Quantum Privacy Amplification and the Security of Quantum Cryptography over Noisy Channels

David Deutsch,[1] Artur Ekert,[1] Richard Jozsa,[2] Chiara Macchiavello,[1] Sandu Popescu,[3] and Anna Sanpera[1]
[1]*Clarendon Laboratory, Department of Physics, University of Oxford, Parks Road, Oxford OX1 3PU, United Kingdom*
[2]*School of Mathematics and Statistics, University of Plymouth, Plymouth, Devon PL4 8AA, United Kingdom*
[3]*Department of Electrical, Computer and Systems Engineering, Boston University, Boston, Massachusetts 02215*
(Received 26 April 1996)

Existing quantum cryptographic schemes are not, as they stand, operable in the presence of noise on the quantum communication channel. Although they become operable if they are supplemented by classical privacy-amplification techniques, the resulting schemes are difficult to analyze and have not been proved secure. We introduce the concept of quantum privacy amplification and a cryptographic scheme incorporating it which is provably secure over a noisy channel. The scheme uses an "entanglement purification" procedure which, because it requires only a few quantum controlled-not and single-qubit operations, could be implemented using technology that is currently being developed. [S0031-9007(96)01288-4]

PACS numbers: 89.70.+c, 02.50.–r, 03.65.Bz, 89.80.+h

Quantum cryptography [1–3] allows two parties (traditionally known as Alice and Bob) to establish a secure random cryptographic key if, first, they have access to a quantum communication channel, and second, they can exchange classical public messages which can be monitored but not altered by an eavesdropper (Eve). Using such a key, a secure message of equal length can be transmitted over the classical channel. However, the security of quantum cryptography has so far been proved only for the idealized case where the quantum channel, in the absence of eavesdropping, is *noiseless*. That is because, under existing protocols, Alice and Bob detect eavesdropping by performing certain quantum measurements on transmitted batches of qubits and then using statistical tests to determine, with any desired degree of confidence, that the transmitted qubits are not entangled with any third system such as Eve. The problem is that there is in principle no way of distinguishing entanglement with an eavesdropper (caused by her measurements) from entanglement with the environment caused by innocent *noise*, some of which is presumably always present.

This implies that all existing protocols are, strictly speaking, inoperable in the presence of noise, since they require the transmission of messages to be suspended whenever an eavesdropper (or, therefore, noise) is detected. Conversely, if we want a protocol that is secure in the presence of noise, we must find one that allows secure transmission to continue even in the presence of eavesdroppers. To this end, one might consider modifying the existing protocols by reducing the statistical confidence level at which Alice and Bob accept a batch of qubits. Instead of the astronomically high level envisaged in the idealized protocol, they would set the level so that they would accept most batches that had encountered a given level of noise. They would then have to assume that some of the information in the batch was known to an eavesdropper. It seems reasonable that classical privacy amplification [4] could then be used to distill, from large numbers of such qubits, a key in whose security one could have an astronomically high level of confidence [5]. However, no such scheme has yet been proved to be secure. Existing proofs of the security of classical privacy amplification apply only to classical communication channels and classical eavesdroppers. They do not cover the new eavesdropping strategies that become possible in the quantum case: for instance, causing a quantum ancilla to interact with the encrypted message, storing the ancilla and later performing a measurement on it that is chosen according to the data that Alice and Bob exchange publicly.

In this paper we present a protocol that is secure in the presence of noise and an eavesdropper. It uses entanglement-based quantum cryptography [2], but with a new element, an "entanglement purification" procedure. This allows Alice and Bob to generate a pair of qubits in a state that is close to a pure, maximally entangled state, and whose entanglement with any outside system is arbitrarily low. They can generate this from any supply of pairs of qubits in mixed states with nonzero entanglement, even if an eavesdropper has had access to those qubits (see also [6,7]).

Our procedure—a *quantum privacy amplification* algorithm—(abbreviated as QPA algorithm) can be performed by Alice and Bob at distant locations by a sequence of local operations which are agreed upon by communication over a public channel. It is related to the procedure described in [8], but is more efficient.

In the idealized theory of entanglement-based quantum cryptography, Alice and Bob have a supply of qubit pairs,

 0031-9007/96/77(13)/2818(4)$10.00

each pair being in the pure, maximally entangled state $|\phi^+\rangle$, where

$$|\phi^\pm\rangle = \tfrac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle),$$
$$|\psi^\pm\rangle = \tfrac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle). \quad (1)$$

These are the so-called "Bell states" which form a convenient basis for the state space of a qubit pair. Alice and Bob each have one qubit from each pair. In the presence of noise, each pair would in general have become entangled with other pairs and with the environment, and would be described by a density operator on the space spanned by (1).

Note that any two qubits that are jointly in a pure state cannot be entangled with any third physical object. Therefore any algorithm that delivers qubit pairs in pure states must also have eliminated the entanglement between any of those pairs and any other system. Our scheme is based on an iterative quantum algorithm which, if performed with perfect accuracy, starting with a collection of qubit pairs in mixed states, would discard some of them and leave the remaining ones in states converging to $|\phi^+\rangle\langle\phi^+|$.

Our first departure from existing quantum cryptographic schemes is to assume that Eve *does* interact with all the qubits that are transmitted or received by either Alice or Bob. Indeed we analyze the scenario that is most favorable for eavesdropping, namely where Eve herself is allowed to prepare all the qubit pairs that Alice and Bob will subsequently use for cryptography. Any realistic situation would also involve environmental noise that is not under Eve's control, but this may be treated as a special case in which Eve is not using the full information available to her.

Suppose, then, that Eve has prepared two qubit pairs in some manner of her own choosing and sends one qubit from each pair to both Alice and Bob. Let the density operators of the two pairs be $\hat{\rho}$ and $\hat{\rho}'$, respectively. Alice performs a unitary operation

$$|0\rangle \to \tfrac{1}{\sqrt{2}}(|0\rangle - i|1\rangle), \quad (2)$$

$$|1\rangle \to \tfrac{1}{\sqrt{2}}(|1\rangle - i|0\rangle) \quad (3)$$

on each of her two qubits; Bob performs the inverse operation

$$|0\rangle \to \tfrac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), \quad (4)$$

$$|1\rangle \to \tfrac{1}{\sqrt{2}}(|1\rangle + i|0\rangle) \quad (5)$$

on his. If the qubits are spin-$\frac{1}{2}$ particles and the computation basis is that of the eigenstates of the z components of their spins, then the two operations correspond, respectively, to rotations by $\pi/2$ and $-\pi/2$ about the x axis.

Then Alice and Bob each perform two instances of the quantum controlled-not operation

$$\overset{\text{control}}{|a\rangle}\ \overset{\text{target}}{|b\rangle} \to \overset{\text{control}}{|a\rangle}\ \overset{\text{target}}{|a \oplus b\rangle} \quad (a,b) \in \{0,1\}, \quad (6)$$

where one pair ($\hat{\rho}$) comprises the two control qubits and the other one ($\hat{\rho}'$) the two target qubits [9]. Alice and Bob then measure the target qubits in the computational basis (e.g., they measure the z components of the targets' spins). If the outcomes coincide (e.g., both spins up or both spins down) they keep the control pair for the next round and discard the target pair. If the outcomes do not coincide, both pairs are discarded.

To see the effect of this procedure, consider the special case in which each pair is in state $\hat{\rho}$ and the joint state of the two pairs is the simple product $\hat{\rho} \otimes \hat{\rho}$. This case will suffice for our applications. We express the density operator $\hat{\rho}$ in the Bell basis $\{|\phi^+\rangle, |\psi^-\rangle, |\psi^+\rangle, |\phi^-\rangle\}$ and denote by $\{A, B, C, D\}$ the diagonal elements in that basis. Note that the first diagonal element $A = \langle\phi^+|\hat{\rho}|\phi^+\rangle$, which we call the "fidelity," is the probability that the qubit would pass a test for being in the state $|\phi^+\rangle$. Thus we wish to drive the fidelity to 1 (which implies that the other three diagonal elements go to 0). Now, in the case where the control qubits are retained, their density operator $\hat{\rho}^{\sim}$ will have diagonal elements $\{\tilde{A}, \tilde{B}, \tilde{C}, \tilde{D}\}$ which depend on average *only* on the diagonal elements of $\hat{\rho}$ (the average is taken over the two different coincident outcomes, e.g., both spins up and both spins out):

$$\tilde{A} = \tfrac{A^2+B^2}{N},$$
$$\tilde{B} = \tfrac{2CD}{N},$$
$$\tilde{C} = \tfrac{C^2+D^2}{N}, \quad (7)$$
$$\tilde{D} = \tfrac{2AB}{N},$$

where $N = (A + B)^2 + (C + D)^2$ is the probability that Alice and Bob obtain coinciding outcomes in the measurements on the target pair. That is, if the procedure is carried out many times on an ensemble of such pairs of pairs, then $\tilde{A}$, $\tilde{B}$, $\tilde{C}$, and $\tilde{D}$ give the average diagonal entries of the surviving pairs. Note that if the average $\tilde{A}$ is driven to 1 then each of the surviving pairs must individually approach the pure state $|\phi^+\rangle\langle\phi^+|$.

In passing, we note that if the two input pairs have *different* states $\hat{\rho}$ and $\hat{\rho}'$ with diagonal elements $\{A, B, C, D\}$ and $\{A', B', C', D'\}$, respectively, then the retained control pairs will, on average, have diagonal elements given by

$$\tilde{A} = \tfrac{AA'+BB'}{N},$$
$$\tilde{B} = \tfrac{C'D+CD'}{N},$$
$$\tilde{C} = \tfrac{CC'+DD'}{N}, \quad (8)$$
$$\tilde{D} = \tfrac{AB'+A'B}{N},$$

where $N = (A + B)(A' + B') + (C + D)(C' + D')$, which generalizes (7).

Suppose that Eve has provided L pairs of qubits, with density operators $\hat{\rho}_1, \hat{\rho}_2, \ldots, \hat{\rho}_L$. This is *not* to say that their overall density operator is necessarily of the product form

$$\hat{\rho}_1 \otimes \hat{\rho}_2 \otimes \cdots \otimes \hat{\rho}_L \tag{9}$$

for Eve may have prepared them in an entangled state. However, let us consider first the case in which the pairs are not entangled with each other, i.e., the overall state *is* of the form (9) above. Alice and Bob know nothing about the state preparation, they are simply presented with an ensemble of L pairs of qubits from which they can (if they wish) estimate the average density operator $\hat{\rho}_{\text{ave}}$:

$$\hat{\rho}_{\text{ave}} = \tfrac{1}{L}(\hat{\rho}_1 + \hat{\rho}_2 + \cdots + \hat{\rho}_L), \tag{10}$$

which characterizes the ensemble of pairs.

Alice and Bob now select pairs at random from the ensemble of provided pairs and apply the QPA procedure to pairs of these selected pairs. Thus we may set $\hat{\rho} = \hat{\rho}_{\text{ave}}$ in (7) and we are in effect studying the properties of the map

$$\begin{pmatrix} A \\ B \\ C \\ D \end{pmatrix} \rightarrow \begin{pmatrix} \tilde{A} \\ \tilde{B} \\ \tilde{C} \\ \tilde{D} \end{pmatrix} = \frac{1}{N} \begin{pmatrix} A^2 + B^2 \\ 2CD \\ C^2 + D^2 \\ 2AB \end{pmatrix}. \tag{11}$$

$\{\tilde{A}, \tilde{B}, \tilde{C}, \tilde{D}\}$ in (11) gives the average diagonal entries for the states of the surviving pairs, i.e., the diagonal entries of the average density operator of the ensemble of surviving pairs. Therefore the repeated application of the QPA procedure—generating successive ensembles of surviving pairs—corresponds to iteration of the map in (11).

Several interesting properties of this map can be easily verified. For example, if at any stage the fidelity A exceeds $\frac{1}{2}$, then after one more iteration, it still exceeds $\frac{1}{2}$. Although A does not necessarily increase monotonically, our target point, $A = 1, B = C = D = 0$, is a fixed point of the map and is the only fixed point in the region $A > \frac{1}{2}$. It is a local attractor. We have been unable to obtain a proof that it is also a global attractor in the region $A > \frac{1}{2}$, but we have verified this by computer simulation. In other words, if we begin with pairs whose average fidelity exceeds $\frac{1}{2}$, but which are otherwise in an arbitrary state (unentangled with each other), then the states of pairs surviving after successive iterations always converge to the unit-fidelity pure state $|\phi^+\rangle$. Since this is a pure state, none of the surviving pairs is, in the limit, entangled with any other system.

To illustrate the behavior of the iteration in Fig. 1 we plot the fidelity as a function of the initial fidelity and the number of iterations, in cases where $A > \frac{1}{2}$ and $B = C = D$ initially.

The above analysis applies to the case in which Eve does not entangle the pairs with each other [c.f. Eq. (9)].

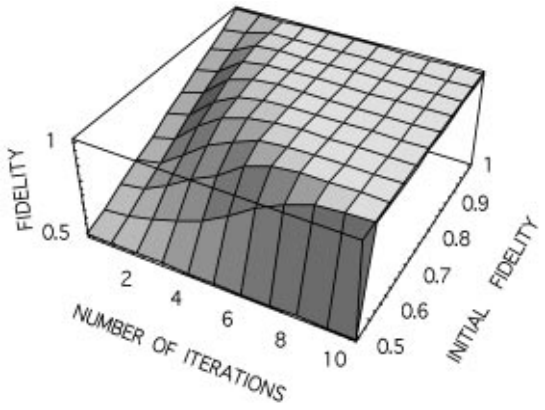

FIG. 1. Average fidelity as a function of the initial fidelity and the number of iterations.

However, if Eve provides pairs which *are* entangled with each other, then Eq. (11) no longer holds, and the QPA iterations may or may not converge to the pure state $|\phi^+\rangle\langle\phi^+|$. Nevertheless it is *never* of advantage to Eve to entangle pairs with each other: Eve knows that Alice and Bob will apply the QPA procedure to the distributed pairs. In the course of the QPA iterations Alice and Bob will periodically check the average fidelity of the surviving pairs, which is achieved by purely local operations and classical communication between them. Thus they determine whether they have achieved an acceptably high fidelity. If Eve provides pairs which are entangle with each other then the QPA procedure may not converge. In this case the protocol will force Alice and Bob to discard the entire transmission, and Eve is merely in effect blocking the quantum channel. (This would also be the case if, for example, she distributed pairs unentangled with each other, but having $A < \frac{1}{2}$.) On the other hand, if Eve provides pairs which *do* converge to $|\phi^+\rangle\langle\phi^+|$ (at an acceptable rate, i.e., at least the rate corresponding to the starting values of A, B, C, and D, which can be measured before starting the QPA procedure), then the QPA procedure is effective in excluding Eve despite the initial entanglement between the pairs. Thus Eve never benefits from providing pairs which are entangled with each other, and hence the above analysis suffices to prove the security of the protocol.

The QPA procedure is rather wasteful in terms of discarded particles—at least on half of the particles (the ones used as targets) are lost at every iteration. The efficiency of the procedure (i.e., the ratio of the number of surviving pairs to the number of initial pairs) depends on the final fidelity required and on the initial state. As an example, in Fig. 2(a) we plot the efficiency as a function of the initial fidelity A (taking $B = C = D$), for purification to fidelity 0.99, and in Fig. 2(b) we show the number of iterations used. The efficiency of our scheme compares very favorably with the entanglement purification scheme as described in [8], and it can be

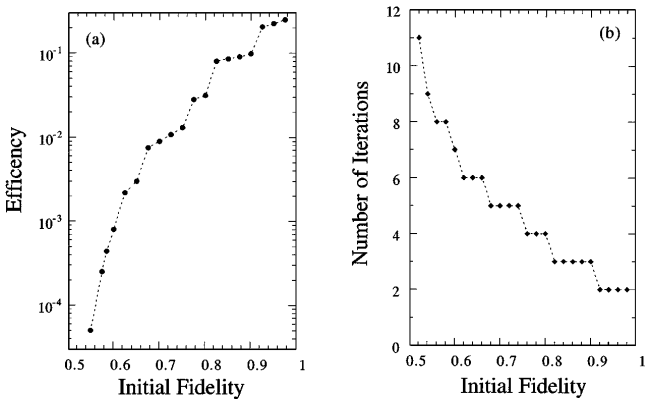

FIG. 2. States with $B = C = D$ are purified up to a fidelity of 0.99. (a) The efficiency of the purification as a function of the initial fidelity A. (b) The number of iterations used in the QPA procedure as a function of the initial fidelity.

directly applied to purify states which are not necessarily of the Werner form [10].

Even though the efficiency of our procedure may be low in many cases, it nevertheless establishes that there *exist* unconditionally secure quantum key distribution protocols. This is in contrast to recent claims [11] that quantum bit commitment protocols can never be unconditionally secure.

The QPA procedure is capable of purifying a collection of pairs in any state $\hat{\rho}$ of the product form (9), whose average fidelity with respect to at least one maximally entangled state (i.e., a Bell state or a state obtained from a Bell state via local unitary operations) is greater than $\frac{1}{2}$ (because any state of that type can be transformed into $|\phi^+\rangle$ via local unitary operations [12]). If we denote by $\mathcal{B}$ a class of pure, maximally entangled states (the generalized Bell states) then the condition that the state $\hat{\rho}$ can be purified using the QPA procedure is

$$\max_{\phi\in\mathcal{B}}\langle\phi|\hat{\rho}|\phi\rangle > \tfrac{1}{2}\,. \tag{12}$$

Note that this condition is not equivalent to the Horodecki condition [13] characterizing mixed states which can violate a generalized Bell inequality (CHSH inequality [14]). Indeed there exist mixed states which satisfy *both* our condition (12) *and* the CHSH inequalities. Thus the QPA algorithm reveals a more complete characterization of nonlocality than that given by Bell's theorem (c.f. also [6,7,15–17]). We hope to elaborate this in a forthcoming paper.

The practical implementation of the QPA procedure would require efficient quantum controlled-not gates operating directly on information carriers. Perhaps the most promising implementation of gates of this type (in the QPA context) is the one proposed by Turchette *et al.* [18]. It operates on polarized photons and allows the polarization of the target photon to be rotated depending on the polarization of the control photon. Although the current efficiency of the device is quite low, recent experimental progress in this field raises hopes for a successful QPA experiment in the not too distant future.

This research was supported in part by Elsag-Bailey PLC. We would like to thank A. Barenco and W. K. Wootters for stimulating discussions. A. E. and R. J. are sponsored by The Royal Society, London. C. M. is sponsored by the European Union HCM Programme. A. S. is sponsored by U.K. Engineering and Physical Sciences Research Council. A. E., R. J., and S. P. acknowledge Rabezzana Grignolino d'Asti.

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984* (IEEE, New York, 1984), p. 175.
[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[3] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[4] C. H. Bennett, G. Brassard, and J.-M. Robert, SIAM J. Comput. **17**, 210 (1988); C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, IEEE Trans. Inf. Theory **41**, 1915 (1995).
[5] H. K. Lo and H. F. Chau, Los Alamos Report No. quant-ph/9511025; D. Mayers, *Lecture Notes in Computer Science* (Springer-Verlag, Berlin, 1995), Vol. 963, pp. 124–135.
[6] M. Horodecki, P. Horodecki, and R. Horodecki, Los Alamos Report No. quant-ph/9605038.
[7] M. Horodecki, P. Horodecki, and R. Horodecki, Los Alamos Report No. quant-ph/9607009.
[8] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).
[9] A. Barenco, D. Deutsch, A. Ekert, and R. Jozsa, Phys. Rev. Lett. **74**, 4083 (1995).
[10] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).
[11] H. K. Lo and H. F. Chau, Los Alamos Report No. quant-ph/9603004; D. Mayers, Los Alamos Report No. quant-ph/9603015.
[12] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
[13] R. Horodecki, P. Horodecki, and M. Horodecki, Phys. Lett. A **200**, 340 (1995).
[14] J. Clauser, M. Horne, A. Shimony, and R. Holt, Phys. Rev. Lett. **23**, 880 (1969).
[15] S. Popescu, Phys. Rev. Lett. **72**, 797 (1994).
[16] S. Popescu, Phys. Rev. Lett. **74**, 2619 (1995).
[17] N. Gisin, Phys. Lett. A **210**, 151 (1996).
[18] Q. A. Turchette, C. J. Hood, W. Lange, H. Mabuchi, and H. J. Kimble, Phys. Rev. Lett. **75**, 4710 (1995).