Private Entanglement over Arbitrary Distances, Even Using Noisy Apparatus

Hans Aschauer and Hans J. Briegel

Theoretische Physik, Ludwig-Maximilians-Universität, Theresienstrasse 37, D-80333 München, Germany

(Received 23 August 2000; revised manuscript received 10 September 2001; published 9 January 2002)

We give a security proof of quantum cryptography based entirely on entanglement purification. Our proof applies to all possible attacks (individual and coherent). It implies the security of cryptographic keys distributed with the help of entanglement-based quantum repeaters. We prove the security of the obtained *quantum channel* which may not be used only for quantum key distribution, but also for secure, albeit noisy, transmission of quantum information.

DOI: 10.1103/PhysRevLett.88.047902 PACS numbers: 03.67.Dd, 03.67.Hk

Quantum cryptography (QC) promises the security of data transmission against any eavesdropping attack allowed by the laws of physics. The first QC protocol was described by Bennett and Brassard as early as 1984 [1]. Later, in 1991 Ekert presented a scheme based on Bell's theorem [2]. Though the security of these protocols is easy to prove under ideal conditions, a lot of work has been spent to prove the security under realistic circumstances. In all QC protocols, a possible eavesdropper is identified because of the disturbance that he or she introduces when trying to gain information about a quantum state that is transmitted. The problem is that every quantum channel introduces innocuous noise itself, which cannot, in principle, be distinguished from noise introduced by an eavesdropper. For that reason, a proof of unconditional security of QC has to assume that all noise in the channel is due to the interference of an eavesdropper.

Two different techniques have been developed to deal with these difficulties: *Classical privacy amplification* allows the eavesdropper to have partial knowledge about the raw key built up between the communicating parties Alice and Bob. From the raw key, a shorter key is "distilled" about which Eve has vanishing (i.e., exponentially small in some chosen security parameter) knowledge. Despite the simple idea, proofs taking into account all eavesdropping attacks allowed by the laws of quantum mechanics have shown to be technically involved [3–5]. Recently, Shor and Preskill [6] have given a simpler physical proof relating the ideas in [3,4] to quantum error correcting codes [7,8]. *Quantum privacy amplification* (QPA) [9], on the other hand, employs an entanglement purification [10,11] protocol that eliminates any entanglement with an eavesdropper by creating a few perfect EPR pairs out of many imperfect (or impure) EPR pairs. In principle, this method guarantees security against any eavesdropping attack. However, the problem is that the QPA protocol assumes ideal quantum operations. In reality, these operations are themselves subject to noise. As shown in [12,13], there is an upper bound $F_{\max}$ for the achievable fidelity of EPR pairs which can be distilled using noisy apparatus. *A priori,* there is no way to be sure that there is no residual entanglement with an eavesdropper. This problem could be solved if Alice and Bob had fault tolerant quantum computers at their disposal, which could then be used to reduce the noise of the apparatus to any desired level. This was an essential assumption in the security proof given by Lo and Chau [14].

In this Letter, we show that the standard two-way entanglement purification protocols alone, with some minor modifications to accommodate certain security aspects which will be discussed below, can be used to efficiently establish a *perfectly private quantum channel,* even when both the physical channel connecting the parties and the local apparatus used by Alice and Bob are noisy. This is of particular interest because, as we show, the *security* threshold for the noise level of the apparatus practically coincides with the *purification* threshold, so that the methods used for long-distance quantum communication, using entanglement-purification-based quantum repeaters [12] can be used for secure quantum communication *without any further requirements.* In particular, no fault tolerant quantum computers are required. This goal is achieved by proving that the final state of the protocol factorizes into a product state of the eavesdropper on one side, and Alice, Bob, and their laboratories (apparatuses) on the other side. Colloquially speaking, we prove that Eve is factored out under the action of the purification protocol, i.e., the finite fidelity at the end of the protocol is only due to entanglement with the apparatus. Our proof applies to all possible attacks (individual, collective, and coherent) and can be utilized directly in long-distance quantum communication. Different from existing work, we (i) prove the security of the entire quantum channel, (ii) do not require fault tolerant quantum computers, and (iii) our results have practical relevance, as the accuracy of the apparatus used by Alice and Bob may be about 2 orders of magnitude lower than the threshold accuracy for fault tolerant quantum computers [12,15].

The scenario is the following. Initially, Alice and Bob share a numbered ensemble of $2N$ qubits $\{(a_1, b_1), \ldots, (a_N, b_N)\}$, N qubits on each side, where N is large. Most generally, the state they obtain can be written in the form

$$\rho_{AB} = \sum_{\substack{\mu_1 \ldots \mu_N \\ \mu_1' \ldots \mu_N'}} \alpha_{\mu_1' \ldots \mu_N'}^{\mu_1 \ldots \mu_N} |\mathcal{B}_{\mu_1}^{(a_1 b_1)} \cdots \mathcal{B}_{\mu_N}^{(a_N b_N)}\rangle \times \langle \mathcal{B}_{\mu_1'}^{(a_1 b_1)} \cdots \mathcal{B}_{\mu_N'}^{(a_N b_N)}|, \quad (1)$$

where $|\mathcal{B}_{\mu_j}^{(a_j b_j)}\rangle$, $\mu_j = 00, 01, 10, 11$ denote the 4 Bell states associated with the two particles a_j and b_j. Specifically, $|\mathcal{B}_{ik}\rangle = (1/\sqrt{2})(|0k\rangle + (-1)^i|1, k + 1 \bmod 2\rangle)$ for $i, k \in \{0, 1\}$. The qubits have been distributed through some noisy channel, which may also include repeater stations involving additional qubits. Note that for the following proof the repeater stations may be entirely under Eve's control. In general, (1) will be an entangled state of $2N$ particles, which allows for the possibility of so-called coherent attacks [16]. This state may be used to establish a perfectly secret quantum channel, under the condition checked by the following protocol.

Upon reception of all pairs, Alice and Bob apply the following protocol to them. Note that steps 1 and 2 are applied only once, while steps 3, 4, and 5 are applied recursively.

Step 1: On each pair of particles (a_j, b_j), they apply randomly one of the four bilateral Pauli rotations $\sigma_k^{(a_j)} \otimes \sigma_k^{(b_j)}$, where $k = 0, 1, 2, 3$.

Step 2: Alice and Bob randomly renumber the pairs, $(a_j, b_j) \to (a_{\pi(j)}, b_{\pi(j)})$ where $\pi(j)$, $j = 1, \ldots, N$ is a random permutation.

After step 2, Alice and Bob may consistently describe the ensemble by the density operator [17]

$$\tilde{\rho}_{AB} = \left(\sum_\mu p_\mu |\mathcal{B}_\mu\rangle\langle\mathcal{B}_\mu|\right)^{\otimes N} \equiv (\rho_{ab})^{\otimes N}, \quad (2)$$

in which the p_μ describe the probability with which each pair is found in the Bell state $|\mathcal{B}_\mu\rangle$ [18]. At this point, Alice and Bob have to make sure that $p_{00} \equiv F > F_{\min}$ for some minimum fidelity $F_{\min} > 1/2$, which they can do by statistical tests on a certain fraction of the pairs. The exact value of $F_{\min}$ depends on the noise parameters of Alice's and Bob's apparatus [12,13].

Next, Alice and Bob apply one of the standard purification protocols as described in [9,10]. For simplicity, we concentrate on the protocol given in [9]; for other recurrence protocols, a similar proof could be given [19]. The protocol uses these steps.

Step 3: Bilateral rotations $1/2(\mathbf{1}^{(a)} - i\sigma_x^{(a)}) \otimes (\mathbf{1}^{(b)} + i\sigma_x^{(b)})$ are applied to all pairs (a, b).

Step 4: To all pairs of pairs a bilateral CNOT operation (BCNOT) is applied.

Step 5: The target pair of the BCNOT operation is measured on both sides in the z direction. If the measurement results coincide, the control pair is kept, otherwise it is discarded.

Since Alice and Bob use imperfect apparatus, it has been shown [12,13] that these protocols converge towards a mixed-state ensemble $\rho_{ab}^{(\infty)}$ with a maximum attainable fidelity $F_{\max} < 1$. If the fidelity of the local operations is moderate, the value of $F_{\max}$ could be quite low (80%, as an example).

In the following we will show that, despite such a poor attainable fidelity, Alice and Bob may happily proceed to apply the purification protocol to establish a secure quantum channel [20]. We show that, as $F \to F_{\max}$, the entanglement of the ensemble with the eavesdropper is reduced exponentially fast with the number of purification steps. In each step of the protocol, we assume that the apparatus introduces errors described by the following map:

$$\rho_{AB} \to \sum_{\mu,\nu=0}^{3} f_{\mu\nu} \sigma_\mu^{(a)} \sigma_\nu^{(b)} \rho_{AB} \sigma_\mu^{(a)} \sigma_\nu^{(b)}, \quad (3)$$

where a and b denote the qubits which are acted upon locally. The $f_{\mu\nu}$ can be interpreted as the joint probability that the Pauli rotations σ_μ and σ_ν are applied to qubits a and b, respectively. Equation (3) includes, for an appropriate choice of the coefficients $f_{\mu\nu}$, the one and two qubit depolarizing channel and combinations thereof, as studied in [12], but is more general.

It is possible to include the laboratories' degrees of freedom in the description. Noise of the form (3) can be attributed to some interaction with the apparatus, which is described by a map

$$|E\rangle_L |\psi\rangle_{AB} \to \sum_{\mu,\nu=0}^{3} |e_{\mu\nu}\rangle_L \sigma_\mu^{(a)} \sigma_\nu^{(b)} |\psi^{(ab)}\rangle. \quad (4)$$

This map explicitly accounts for the state of the apparatus before and after the interaction. The states $|e_{\mu\nu}\rangle$ are pairwise orthogonal and have the norm $\langle e_{\mu\nu}|e_{\mu\nu}\rangle = f_{\mu\nu}$. It is important to note that the laboratory degrees of freedom $|e_{\mu\nu}\rangle$ can, in principle, be identified in any physical environment that generates noise of the form (3), if the specific interaction Hamiltonian is known.

For our purpose, however, the physical details of the environment are of no concern, and we may replace the real process by the following scenario, where both Alice and Bob have a "little demon" (L) in the laboratory. For simplicity, we concentrate on the demon in Alice's laboratory only. Note that the generalization to noise in both labs is trivial. Before every purification step, the demon applies randomly one of the 16 rotations $\sigma_\mu^{(a)} \otimes \sigma_\nu^{(b)}$ to the qubits involved in this step, and keeps a record of which rotations he chose. For example, in the case of uncorrelated white noise (depolarizing channel), it leaves each qubit in its state ($\sigma_0 \equiv I$) with some probability f_0, but rotates its state by σ_j with equal probabilities $f_j = \frac{1-f_0}{3}$.

By doing this, the demon may accumulate a record of all errors in the history of each qubit throughout the process. Instead of keeping track of this growing list, he updates in each purification step a single *flag* $\phi \equiv (ij)$ that is associated with each of the pairs. The purpose of the error flag is to keep the information required for "undoing" the random rotations that occurred in the history of each pair. Note that, while this can be done trivially for unitary networks, the situation is quite different with the QPA distillation protocol, which includes measurements. Technically, the flag consists of two classical bits, called the error phase

bit i and the error amplitude bit j, and is calculated in the following way: If a $\sigma_x(\sigma_z, \sigma_y)$ error occurs, L inverts the error amplitude bit (error phase bit, both error bits).

Whenever Alice and Bob agree publicly to keep a control pair P_1 (because of coinciding measurement outcomes on the target pair P_2, see step 5 of the protocol), L "updates" the value of the error flag $(i_u j_u)$ of the kept pair with the *flag update function*: $(i_u j_u) = (i \oplus i', i \oplus j)$ if $i' \oplus j' \oplus i \oplus j = 0$, and $(i_u j_u) = (0, 0)$ otherwise. Note that the error flag which belongs to a pair is, by construction, only a function of the error record. It is important to realize that what the lab demon is doing is *not* quantum error correction, as he is not applying any correction operation on the qubits during the entire protocol. Instead of calculating the flags during the run of the protocol, they could equally be calculated after the protocol is finished.

At each purification step, the lab demon divides the total ensemble into four subensembles $\rho_{\mathrm{AB}}^{(ij)}$ corresponding to the value (ij) of the error flag. Initially, before the QPA protocol starts, he assigns some random or fixed values to the labels, while the subensembles are all described by the same state. That is, the error flags and the states of the pairs are initially completely uncorrelated. It is noteworthy that Bell diagonality of the states $\rho_{\mathrm{AB}}^{(ij)} = A^{(ij)}|\mathcal{B}_{00}\rangle\langle\mathcal{B}_{00}| + B^{(ij)}|\mathcal{B}_{11}\rangle\langle\mathcal{B}_{11}| + C^{(ij)}|\mathcal{B}_{01}\rangle\langle\mathcal{B}_{01}| + D^{(ij)}|\mathcal{B}_{10}\rangle\langle\mathcal{B}_{10}|$ is preserved. This is due to the fact that all operations in the protocol map Bell states onto Bell states.

In the following, we analyze the purification process in terms of these four different subensembles $\rho_{\mathrm{AB}}^{(ij)}$. In total, we have to keep track of 16 coefficients that occur in the expansion of each of the $\rho_{\mathrm{AB}}^{(ij)}$ in the Bell basis. These coefficients after the $(n+1)$th QPA step are functions of the coefficients after the nth QPA step:

$$\begin{aligned} A_n^{(00)} &\to A_{n+1}^{(00)}(A_n^{(00)}, A_n^{(01)}, \ldots, D_n^{(11)}), \\ A_n^{(01)} &\to A_{n+1}^{(01)}(A_n^{(00)}, A_n^{(01)}, \ldots, D_n^{(11)}), \\ &\vdots \\ D_n^{(11)} &\to D_{n+1}^{(11)}(A_n^{(00)}, A_n^{(01)}, \ldots, D_n^{(11)}). \end{aligned} \tag{5}$$

The explicit form of the 16 recurrence relations (5) can be given, but they are rather lengthy. They imply a reduced set of 4 recurrence relations for the quantities $A_n = \sum_{ij} A_n^{(ij)}, \ldots, D_n = \sum_{ij} D_n^{(ij)}$ which describe the evolution of the total ensemble under the purification protocol. For $n \to \infty$, these quantities converge towards a fix point $(A_\infty, B_\infty, C_\infty, D_\infty)$ where $A_\infty = F_{\max}$ is the maximal attainable fidelity [12]. Different from the fidelity $F_n \equiv A_n$, we define the *conditional fidelity* $F_n^{\mathrm{cond}} = A_n^{(00)} + B_n^{(11)} + C_n^{(01)} + D_n^{(10)}$. This is the fidelity of the ensemble that Alice and Bob could attain, if the lab demon disclosed the error flags (or, for that matter, only the history of the random rotations, from which the flags can be calculated): Depending on the error flag of a pair, Alice could then choose a local rotation that transforms the pair into the Bell state $|\mathcal{B}_{00}\rangle$ with probability F^{cond}.

Evaluation of the recurrence relation yields that there are three different regimes of noise parameters: In the high-noise regime (low values of f_{00}), no purification is possible; the protocol converges to completely depolarized pairs. In the low-noise regime (high values of f_{00}), the protocol purifies *and* the conditional fidelity converges to unity: the protocol is in the security regime (see Fig. 1). Between these two regimes, just above the purification threshold, there exists a very narrow third regime: The protocol purifies, while the conditional fidelity does *not* converge to unity. It is not known whether or not secure communication is possible in this regime. For the depolarizing channel, for example, the intermediate regime is contained in the interval $f_0 \in (0.8983, 0.8988)$, while the security regime covers the entire interval $f_0 \in [0.8988, 1]$. The security regime thus coincides, for all practical purposes, with the purification regime, but it is interesting to see that these regimes are not strictly identical. It shows that the process of factorization is, in the situation of imperfect apparatus, not trivially connected to the process of purification. More details about these regimes will be published elsewhere [17]. When the protocol is in the security regime, both the fidelity F_n and the conditional fidelity F_n^{cond} reach their respective fix points exponentially fast with the same exponents (see Fig. 2). From this it follows that there exists a polynomial relation between the resources used in the purification process (number of initial pairs) and the security parameter $1 - F^{\mathrm{cond}}$. All results obtained from the evaluation of the recurrence relations (5) were also checked with the help of Monte Carlo simulations, in which the QPA protocol was applied to typical ensembles of Bell states.

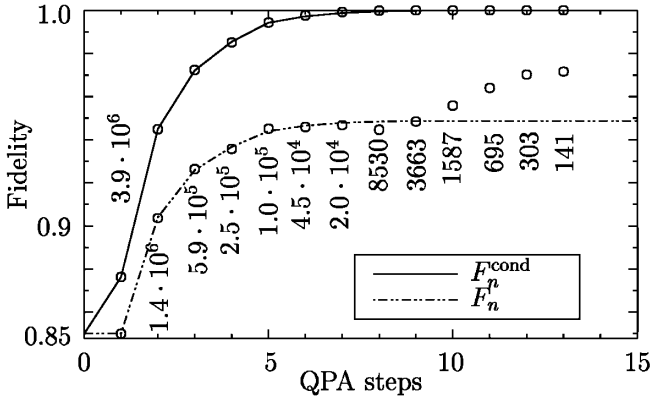

FIG. 1. The fidelities F and F_{cond} as a function of the number of steps in the QPA protocol [analytical results (lines) and Monte Carlo simulation (circles)]. For the calculation, one- and two-qubit white noise with a noise fidelity of 97% has been assumed. The Monte Carlo simulation was started with 10^7 pairs; the numbers indicate how many pairs are left after each step of the purification protocol. This decreasing number is the reason for the increasing fluctuations around the analytical curves.

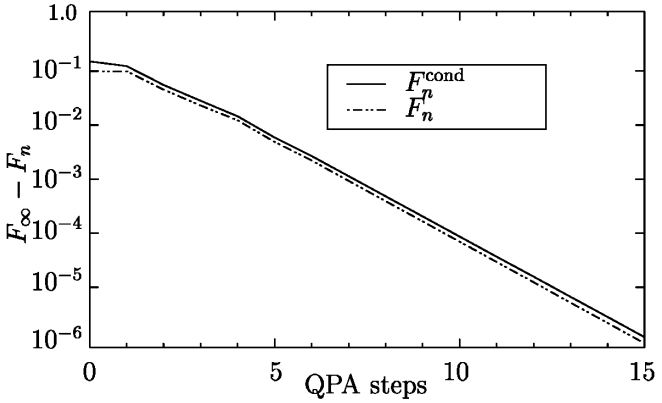

FIG. 2. $F_\infty - F_n$ and $1 - F_n^{\mathrm{cond}}$ plotted logarithmically against the purification step n. The parameters are the same as in Fig. 1.

Our results imply that the error flags and the states of the subensembles become *strictly correlated* during execution of the purification protocol: The subensemble (ij) ends in the state $|\mathcal{B}_{ij}\rangle$. In other words, the little demon has acquired *complete knowledge* about the states of all pairs after sufficiently many purifications steps; the system consisting of the pairs and the lab is thus in a pure state. Now the same argument as in [9] applies: a system in a pure state cannot be entangled with any other system—any eavesdropper is factored out, as his or her entanglement with the pairs is lost.

This proof can be extended to more general noise models if a slightly modified protocol is used, where step 1 is repeated after every distillation round [21]. This effectively regularizes any type of local noise process to a process of the type (3) that conserves the Bell diagonality of the ensemble, for which we can apply the lab-demon interpretation [22].

The fact that the security regime of the protocol almost coincides with the purification regime is of strong practical interest because it implies that EPR pairs distributed over long distances with quantum repeaters can be directly used for secure quantum communication [23].

To summarize, Alice and Bob obtain, with the help of a standard entanglement purification protocol, entangled EPR pairs. These pairs have a limited fidelity $F \lesssim F_{\max} < 1$ which depends on the noise introduced by local operations in their laboratory. Alice and Bob may nevertheless use these pairs for secure quantum or classical communication, e.g., teleportation [24] or key distribution. At this stage, no further security tests are necessary. Since we have shown that there exists no residual entanglement with an eavesdropper, they may use all the pairs for the key. While there may be a significant error rate in the message, Alice and Bob are allowed to apply classical error correction to the transmitted message without disclosing any valuable information to Eve.

We thank C. H. Bennett, A. Ekert, L. Hardy, H. Inamori, N. Lütkenhaus, R. Raussendorf, A. Schenzle, and H. Weinfurter for valuable discussions. We are grateful to G. Giedke, N. Lütkenhaus, and H.-K. Lo for constructive remarks on the manuscript. This work has been supported in part by the Schwerpunktsprogramm QIV of the DFG.

[1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1985), pp. 175–179.
[2] A. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[3] D. Mayers, in *Advances in Cryptology-Proceedings of Crypto '96* (Springer-Verlag, New York, 1996), pp. 343–357; see also quant-ph/9802025.
[4] E. Biham *et al.,* in *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing* (ACM Press, New York, 2000), pp. 715–724.
[5] H. Inamori, quant-ph/0008064.
[6] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[7] A. R. Calderbank and P. Shor, Phys. Rev. A **54**, 1098 (1996).
[8] A. M. Steane, Phys. Rev. Lett. **77**, 793 (1996).
[9] D. Deutsch *et al.,* Phys. Rev. Lett. **77**, 2818 (1996).
[10] C. H. Bennett *et al.,* Phys. Rev. Lett. **76**, 722 (1996).
[11] C. H. Bennett *et al.,* Phys. Rev. A **54**, 3824 (1996).
[12] H.-J. Briegel *et al.,* Phys. Rev. Lett. **81**, 5932 (1998).
[13] G. Giedke *et al.,* Phys. Rev. A **59**, 2641 (1999).
[14] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).
[15] For a review, see, e.g., J. Preskill, quant-ph/9712048.
[16] J. I. Cirac and N. Gisin, Phys. Lett. A **229**, 1 (1997).
[17] H. Aschauer and H. J. Briegel, quant-ph/0111066.
[18] While, strictly speaking, this equality holds only for $N \to \infty$, the subsequent arguments also holds for the exact but more complicated form of (2) for finite N.
[19] The hashing protocol usually performs much worse since the noise introduced with every CNOT operation accumulates and rapidly shatters the potential information that could ideally be gained from the parity measurement.
[20] The fact that already the rotations used in steps 1 and 2 will be subject to noise is immaterial. As no measurements are performed, all such noise may be entirely attributed to the channel.
[21] We are grateful to C. H. Bennett for pointing out this possibility.
[22] Here it is, however, required that Alice and Bob are able to perform one-qubit rotations used in step 1 well enough to keep the evolution Bell diagonal.
[23] The relevance of this result is underlined by a recent proposal by Pan *et al.* [25], who describe a scheme of EPP using only optical elements, with which one would be able to reach the desired error threshold.
[24] C. H. Bennett *et al.,* Phys. Rev. Lett. **70**, 1895 (1993).
[25] J.-W. Pan *et al.,* Nature (London) **410**, 1067 (2001).