{n^{(k)}} p_i^{(k)} |\Psi_i^{(k)}\rangle\langle\Psi_i^{(k)}|\,, \tag{1}$$

where the states $\{|\Psi_i^{(k)}\rangle\}$ with the same index k are mutually orthogonal, that is, $\langle\Psi_i^{(k)}|\Psi_j^{(k)}\rangle = \delta_{ij}$ for $k = 0, 1$. We assume that coefficients $p_i^{(k)}$ are nonzero so that $n^{(k)}$ represents the dimension of the Hilbert subspace $\mathcal{H}^{(k)}$ spanned by $\rho^{(k)}$.

For each transmission event, Alice chooses a bit value 0 or 1 randomly and sends Bob the corresponding state, $\rho^{(0)}$ or $\rho^{(1)}$. Bob then performs a measurement on the received state in order to determine which of the two states the received one is. We limit ourselves here to the ideal situation where Bob can determine whether or not the measurement was successful, and in the successful event Bob obtains the bit value chosen by Alice without errors if there is no intervention. One simple example of such measurement is the one based on the following projection operators $\overline{P}^{(k)}$ $(k = 0, 1)$,

$$\overline{P}^{(k)} = 1 - P^{(k)} \equiv 1 - \sum_{i=1}^{n^{(k)}} |\Psi_i^{(k)}\rangle\langle\Psi_i^{(k)}| , \qquad (2)$$

where $P^{(0)}$ and $P^{(1)}$ are, respectively, the projection operators to the subspaces $\mathcal{H}^{(0)}$ and $\mathcal{H}^{(1)}$. Bob subjects the received state to one of the above projections chosen randomly. When $\overline{P}^{(0)}$ is chosen, the outcome for the state $\rho^{(0)}$ is always negative because $\overline{P}^{(0)}\rho^{(0)} = 0$, and the state $\rho^{(1)}$ yields positive results with the probability $p^{(1)} =$ Tr$\{\overline{P}^{(0)}\rho^{(1)}\}$. Similarly, only $\rho^{(0)}$ may survive the projection $\overline{P}^{(1)}$, and the probability $p^{(0)}$ is Tr$\{\overline{P}^{(1)}\rho^{(0)}\}$. Thus Bob is sure that the measurement failed when the outcome was negative, and in the other cases he is sure that he obtained the correct value. The only requirement for this scheme is that the probabilities $p^{(0)}$ and $p^{(1)}$ are nonzero. This requirement can be otherwise stated as

$$N > n^{(0)} \quad \text{and} \quad N > n^{(1)}, \qquad (3)$$

where N is the dimension of the whole relevant Hilbert space $\mathcal{H} \equiv \mathcal{H}^{(0)} + \mathcal{H}^{(1)}$.

Now we consider the possible strategies of the eavesdropper Eve. A simple strategy is to conduct a measurement similar to the above example of Bob's measurement. When the outcome is negative, Eve tries to send Bob a fake state ρ that satisfies $\overline{P}^{(0)}\rho = \overline{P}^{(1)}\rho = 0$, so that Alice and Bob cannot detect an error in their transmissions. Such attack must be prevented by assuring that the fake state does not exist. This requires

$$\mathcal{H}^{(0)} \cap \mathcal{H}^{(1)} = \{\mathbf{0}\}, \qquad (4)$$

or, equivalently,

$$N = n^{(0)} + n^{(1)}. \qquad (5)$$

Note that under this condition, the inequalities (3) are always satisfied.

The absence of the fake state limits Eve's strategy to the measurements that keep $\rho^{(0)}$ and $\rho^{(1)}$ in $\mathcal{H}^{(0)}$ and $\mathcal{H}^{(1)}$, respectively. Her second strategy will thus be to project the state onto a subspace $\mathcal{H}_{\mathrm{M}}$ that satisfies $\mathcal{H}_{\mathrm{M}} \subset \mathcal{H}^{(0)}$ and $\mathcal{H}_{\mathrm{M}} \perp \mathcal{H}^{(1)}$. By this measurement, Eve would detect some of the bits with value 0 without introducing any error in the transmission. Thus, for the transmission to be secure, Alice and Bob must eliminate the presence of $\mathcal{H}_{\mathrm{M}}$ with a nonzero dimension. This requirement is written as follows:

$$\mathcal{H}^{(0)} \cap \mathcal{H}^{(1)\perp} = \{\mathbf{0}\}, \qquad (6)$$

where $\mathcal{H}^{(1)\perp}$ is the orthogonal complement of the subspace $\mathcal{H}^{(1)}$. From the symmetry of the argument between $\mathcal{H}^{(0)}$ and $\mathcal{H}^{(1)}$, $\mathcal{H}^{(1)} \cap \mathcal{H}^{(0)\perp} = \{\mathbf{0}\}$ must also be satisfied, but this condition is equivalent to Eq. (6) under condition (4). It is not difficult to show that under conditions (4) and (6), $\mathcal{H}^{(0)}$ and $\mathcal{H}^{(1)}$ have the same dimension: $n^{(0)} = n^{(1)} \equiv n$.

In the case of $n = 1$, the states sent by Alice are the two pure states, $|\Psi_1^{(0)}\rangle$ and $|\Psi_1^{(1)}\rangle$, and condition (6) is equivalent to the nonorthogonality condition $\langle\Psi_1^{(0)}|\Psi_1^{(1)}\rangle \neq 0$. Thus condition (6) may be considered a "nonorthogonality" condition generalized to the case of two mixed states.

Under conditions (4) and (6), Eve cannot make projections that exclude one of the two possible states. Using a third strategy, however, she can still perform a nontrivial projection and may gain some information without introducing error in the transmission. To see this, define the transformation $T^{(0)}$ on the subspace $\mathcal{H}^{(0)}$ by $T^{(0)} \equiv P^{(0)}P^{(1)}$. It is easy to show that $T^{(0)}$ is an Hermitian operator. Therefore, there exists a set of complete orthonormal bases $\{|\phi_i^{(0)}\rangle\}_{i=1,\ldots,n}$ for $\mathcal{H}^{(0)}$ that satisfy

$$T^{(0)}|\phi_i^{(0)}\rangle = \lambda_i|\phi_i^{(0)}\rangle, \qquad (7)$$

where λ_i is real and

$$\langle\phi_i^{(0)}|\phi_j^{(0)}\rangle = \delta_{ij}. \qquad (8)$$

The operator $P^{(1)}$ is the projection onto the subspace $\mathcal{H}^{(1)}$, and condition (6) ensures that $|\phi_i^{(0)}\rangle \notin \mathcal{H}^{(1)\perp}$, so that $P^{(1)}|\phi_i^{(0)}\rangle \neq \mathbf{0}$. By taking the norm of this projected state, we obtain

$$\langle\phi_i^{(0)}|P^{(1)}|\phi_i^{(0)}\rangle = \langle\phi_i^{(0)}|P^{(0)}P^{(1)}|\phi_i^{(0)}\rangle = \lambda_i > 0, \qquad (9)$$

where we used Eq. (7) and the fact that $P^{(0)}$ is the projection onto $\mathcal{H}^{(0)}$. Now we can define a set of normal operators $\{|\phi_i^{(1)}\rangle\}_{i=1,\ldots,n}$ on $\mathcal{H}^{(1)}$ by

$$|\phi_i^{(1)}\rangle \equiv \frac{P^{(1)}|\phi_i^{(0)}\rangle}{\sqrt{\lambda_i}}. \qquad (10)$$

As for the orthogonality in this set, we have

$$\begin{aligned}\langle\phi_i^{(1)}|\phi_j^{(1)}\rangle &= \frac{1}{\sqrt{\lambda_i}}\langle\phi_i^{(0)}|P^{(1)}|\phi_j^{(1)}\rangle = \frac{1}{\sqrt{\lambda_i}}\langle\phi_i^{(0)}|\phi_j^{(1)}\rangle \\ &= \frac{1}{\sqrt{\lambda_i}}\langle\phi_i^{(0)}|P^{(0)}|\phi_j^{(1)}\rangle \\ &= \frac{1}{\sqrt{\lambda_i\lambda_j}}\langle\phi_i^{(0)}|P^{(0)}P^{(1)}|\phi_j^{(0)}\rangle \\ &= \sqrt{\frac{\lambda_j}{\lambda_i}}\langle\phi_i^{(0)}|\phi_j^{(0)}\rangle = \delta_{ij}. \qquad (11)\end{aligned}$$

Therefore, $\{|\phi_i^{(1)}\rangle\}$ constitutes a complete orthonormal basis for $\mathcal{H}^{(1)}$. Equation (11) also shows the orthogonality between the bases in the different subspaces,

$$\langle\phi_i^{(0)}|\phi_j^{(1)}\rangle = \sqrt{\lambda_i}\,\delta_{ij}. \qquad (12)$$

Consider the Hilbert subspace $\mathcal{H}_i$ that is spanned by the two state vectors $|\phi_i^{(0)}\rangle$ and $|\phi_i^{(1)}\rangle$. The dimension of this subspace is 2 because condition (4) ensures that $|\phi_i^{(0)}\rangle$

and $|\phi_i^{(1)}\rangle$ are linearly independent. From the relations (8), (11), and (12) we see that the subspaces $\mathcal{H}_i$ ($i = 1,\ldots,n$) are mutually orthogonal. Thus, we can consider a measurement on $\mathcal{H}$ made of the projections, P_i, onto the subspaces $\mathcal{H}_i$. When Eve makes this measurement it cannot be detected by Bob because all P_i commute with $\overline{P}^{(0)}$ and $\overline{P}^{(1)}$.

Now Alice and Bob have to make this kind of attack futile. This is done by choosing their states such that the probability of yielding each result i in the above measurement is the same for both states,

$$\langle\phi_i^{(0)}|\rho^{(0)}|\phi_i^{(0)}\rangle = \langle\phi_i^{(1)}|\rho^{(1)}|\phi_i^{(1)}\rangle \quad \text{for } i = 1,\ldots,n\,. \tag{13}$$

We need to consider the cases in which some of the eigenvalues λ_i in (7) are degenerate. In these cases, Eve has some freedom in choosing the base states $|\phi_i^{(0)}\rangle$ for the degenerate eigenvalues [$|\phi_i^{(1)}\rangle$ are automatically determined through (10)]. The relation (13) should be satisfied for all possible choices for the base states $|\phi_i^{(0)}\rangle$. Alternatively, we can state the above requirement as follows: For a possible choice of the basis $\{|\phi_i^{(0)}\rangle\}$,

$$\langle\phi_i^{(0)}|\rho^{(0)}|\phi_j^{(0)}\rangle = \langle\phi_i^{(1)}|\rho^{(1)}|\phi_j^{(1)}\rangle \tag{14}$$

holds for all pairs of $\{i,j\}$ that satisfy $\lambda_i = \lambda_j$.

So far, Eve's strategy has been confined to the decomposition to the orthogonal subspaces. Using a fourth strategy, however, she can implement a more elaborate attack, which is described by an initial state of Eve's measurement apparatus $|u\rangle$ on the Hilbert space $\mathcal{H}_{\rm E}$ and a unitary operator U in the product space of $\mathcal{H}$ and $\mathcal{H}_{\rm E}$. Suppose that Eve has conducted the measurement by the projection $\{P_i\}$ described before and has happened to find the result was for a particular value of the suffix i. The postmeasurement state is $|\phi_i^{(0)}\rangle$ or $|\phi_i^{(1)}\rangle$, depending on the states that Alice has chosen. At this stage, Eve subjects this state together with her measurement apparatus $|u\rangle$ to the interaction U_{ji} that changes the states as follows:

$$U_{ji}|\phi_i^{(0)}\rangle|u\rangle = |\phi_j^{(0)}\rangle|u^{(0)}\rangle\,, \tag{15}$$

$$U_{ji}|\phi_i^{(1)}\rangle|u\rangle = |\phi_j^{(1)}\rangle|u^{(1)}\rangle\,, \tag{16}$$

where $|u^{(0)}\rangle$ and $|u^{(1)}\rangle$ are normalized states of Eve's apparatus, and the choice of the suffix j is up to Eve. To see the condition for the existence of the unitary operator U_{ij}, consider the normalized state

$$|\overline{\phi}_i^{(0)}\rangle \equiv \frac{1}{\sqrt{1-\lambda_i}}\,(|\phi_i^{(1)}\rangle - \sqrt{\lambda_i}\,|\phi_i^{(0)}\rangle)\,, \tag{17}$$

which is, from Eq. (12), orthogonal to $|\phi_i^{(0)}\rangle$. According to Eqs. (15) and (16), U_{ij} should operate on this state as follows:

$$U_{ij}|\overline{\phi}_i^{(0)}\rangle|u\rangle = \frac{1}{\sqrt{1-\lambda_i}}\,(|\phi_j^{(1)}\rangle|u^{(1)}\rangle - \sqrt{\lambda_i}\,|\phi_j^{(0)}\rangle|u^{(0)}\rangle)\,. \tag{18}$$

When $\langle u^{(0)}|u^{(1)}\rangle = \sqrt{\lambda_i/\lambda_j}$, the right-hand side of this equation is normalized and orthogonal to the right-hand side of Eq. (15), so that the unitary operator U_{ij} exists. This measurement introduces no error in the transmission, and Eve is able to eavesdrop over some of the transmitted bits if she can choose the suffix j with $\lambda_j > \lambda_i$, because in this case $\rho^{(0)}$ and $\rho^{(1)}$ leave her apparatus in different states. Thus, for secure transmissions,

$$\lambda_1 = \lambda_2 = \cdots = \lambda_n \equiv \lambda \tag{19}$$

must be satisfied. Under this condition, condition (14) is rewritten as

$$\langle\phi_i^{(0)}|\rho^{(0)}|\phi_j^{(0)}\rangle = \langle\phi_i^{(1)}|\rho^{(1)}|\phi_j^{(1)}\rangle \quad \text{for any } i,j\,. \tag{20}$$

Next we will prove that the relations (4), (6), (19), and (20) constitute a sufficient condition for the secure transmission. That is, we prove that these relations determine a condition under which any of Eve's measurement that does not introduce an error in the transmission gives no information on the values of the transmitted bits. Suppose that Eve prepares an initial state of her measurement apparatus $|u\rangle$ on the Hilbert space $\mathcal{H}_{\rm E}$ and subjects it, together with the state $\rho^{(k)}$ sent by Alice, to a unitary operator U in the product space of $\mathcal{H}$ and $\mathcal{H}_{\rm E}$. The state $\tilde{\rho}^{(k)}$ after this interaction is

$$\tilde{\rho}^{(k)} = U[\rho^{(k)} \otimes |u\rangle\langle u|]U^\dagger. \tag{21}$$

To keep transmission errors from being introduced, $\tilde{\rho}^{(k)}$ traced over $\mathcal{H}_{\rm E}$ must be on the subspace $\mathcal{H}^{(k)}$. Thus we can write

$$U(|\phi_i^{(k)}\rangle|u\rangle) = \sum_{l=1}^{n}\sqrt{\alpha_{il}^{(k)}}\,|\phi_l^{(k)}\rangle|u_{il}^{(k)}\rangle\,, \tag{22}$$

where $|u_{il}^{(k)}\rangle$ are state vectors on $\mathcal{H}_{\rm E}$ and where $\alpha_{il}^{(k)}$ are the positive (or zero) real parameters introduced so that $|u_{il}^{(k)}\rangle$ are normalized as $\langle u_{il}^{(k)}|u_{il}^{(k)}\rangle = 1$. By taking the inner product of (22) and its conjugate and using (8) and (11), we get

$$\sum_{l=1}^{n}\alpha_{il}^{(k)} = 1\,. \tag{23}$$

Similarly, taking the inner product between the different values of the index k and using (12), we obtain

$$\begin{aligned}\sum_{l=1}^{n}\sqrt{\frac{\lambda_l}{\lambda_i}}\sqrt{\alpha_{il}^{(0)}\alpha_{il}^{(1)}}\,\langle u_{il}^{(0)}|u_{il}^{(1)}\rangle &= \sum_{l=1}^{n}\sqrt{\alpha_{il}^{(0)}\alpha_{il}^{(1)}}\,\langle u_{il}^{(0)}|u_{il}^{(1)}\rangle \\ &= 1\,,\end{aligned} \tag{24}$$

where (19) was used. For the middle term of (24), we have the following inequalities under the relation (23):

$$\begin{aligned}\left|\sum_{l=1}^{n}\sqrt{\alpha_{il}^{(0)}\alpha_{il}^{(1)}}\,\langle u_{il}^{(0)}|u_{il}^{(1)}\rangle\right| &\leq \sum_{l=1}^{n}\sqrt{\alpha_{il}^{(0)}\alpha_{il}^{(1)}}\,|\langle u_{il}^{(0)}|u_{il}^{(1)}\rangle| \\ &\leq \sum_{l=1}^{n}\sqrt{\alpha_{il}^{(0)}\alpha_{il}^{(1)}} \leq 1\,.\end{aligned} \tag{25}$$

The three equalities in this expression must hold if (24) is to be satisfied. Thus we obtain

$$\alpha_{il}^{(0)} = \alpha_{il}^{(1)} \quad \text{and} \quad |u_{il}^{(0)}\rangle = |u_{il}^{(1)}\rangle\,. \tag{26}$$

The state left to Eve, $\rho_{\rm E}^{(k)}$, is obtained by tracing $\tilde{\rho}^{(k)}$ in (21) over $\mathcal{H}$ and is written as follows by using (22):

$$\begin{aligned}\rho_{\mathrm{E}}^{(k)} = \mathrm{Tr}_{\mathcal{H}}\, \tilde{\rho}^{(k)} &= \mathrm{Tr}_{\mathcal{H}}\left[\sum_{i,j} \langle \phi_i^{(k)} | \rho^{(k)} | \phi_j^{(k)} \rangle U [| \phi_i^{(k)} \rangle \langle \phi_j^{(k)} | \otimes | u \rangle \langle u |] U^\dagger \right] \\ &= \mathrm{Tr}_{\mathcal{H}}\left[\sum_{i,j,l,m} \langle \phi_i^{(k)} | \rho^{(k)} | \phi_j^{(k)} \rangle \sqrt{\alpha_{il}^{(k)} \alpha_{jm}^{(k)}} [| \phi_l^{(k)} \rangle \langle \phi_m^{(k)} | \otimes | u_{il}^{(k)} \rangle \langle u_{jm}^{(k)} |] \right] \\ &= \sum_{i,j,l} \langle \phi_i^{(k)} | \rho^{(k)} | \phi_j^{(k)} \rangle \sqrt{\alpha_{il}^{(k)} \alpha_{jl}^{(k)}}\, | u_{il}^{(k)} \rangle \langle u_{jl}^{(k)} | \,. \end{aligned} \tag{27}$$

Using Eqs. (20) and (26) in this expression results in $\rho_{\mathrm{E}}^{(0)} = \rho_{\mathrm{E}}^{(1)}$, which means that Eve is ignorant of which of the states Alice chose to send. Thus we conclude that the transmission is secure if and only if conditions (4), (6), (19), and (20) are satisfied.

The requirement for the security derived above can be stated in a quite simple form by using a unitary operator representing a multiple rotation with a nonorthogonal angle. Let us define a rotation $R_i(\theta)$ in the two-dimensional Hilbert space $\mathcal{H}_i$ as follows:

$$R_i(\theta) \equiv \exp[\theta(|\overline{\phi}_i^{(0)}\rangle\langle\phi_i^{(0)}| - |\phi_i^{(0)}\rangle\langle\overline{\phi}_i^{(0)}|)], \tag{28}$$

where the state $|\overline{\phi}_i^{(0)}\rangle$ is defined in (17). It is not difficult to show that $R_i(\theta_i)|\phi_i^{(0)}\rangle = |\phi_i^{(1)}\rangle$, where θ_i is in $(0, \pi/2)$ and satisfies $\cos\theta_i = \sqrt{\lambda_i}$. We can define a rotation $R(\theta)$ in the $2n$-dimensional Hilbert space $\mathcal{H}$ by a direct product of $R_i(\theta)$,

$$R(\theta) \equiv \prod_{i=1}^{n} R_i(\theta)\,. \tag{29}$$

Then it is obvious from Eqs. (19) and (20) that $\rho^{(0)}$ and $\rho^{(1)}$ are connected with the following relation:

$$\rho^{(1)} = R(\theta)\rho^{(0)}R^\dagger(\theta)\,, \tag{30}$$

where $\cos\theta = \sqrt{\lambda}$. The conditions (4) and (6) are now restated that θ should not be a multiple of $\pi/2$. Thus, the two states used as the carrier must be identical except for the rotation by a nonorthogonal angle θ.

Expression (30) also helps us imagine a practical implementation of the scheme presented here. Assume that Alice has a noisy source which produces an initial state, and the state is not pure but is in a known n-dimensional Hilbert space. She subjects this state to an apparatus that realizes a rotation in the form of Eq. (29). The data bits are encoded as two different settings of the apparatus, that is, as different values of the angle, θ_0 and θ_1 (the difference should not be a multiple of $\pi/2$). Bob injects received states into his apparatus having the same interaction as Alice with a random choice of the two angle $-\theta_0$ and $-\theta_1$, and he performs the projection measurement that separates off the n-dimensional Hilbert space.

In the whole discussion above, it is assumed that the transmission channel does not alter the states. The story will be different if the noise introduced by the channel is considered. We have also restricted the verification of the secrecy to the original scheme [4] of error detection, in deriving the necessary conditions above. If Bob is allowed to choose measurements other than $\overline{P}^{(0)}$ and $\overline{P}^{(1)}$ at his disposal, he may check the statistics of the results and infer the presence of eavesdropping. If Alice and Bob are satisfied with this weaker test, the necessary condition for the states may be weaker, but details are beyond the scope of this Letter. One apparent necessary (but not sufficient) condition is that the two density operators are noncommuting, since Eve can make copies of them if they commute [11].

In summary, we derived a necessary and sufficient condition that a quantum cryptosystem with two mixed states must meet in order to establish secure key distribution. A properly generalized condition for the nonorthogonality in the pure-state case was derived and was shown, by describing successful strategies for the eavesdropper, to be insufficient for ensuring security. For the transmissions to be secure the structure of the two mixed states must be identical, in the sense that the states are connected by a rotation operator.

[1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.
[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[3] A. K. Ekert, J. G. Rarity, P. R. Tapster, and G. M. Palma, Phys. Rev. Lett. **69**, 1293 (1992).
[4] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[5] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995).
[6] L. Goldenberg and L. Vaidman, Phys. Rev. Lett. **75**, 1239 (1995).
[7] C. H. Bennett, F. Bessette, G. Brassard, and L. Salvail, J. Cryptol. **5**, 3 (1992).
[8] A. Muller, J. Breguet, and N. Gisin, Europhys. Lett. **23**, 383 (1993).
[9] P. D. Townsend, Electron. Lett. **30**, 809 (1994).
[10] J. D. Franson and H. Ilves, Appl. Opt. **33**, 2949 (1994).
[11] H. Barnum *et al.*, Phys. Rev. Lett. **76**, 2818 (1996).