Security proof of quantum cryptography based entirely on entanglement purification

Hans Aschauer* and Hans J. Briegel†

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

We give a proof that entanglement purification, even with noisy apparatus, is sufficient to disentangle an eavesdropper (Eve) from the communication channel. In the security regime, the purification process factorizes the overall initial state into a tensor-product state of Alice and Bob, on one side, and Eve on the other side, thus establishing a completely private, albeit noisy, quantum communication channel between Alice and Bob. The security regime is found to coincide for all practical purposes with the purification regime of a two-way recurrence protocol. This makes two-way entanglement purification protocols, which constitute an important element in the quantum repeater, an efficient tool for secure long-distance quantum cryptography.

PACS number(s): 03.67.Dd, 03.67.Hk, 03.65.Ta

I. INTRODUCTION

A central problem of quantum communication is how to faithfully transmit unknown quantum states through a noisy quantum channel [1]. While information is sent through such a channel (for example, an optical fiber), the carriers of the information interact with the channel, which gives rise to the phenomenon of decoherence and absorption; an initially pure quantum state becomes a mixed state when it leaves the channel. For quantum communication purposes, it is necessary that the transmitted qubits retain their genuine quantum properties, for example, in form of an entanglement with qubits on the other side of the channel.

There are two well-established methods to deal with the problem of noisy channels. The theory of quantum error correction [2,3] has mainly been developed to make quantum computation possible despite the effects of decoherence and imperfect apparatus. Since data transmission—like data storage—can be regarded as a special case of a computational process, clearly quantum error correction can also be used for quantum communication through noisy channels. An alternative approach, which has been developed roughly in parallel with the theory of quantum error correction, is the purification of mixed entangled states [4–6].

In quantum cryptography [7,8], noise in the communication channel plays a crucial role. In the worst-case scenario, all noise in the channel is attributed to an eavesdropper, who manipulates the qubits in order to gain as much information on their state as possible, while introducing only a moderate level of noise [9–12].

To deal with this situation, two different techniques have been developed. *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 been shown to be technically involved [13–15]. Recently, Shor and Preskill [16] have given a simpler physical proof relating the ideas in Refs. [13,14] to quantum error correcting codes [2] and, equivalently, to one-way entanglement purification protocols [5]. *Quantum privacy amplification* (QPA) [6], on the other hand, employs a two-way entanglement purification recurrence protocol [5] that eliminates any entanglement with an eavesdropper by creating a few perfect Einstein-Podolsky-Rosen (EPR) pairs out of many imperfect (or impure) EPR pairs. The perfect EPR pairs can then be used for secure key distribution in entanglement-based quantum cryptography [6,8,17]. 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 Refs. [18–20], 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 [21].

In this paper, we show that the standard two-way entanglement purification protocol alone, with some minor modifications to accomodate certain security aspects as 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 [22].

In Sec. II we will briefly review the concepts of entanglement purification and of the quantum repeater, and discuss why it is interesting to combine the security features of entanglement purification with the long-distance feature of the quantum repeater. Section III will give the main result of our work: we prove that it is possible to *factor out* an eavesdropper using entanglement purification, even when the apparatus used by Alice and Bob is noisy. One important detail in the proof is the *flag update function*, which we will derive in Sec. IV. We conclude the paper with a discussion in Sec. V.

*Electronic address: Hans.Aschauer@Physik.uni-muenchen.de

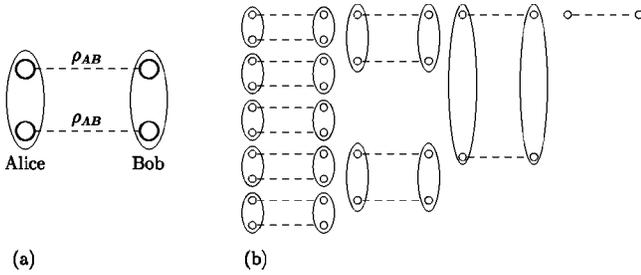†Electronic address: Hans.Briegel@Physik.uni-muenchen.de

FIG. 1. The entanglement purification protocol (a) and the entanglement distillation process (b).

II. ENTANGLEMENT PURIFICATION AND THE QUANTUM REPEATER

A. Entanglement purification

As two-way entanglement purification protocols (2-EPP) play an important role in this paper, we will briefly review one example of a a recurrence protocol that was described in Ref. [6], and called QPA by the authors. It is important to note that we distinguish the entanglement purification *protocol* from the distillation *process*. The first consists of probabilistic local operations (unitary rotations and measurements), where two pairs of qubits are combined, and either one or zero pairs are kept, depending on the measurement outcomes. The latter, on the other hand, is the procedure where the purification protocol is applied to large ensemble of pairs recursively (see Fig. 1).

In the quantum privacy amplification 2-EPP, two pairs of qubits, shared by Alice and Bob, are considered to be in the state $\rho_{A_1B_1} \otimes \rho_{A_2B_2}$. Without loss of generality (see later), we may assume that the state of the pairs is of the Bell-diagonal form,

$$\rho_{AB} = A|\Phi^+\rangle\langle\Phi^+| + B|\Psi^-\rangle\langle\Psi^-| + C|\Psi^+\rangle\langle\Psi^+|$$
$$+ D|\Phi^-\rangle\langle\Phi^-|. \qquad (1)$$

Following Ref. [6], the protocol consists of three steps.

(1) Alice applies to her qubits a $\pi/2$ rotation, U_x, Bob a $-\pi/2$ rotation about the x axis, U_x^{-1}.

(2) Alice and Bob perform the bilateral controlled-NOT (BCNOT) operation

$$\text{BCNOT}_{A_1B_1}^{A_2B_2} = \text{CNOT}_{A_1}^{A_2} \otimes \text{CNOT}_{B_1}^{B_2}$$

on the four qubits.

(3) Alice and Bob measure both qubits of the target pair A_2B_2 of the BCNOT operation in the z direction. If the measurement results coincide, the source pair A_1B_1 is kept, otherwise it is discarded. The target pair is always discarded, as it is projected onto a product state by the bilateral measurement.

By a straigtforward calculation, one gets the result that the state of the remaining pair is still a Bell-diagonal state, with the diagonal coefficients [6]

$$A' = \frac{A^2 + B^2}{N}, \quad B' = \frac{2CD}{N},$$

$$(2)$$

$$C' = \frac{C^2 + D^2}{N}, \quad D' = \frac{2AB}{N},$$

and the normalization coefficient $N = (A+B)^2 + (C+D)^2$, which is the probability that Alice's and Bob's measurement results in step 3 coincide. Note that, up to the normalization, these recurrence relations are a quadratic form in the coefficients A, B, C, and D. These relations allow for the following interpretation [which can be used to obtain the relations (2) in the first place]. As all pairs are in the Bell-diagonal state (1), one can interpret A, B, C, and D as the relative frequencies with which the states $|\Phi^+\rangle, |\Psi^-\rangle, |\Psi^+\rangle$, and $|\Phi^-\rangle$, respectively, appear in the ensemble. By looking at Eq. (2) one finds that the result of combining two $|\Phi^+\rangle$ or two $|\Psi^-\rangle$ pairs is a $|\Phi^+\rangle$ pair, combining a $|\Psi^+\rangle$ and a $|\Phi^-\rangle$ (or vice versa) yields a $|\Psi^-\rangle$ pair, and so on. Combinations of A, B, C, and D that do not occur in Eq. (2), namely, AC, AD, BC, and BD, are "filtered out," i.e., they give different measurement results for the bilateral measurement in step 3 of the protocol. We will use this way of calculating recurrence relations for more complicated situations later.

Numerical calculations [6] and, later, an analytical investigation [23] have shown that for all initial states (1) with $A > 1/2$, the recurrence relations (2) approach the fixpoint $A = 1, B = C = D = 0$; this means that given a sufficiently large number of initial pairs, Alice and Bob can distill asymptotically pure EPR pairs.

B. Entanglement purification with noisy apparatus and the quantum repeater

Under realistic conditions, the local operations (quantum gates, measurements) themselves, which constitute a purification protocol, will never be perfect and thus introduce a certain amount of noise to the ensemble when they are applied by Alice and Bob. The following questions then arise. How does a protocol perform under the influence of local noise? How robust is it and what is the threshold for purification? These questions have been dealt with in Refs. [18–20]. The main results are, in brief, that for a finite level of local noise, there is a maximum achievable fidelity $F_{\max} < 1$ beyond which purification is not possible. Similarly, the minimum required fidelity $F_{\min} > 1/2$ for purification has increased with respect to the ideal protocol [4]. The purification regime $[F_{\min}, F_{\max}][1/2,1]$ has thus become smaller compared to the noiseless case. With an increasing noise level, the size of the purification regime shrinks until, at the purification threshold, $F_{\min}$ and $F_{\max}$ coincide and the protocol breaks down. At this point, the noise of the local operations corresponds to a loss of information that is larger than the gain of information by a distillation step in the ideal case.

For a moderate noise level (of the order of a few percent for the recurrence protocols of Refs. [4,6]), entanglement purification remains an efficient tool for establishing high-fidelity (although not perfect) EPR pairs, and thus for quantum communication over distances of the order of the coherence length of a noisy channel. The restriction to the coherence length is due to the fact that the fidelity of the initial ensemble needs to be above the value $F_{\min}(> 1/2)$.

Long-distance quantum communication describes a situation where the length of the channel connecting the parties is typically much longer than its coherence length and absorption length. As the depolarization errors and the absorption losses scale exponentially with the length of the channel, one cannot send qubits directly through the channel.

To solve this problem, there are two solutions known. The first is to treat quantum communication (QC) as a (very simplistic) special case of quantum computation. The methods of fault tolerant quantum computation [24,25] and quantum error correction could then be used for the communication task. An explicit scheme for data transmission and storage has been discussed by Knill and Laflamme [26], using the method of concatenated quantum coding. While this idea shows that it is *in principle* possible to get polynomial or even polylogarithmic [27–29] scaling in quantum communication, it has an important drawback: long-distance quantum communication using this idea is as difficult as fault tolerant quantum computation, despite the fact that *short* distance QC is (from a technological point of view) already ready for practical use.

The other solution for the long-distance problem is the entanglement based quantum repeater [18,19] with two-way classical communication. It employs both entanglement purification [4–6] and entanglement swapping [30–32] in a metaprotocol, the nested two-way entanglement purification protocol (NEPP). The apparatus used for quantum operations in the NEPP tolerates noise on the (sub) percent level. As this tolerance is two orders of magnitude less restrictive than for fault tolerant quantum computation, it seems to make the quantum repeater a promising concept also for practical realization in the future. Please note that the quantum repeater has been designed not only to solve the problem of *decoherence*, but also of *absorption*. For the latter, the possiblity of quantum storage is required at the repeater stations. An explicit implementation that takes into account absorption is given by the photonic channel of Refs. [33,34] (see also Ref. [35]).

C. The quantum repeater and quantum privacy amplification

The aim of this paper, as mentioned in the Introduction, is to show that entanglement distillation using realistic apparatus is sufficient to create *private entanglement* [36] between Alice and Bob, i.e., pairs of entangled qubits of which Eve is guaranteed to be disentangled even though they are not pure EPR pairs. If these pairs are used to teleport quantum information from Alice to Bob, they can be regarded as a *noisy but private quantum channel*.

This will also prove the security of quantum communication using the entanglement-based quantum repeater, since it is only necessary to consider the outermost entanglement purification step in the NEPP, which is performed by Alice and Bob exclusively, i.e., without the support of the parties at the intermediate repeater stations. In particular, it is not necessary to analyze the effect of noisy Bell measurements on the security. In the worst-case scenario, Alice and Bob assume that all repeater stations are completely under Eve's control, anyway. For this reason, Alice and Bob are not allowed to make assumptions on the method how the pairs have been distributed.

The role of the quantum repeater in the *security* proof is thus the following. It tells us that it is possible to distribute EPR pairs of high fidelity over arbitrary distances (with polynomial overhead), given that the noise level of the apparatus (or operations) used in the entanglement purification is below a certain (subpercent) level. The noise in the apparatus will reflect itself in the fact that the final distributed pairs between Alice and Bob are also imperfect (i.e., not pure Bell states), and so the question arises whether these imperfect pairs can be used for, e.g., *secure* key distribution. The answer is yes. Since the security regime practically coincides with the purification regime (see Sec. III D), quantum communication is guaranteed to be secure whenever the noise level of the local operations is in the operation regime of the quantum repeater.

III. FACTORIZATION OF EVE

In this section we will show that 2-EPP with noisy apparatus is sufficient to factor out Eve in the Hilbert space of Alice, Bob, their laboratories, and Eve. For the proof, we will first introduce the concept of the lab demon as a simple model of noise. Then we will consider the special case of binary pairs, where we have obtained analytical results. Using the same techniques, we generalize the result to the case of Bell-diagonal ensembles. To conclude the proof, we show how the most general case of ensembles, described by an arbitray entangled state of all the qubits on Alice's and Bob's side, can be reduced to the case of Bell-diagonal ensembles.

A. The effect of noise

In this section we will answer the following question. What is the effect of an error, introduced by some noisy operation at a given point of the distillation process? We restrict our attention to the following type of noise.

(1) It acts locally, i.e., the noise does not introduce correlations between remote quantum systems.

(2) It may introduce correlations between quantum systems on which a joint unitary operation is performed, e.g., a controlled-NOT operation may be accompanied by correlated two-qubit noise.

(3) It is memoryless, i.e., on a time scale imposed by the sequence of steps in a given protocol, there are no correlations between the ''errors'' that occur at different times.

The action of noisy apparatus on a quantum system in state $\rho \in \mathcal{B}(\mathcal{H})$ can be formally described by some trace conserving, completely positive map. Any such map can be written in the operator-sum representation [37,1],

$$\rho \rightarrow \sum_i A_i \rho A_i^\dagger, \tag{3}$$

with linear operators A_i, that fulfill the normalization condition $\Sigma_i A A^\dagger = \mathbf{1}$. The operators A_i are the so-called *Kraus operators* [37].

As we have seen above, in the purification protocol the controlled-NOT operation, which acts on two qubits a_1 and a_2, plays an important role. For that reason, it is necessary to consider noise that acts on a two-qubit Hilbert space $\mathcal{H} = \mathbb{C}^2_{a_1} \otimes \mathbb{C}^2_{a_2}$. Equation (3) describes the most general nonselective operation that can, in principle, be implemented. For technical reasons, however, we restrict our attention to the case that the Kraus operators are proportional to products of Pauli matrices. The reason for this choice is that Pauli operators map Bell states onto Bell states, which will allow us to introduce the very useful concept of *error flags* later.

In the case of entanglement purification, the qubits a_1 and a_2 belong to Alice. On the other hand, we can only describe the state of the pairs if we take Bob's degrees of freedom into account. For that reason, we denote these degrees of freedom by an ellipsis $(\cdots)$. Thus, for noise in Alice's apparatus, Eq. (3) can then be written as

$$\rho_{a_1 a_2 \ldots} \rightarrow \sum_{\mu,\nu=0}^{3} f_{\mu\nu} \sigma_\mu^{(a_1)} \sigma_\nu^{(a_2)} \rho_{a_1 a_2 \ldots} \sigma_\mu^{(a_1)} \sigma_\nu^{(a_2)}, \quad (4)$$

with the normalization condition $\Sigma_{\mu,\nu=0}^{3} f_{\mu\nu} = 1$. $\sigma_0 = id$ denotes the identity, and $\sigma_1, \sigma_2,$ and σ_3 are the usual Pauli–operators. A similar expresion exist for noise in Bob's laboratory. Note that Eq. (4) includes, for an appropriate choice of the coefficients $f_{\mu\nu}$, the one- and two-qubit depolarizing channel and combinations thereof, as studied in Refs. [18,19]; but it is more general. Below, we will refer to these special Kraus operators as *error operators*.

The proof can be extended to more general noise models if a slightly modified protocol is used, where the twirl operation of step 1 is repeated after every distillation round [38]. The concatenated operation, which consists of a general noisy operation followed by this *regularization* operation, is Bell diagonal, i.e., it maps Bell-diagonal states onto Bell-diagonal states, but since it maps *all* states to a Bell-diagonal state, it clearly cannot be written in the form (4). However, for the purpose of the proof, it is in fact only necessary that the concatenated map restricted to the space of all Bell-diagonal ensembles can be written in the form (4); we call such a map a *restricted Bell-diagonal map*. Clearly, not all restricted Bell-diagonal maps are of the form (4), which can be seen by considering a map that maps any Bell-diagonal state to a pure Bell state. Such a map could, however, not be implemented locally. Thus the question remains whether a restricted Bell-diagonal map that can be implemented locally can be written in the form (4). Though we are not aware of a formal proof of such a theorem, we conjecture that it holds true: the reduced density operator of each qubit must remain in the maximally mixed state, which is indeed guaranteed by a mixture of unitary rotations. We also have numerical evidence that supports this conjecture. Note that in the case of such an active regularization procedure, it is important that the Pauli rotations in step 1 can be performed well enough

to keep the evolution Bell diagonal. This is, however, not a problem, since Alice and Bob are able to propagate the Pauli rotations through the unitary operations of the EPP, which allows them to perform the rotations just before a measurement, or, equivalently, to rotate the measurement basis. This is similar to the concept of error correctors (where the error consists in *omitting* a required Pauli-operation), as described in Sec. IV A, and to the by-product matrix formalism developed in Ref. [39].

The coefficients $f_{\mu\nu}$ in Eq. (4) can be interpreted as the joint probability that the Pauli rotations σ_μ and σ_ν occur on qubits a_1 and a_2, respectively. For pedagogical purposes we employ the following interpretation of Eq. (4). Imagine that there is a (ficticious) little demon in Alice's laboratory—the "lab demon"—which applies in each step of the distillation process randomly, according to the probability distribution $f_{\mu\nu}$, the Pauli rotation σ_μ and σ_ν to the qubits a_1 and a_2, respectively. The lab demon summarizes all relevant aspects of the lab degrees of freedom involved in the noise process.

Noise in Bob's laboratory, can, as long as we restrict ourselves to Bell-diagonal ensembles, be attributed to noise introduced by Alice's lab demon, without loss of generality; this is, however, not a crucial restriction, as we will show in Sec. III E. It is also possible to think of a second lab demon in Bob's lab who acts similarly to Alice's lab demon. This would not affect the arguments employed in this paper.

The lab demon does not only apply rotations randomly, he also maintains a list in which he keeps track of which rotation he has applied to which qubit pair in which step of the distillation process. What we will show in the following section is that, from the mere content of this list, the lab demon will be able to extract—in the asymptotic limit—full information about the state of each residual pair of the ensemble. This will then imply that, given the lab demons knowledge, the state of the distilled ensemble is a tensor product of pure Bell states. Furthermore, Eve cannot have information on the specific sequence of Bell pairs (beyond their relative frequencies)—otherwise she would also be able to learn, to some extent, at which stage the lab demon has applied which rotation.

From that it follows that Eve is *factored out*, i.e., the overall state of Alice's, Bob's and Eve's particles is described a density operator of the form

$$\rho_{ABE} = \left(\sum_{i,j=0}^{1} f^{(i,j)} |\mathcal{B}_{i,j}\rangle_{AB} \langle \mathcal{B}_{i,j}| \right) \otimes \rho_E, \quad (5)$$

where $\Sigma_{i,j} f^{(i,j)} = 1$, and $\mathcal{B}_{i,j}$ describe the four Bell states as defined in Sec. III E.

Note that the lab demon was only introduced for pedagogical reasons. In reality, there will be other mechanisms of noise. However, all physical processes that result in the same completely positive map (4) are equivalent, i.e., cannot be distinguished from each other if we only know how they map an input state ρ_i onto an output state ρ_f. In particular, the processes must lead to the same level of security (regardless of whether or not error flags are measured or calculated by anybody): otherwise they would be distinguishable.

In order to separate conceptual considerations from the technical ones and to obtain analytical results, we will first concentrate on the special case of binary pairs and a simplified error model. After that, we generalize the results to *any* initial state.

B. Binary pairs

In this section we restrict our attention to pairs in the state

$$\rho_{AB} = A|\Phi^+\rangle_{AB}\langle\Phi^+| + B|\Psi^+\rangle_{AB}\langle\Psi^+|, \quad (6)$$

and to errors of the form

$$\rho_{AB}^{(1)}\otimes\rho_{AB}^{(2)} \rightarrow \sum_{\mu,\nu\in\{0,1\}} f_{\mu\nu} U_\mu^{(1)} U_\nu^{(2)} \rho_{AB}^{(1)}\otimes\rho_{AB}^{(2)} U_\mu^{(1)\dagger} U_\nu^{(2)\dagger}, \quad (7)$$

with $U_0^{(i)} = \mathrm{id}^{(a_i)}$ and $U_1^{(i)} = \sigma_x^{(a_i)}$. Equation (7) describes a *two-bit correlated spin-flip channel*. The indices 1 and 2 indicate the source and target bit of the BCNOT operation, respectively. It is straightforward to show that, using this error model in the 2-EPP, binary pairs will be mapped onto binary pairs.

At the beginning of the distillation process, Alice and Bob share an ensemble of pairs described by Eq. (6). Let us imagine that the lab demon attaches one classical bit to each pair, which he will use for bookkeeping purposes. At this stage, all of these bits, which we call "error flags," are set to zero. This reflects the fact that the lab demon has the same *a priori* knowledge about the state of the ensemble as Alice and Bob.

In each purification step, two of the pairs are combined. The lab demon first simulates the noise channel (7) on each pair of pairs by the process described. Whenever he applies a σ_x operation to a qubit, he inverts the error flag of the corresponding pair. Alice and Bob then apply the 2-EPP to each pair of pairs; if the measurement results in the last step of the protocol coincide, the source pair will be kept. Obviously, the error flag of that remaining pair will also depend on the error flag of the the target pair, i.e., the error flag of the remaining pair is a function of the error flags of both "parent" pairs, which we call the *flag update function*. In the case of binary pairs, the flag update function maps two bits (the error flags of *both* parents) onto one bit. In total, there exist 16 different functions $f:\{0,1\}^2\rightarrow\{0,1\}$. From these, the lab demon chooses the logical AND function as the flag update function, i.e., the error flag of the remaining pair is set to "1" if and only if both parent's error flags had the value "1."

After each purification step, the lab demon divides all pairs into two subensembles, according to the value of their error flags. By a straightforward calculation, we obtain for the coefficients A_i and B_i, which completely describe the state of the pairs in the subensemble with error flag i, the following recurrence relations:

$$A_0' = \frac{1}{N}[f_{00}(A_0^2 + 2A_0A_1) + f_{11}(B_1^2 + 2B_0B_1) + f_s(A_0B_1 + A_1B_1 + A_0B_0)],$$

$$A_1' = \frac{1}{N}(f_{00}A_1^2 + f_{11}B_0^2 + f_s A_1B_0),$$

$$\quad (8)$$

$$B_0' = \frac{1}{N}[f_{00}(B_0^2 + 2B_0B_1) + f_{11}(A_1^2 + 2A_0A_1) + f_s(B_0A_1 + B_1A_1 + B_0A_0)],$$

$$B_1' = \frac{1}{N}(f_{00}B_1^2 + f_{11}A_0^2 + f_s B_1A_0),$$

with $N = (f_{00}+f_{11})[(A_0+A_1)^2 + (B_0+B_1)^2] + 2f_s(A_0+A_1)(B_0+B_1)$ and $f_s = f_{01}+f_{10}$.

For the case of uncorrelated noise, $f_{\mu\nu} = f_\mu f_\nu$, we obtain the following analytical expression for the fixpoints of the map (8):

$$A_0^\infty = \frac{1}{2}\pm\frac{\sqrt{f_0 - 3/4}}{f_0 - 1} \quad \text{or} \quad A_0^\infty = \frac{1}{2},$$

$$A_1^\infty = 0, \quad B_0^\infty = 0, \quad B_1^\infty = 1 - A_0^\infty. \quad (9)$$

In the following, we will concentrate on the nontrivial fixpoint defined by the plus sign in the expression for A_0^∞ above, which is the relevant fixpoint for our discussion. Note that, while Eq. (9) gives a nontrivial fixpoint of Eq. (8) for $f_0 \geq 3/4$, this does not imply that this fixpoint is an attractor. In order to investigate the attractor properties, we calculate the eigenvalues of the matrix of first derivatives,

$$M_D = \begin{pmatrix} \dfrac{\partial A_0'}{\partial A_0} & \cdots & \dfrac{\partial B_1'}{\partial A_0} \\ \vdots & \ddots & \vdots \\ \dfrac{\partial A_0'}{\partial B_1} & \cdots & \dfrac{\partial B_1'}{\partial B_1} \end{pmatrix}\Bigg|_{\text{fixpoint}}. \quad (10)$$

We find that the modulus of the eigenvalues of this matrix is smaller than unity for $f_0^{\text{crit}} = 0.771\,844\,51 < f_0 \leq 1$, which means that in this interval, the fixpoint (9) is also an attractor. This is in excellent agreement with a numerical evaluation of Eq. (8), where we found that $0.771\,82 < f_0^{\text{crit}} < 0.771\,88$.

We have also evaluated Eq. (8) numerically in order to investigate correlated noise (see Fig. 2). Like in the case of uncorrelated noise, we found that the coefficients A_0 and B_1 reach, during the distillation process, some finite value, while the coefficients A_1 and B_0 decrease exponentially fast, whenever the noise level is moderate.

In other words, both subensembles, characterized by the value of the respective error flags, approach a pure state asymptotically. The pairs in the ensemble with error flag "0" are in the state $|\Phi^+\rangle$, while those in the ensemble with error flag "1" are in the state $|\Psi^+\rangle$.
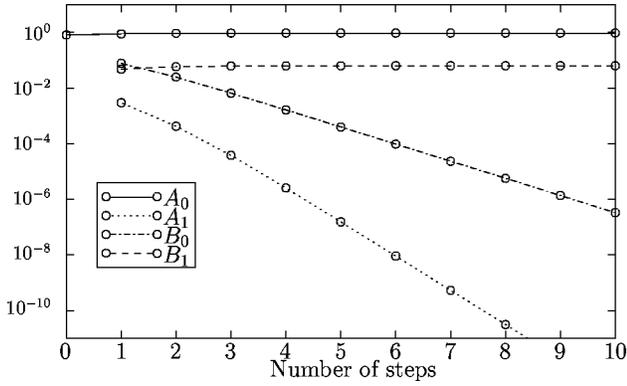
FIG. 2. The evolution of the four parameters A_0, A_1, B_0, and B_1 in the security regime. Note that both A_1 and B_0 decrease exponentially fast in the number of steps. The initial fidelity was 80%, and the values of the noise parameters were $f_{00} = 0.8575$, $f_{01} = f_{10} = f_{11} = 0.0475$.

1. A map of the fixpoints

In Fig. 3, the values of A_0^∞, A_1^∞, B_0^∞, B_1^∞, and $F^{\mathrm{cond},\infty}$ have been plotted as a function of the noise parameter f_0. Most interesting in this graph is the shape of the curve representing the conditional fidelity. For all noise parameters $f_0 \leq 0.75$, the conditional fidelity reaches at the fixpoint the value 0.5, while for noise parameters $f_0 \geq 0.771\,844\,51$, the conditional fidelity reaches unity. In the intermediate regime $(0.75 < f_0 < 0.771\,844\,51)$, the curve can be fitted by a square-root function $F^{\mathrm{cond}}(f_0) = 0.5 + 3.4\sqrt{f_0 - 0.75}$.

The emergence of the intermediate regime of noise parameters, where the 2-EPP is able to purify and the lab demon does not gain full information on the state of the pairs is somewhat surprising and shows that the factorization of the eavesdropper is by no means a trivial consequence of (noisy) EPP. From a mathematical point of view, it is consistent with the finding after Eq. (10).
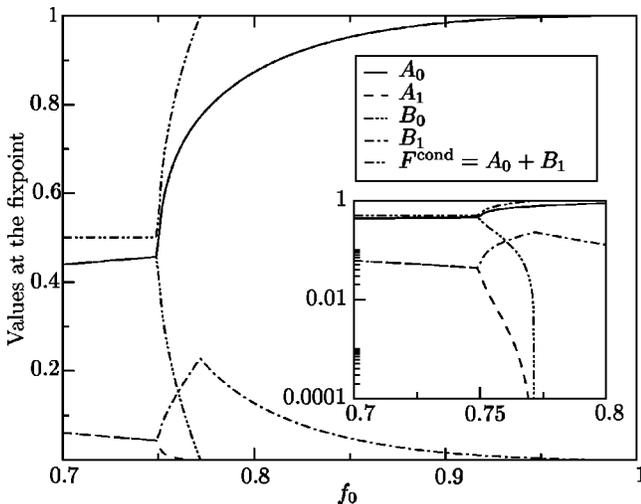

FIG. 3. The values of A_0, A_1, B_0, B_1, and F^{cond} at the fixpoint as a function of the noise parameter f_0.
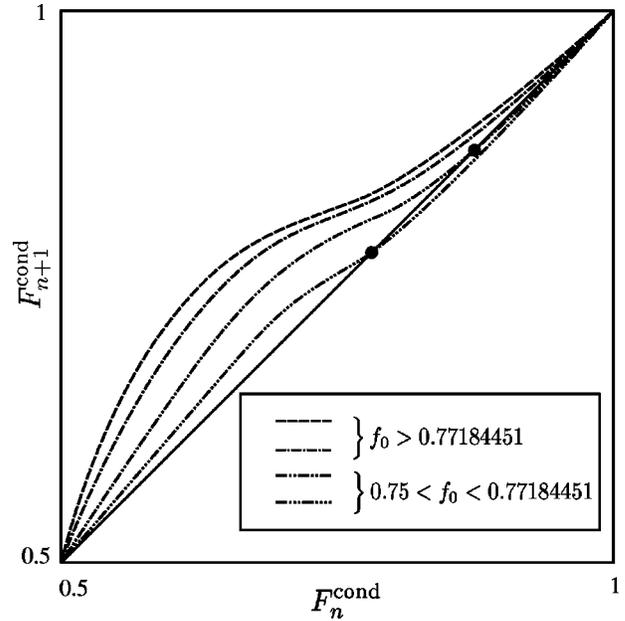

FIG. 4. Illustration of the purification curve for various noise levels f_0. In order to make the point clear, the effect has been strongly overdrawn. See text.

2. The purification curve

To understand the emergence of the intermediate regime better, we have plotted the purification curve for binary pairs, i.e., the $F_n^{\mathrm{cond}} - F_{n+1}^{\mathrm{cond}}$ diagram. A problem with this diagram is that the state of the pairs is specified by three independent parameters $(A_0, A_1, B_0, B_1$ minus normalization), so that such plots can only show a specific section through the full parameter space. Below we explain in detail how these sections have been constructed. Figure 4 shows an overdrawn illustration of what we found: for noise parameters close to the purification threshold, the purification curves have a point of inflection. If the noise level increases (i.e., f_0 decreases), the curves are quasi "pulled-down." For $f_0 = 0.771\,844\,51$, the slope of the purification curve at the fixpoint $F^{\mathrm{cond}} = 1$ equals unity. If we further decrease f_0, the
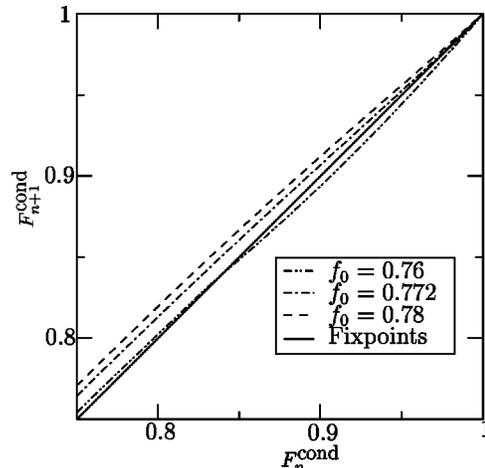

FIG. 5. Actual data from which Fig. 4 has been inferred.

fixpoint is no longer an attractor, but due to the existence of the point of inflection, a new attractive fixpoint appears.

To obtain the one-parametric curves shown in Fig. 5, we used the following technique. Starting with the point $(A_0,A_1,B_0,B_1)^{n=0}=(0.6,0,0.4,0)$, we calculated $(A_0,A_1,B_0,B_1)^{n=1}$ by applying the recursion relations (8) once. The points on the straight line in parameter space connecting these two points have then been used as input values for the map given by the nth power of Eq. (8). For the plot, the resulting curve segments have been concatenated. This procedure has been repeated for all noise parameters f_0 that are specified in Fig. 5. Note that at the critical value $f_0^{\text{crit}} = 0.771\,844\,51$, the number of iterations required to reach any ϵ environment of the fixpoint *diverges*. This fact will later be discussed in a more general case, see Fig. 9.

To conclude this section, we summarize. For all values $0.771\,844\,51 \equiv f_0^{\text{crit}} \leq f_0 \leq 1$ the 2-EPP purifies and at the same time any eavesdropper is factored out. In a small interval, $0.75 < f_0 < f_0^{\text{crit}} \equiv 0.771\,844\,51$, just above the threshold of the purification protocol, the conditional fidelity does not reach unity, while the protocol is in the purification regime. Even though this interval is small and of little practical relevance (for these values of f_0 we are already out of the repeater regime [18] and purification is very inefficient), its existence shows that the process of factorization is not trivially connected to the process of purification.

C. Bell-diagonal initial states

Now we want to show that the same result is true for arbitrary Bell-diagonal states [Eq. (1)] and for noise of the form (4). The procedure is the same as in the case of binary pairs; however, a few modifications are required.

In order to keep track of the four different error operators σ_μ in Eq. (4), the lab demon has to attach two classical bits to each pair; let us call them the phase error bit and amplitude error bit. Whenever a $\sigma_x(\sigma_z,\sigma_y)$ error occurs, the lab demon inverts the error amplitude bit (error phase bit, both error bits). To update these error flags, he uses the update function given in Table I. The physical reason for the choice of the flag update function will be given in the following section.

Here, the lab demon divides all pairs into four subensembles, according to the value of their error flag. In each of the subensembles the pairs are described by a Bell diagonal density operator, like in Eq. (1), which now depends on the subensemble. That means, in order to completely specify the state of all four subensembles, there are 16 real numbers $A^{ij},B^{ij},C^{ij},D^{ij}$ with $i,j \in \{0,1\}$ required, for which one obtaines recurrence relations of the form

$$A_n^{(00)} \to A_{n+1}^{(00)}(A_n^{(00)},A_n^{(01)}, \ldots, D_n^{(11)}),$$

$$A_n^{(01)} \to A_{n+1}^{(01)}(A_n^{(00)},A_n^{(01)}, \ldots, D_n^{(11)}),$$

$$\vdots \tag{11}$$

$$D_n^{(11)} \to D_{n+1}^{(11)}(A_n^{(00)},A_n^{(01)}, \ldots, D_n^{(11)}).$$

TABLE I. The value (phase error, amplitude error) of the updated error flag of a pair that is kept after a 2-EPP step, given as a function of the error flags of P_1 and P_2 (left to right and top to bottom, respectively).

	(00)	(01)	(10)	(11)
(00)	(00)	(00)	(00)	(10)
(01)	(00)	(01)	(11)	(00)
(10)	(00)	(11)	(01)	(00)
(11)	(10)	(00)	(00)	(00)

These generalize the recurrence relations (8) for the case of binary pairs, and the relations (2) for the case of noiseless apparatus.

Like the recurrence relations (2) and (8), respectively, these relations are (modulo normalization) quadratic forms in the 16 state variables $\vec{a} = (A^{(00)},A^{(00)}, \ldots, D^{(11)})^T$, with coefficients that depend on the error parameters $f_{\mu\nu}$ only. In other words, Eq. (11) can be written in the more compact form

$$\vec{a}_j' = \vec{a} M_j \vec{a}^T, \tag{12}$$

where, for each $j \in \{1, \ldots, 16\}$, M_j is a real 16×16 matrix whose coefficients are polynomials in the noise parameters $f_{\mu\nu}$.

D. Numerical results

The 16 recurrence relations (11) imply a reduced set of four recurrence relations for the quantities $A_n = \Sigma_{ij} A_n^{(ij)}, \ldots, D_n = \Sigma_{ij} D_n^{(ij)}$ that describe the evolution of the total ensemble (that is, the *blend* [40] of the four subensembles) under the purification protocol. Note that these values are the only ones that are known and accessible to Alice and Bob, as they have no knowledge of the values of the error flags. It has been shown in Ref. [18] that under the action of the noisy entanglement distillation process, these quantities converge towards a fixpoint $(A_\infty,B_\infty,C_\infty,D_\infty)$, where $A_\infty = F_{\max}$ is the maximal attainable fidelity [19].

Figure 6 shows for typical initial conditions the evolution of the 16 coefficients $A_n^{(00)} \cdots D_n^{(11)}$. They are organized in a 4×4 matrix, where one direction represents the Bell state of the pair, and the other indicates the value of the error flag. The figure shows the state (a) at the beginning of the entanglement purification procedure, (b) after few purification steps, and (c) at the fixpoint. As one can see, initially all error flags are set to zero and the pairs are in a Werner state with a fidelity of 70%. After a few steps, the population of the diagonal elements starts to grow; however, none of the elements vanishes. At the fixpoint, all off-diagonal elements vanish, which means that there are *strict correlations* between the states of the pairs and their error flags.

In order to determine how fast the state converges, we investigate two important quantities: the first is the fidelity $F_n \equiv A_n$, and the second is the *conditional fidelity* $F_n^{\text{cond}} \equiv A_n^{(00)} + B_n^{(11)} + C_n^{(01)} + D_n^{(10)}$. Note that the first quantity is
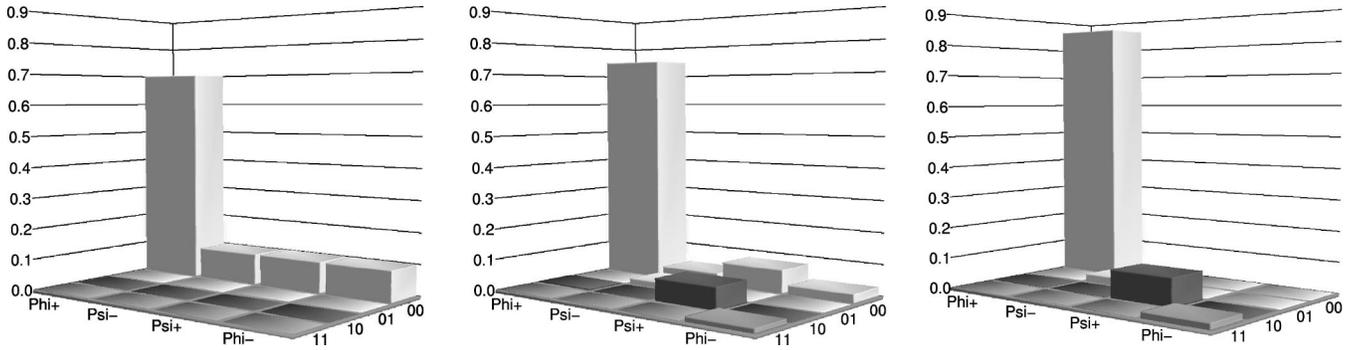
FIG. 6. Typical evolution of the extended state under the purification protocol for the noise parameters $f_{00} = 0.839\,81$, $f_{0j} = f_{i0} = 0.021\,131$, and $f_{ij} = 0.003\,712$ for $i, j \in \{1, 2, 3\}$. This corresponds to a combination of one- and two-qubit white noise, as studied in Refs. [18,19], with noise parameters $p_1 = 0.92$ and $p_2 = 0.9466$, considering noise in Alice's lab only, or $p_1 = 0.9592$ and $p_2 = 0.973$, considering noise in Alice's and Bob's laboratory. We have chosen these values for didactical reasons, in order to make the effect more visible.

the sum over the four $|\Phi^+\rangle$ components in Fig. 6, while the latter is the sum over the four diagonal elements. The conditional fidelity is the fidelity that Alice and Bob would assign to the pairs if they knew the values of the error flags, i.e.,

$$F_n^{\text{cond}} = \sum_{i,j} \langle \Phi^+ | \sigma_{i,j} \rho_{i,j} \sigma_{i,j} | \Phi^+ \rangle, \qquad (13)$$

where $\rho_{i,j}$ is the non-normalized state of the subensemble of the pairs with the error flag (i, j). For convenience, we use the phase- and spin-flip bits i and j as indices for the Pauli matrices, i.e., $\sigma_{00} = \text{id}, \sigma_{01} = \sigma_x, \sigma_{11} = \sigma_y, \sigma_{10} = \sigma_z$. We will utilize the advantages of this notation in Sec. IV.

The results that we obtain are similar to those for the binary pairs. We can again distinguish three regimes of noise parameters $f_{\mu\nu}$. In the high-noise regime (i.e., small values of f_{00}), the noise level is above the threshold of the 2-EPP and both the fidelity F and the conditional fidelity F^{cond} converges to the value 0.25. In the low-noise regime (i.e., large values of f_{00}), F converges to the maximum fidelity $F_{\max}$

and F^{cond} converges to unity (see Fig. 7). This regime is the *security regime*, where we know that secure quantum communication is possible. Like for binary pairs, there exists also an intermediate regime, where the 2-EPP purifies but F^{cond} does not converge to unity. For an illustration, see Fig. 8. Note that the size of the intermediate regime is very small, compared to the security regime. Whether or not secure quantum communication is possible in this regime is unknown. However, the answer to this question is irrelevant for all practical purposes, because in the intermediate regime the distillation process converges very slowly, as shown in Fig. 9. In fact, the divergent behavior of the process near the critical points has features remnant of a phase transition in statistical mechanics.

To estimate the size of the intermediate regime and to compare it to the case of binary pairs (Fig. 3), we consider the case of one-qubit white noise, i.e., $f_{\mu\nu} = f_\mu f_\nu$ and $f_1 = f_2 = f_3 = (1 - f_0)/3$. Here, this regime is known to be bounded by

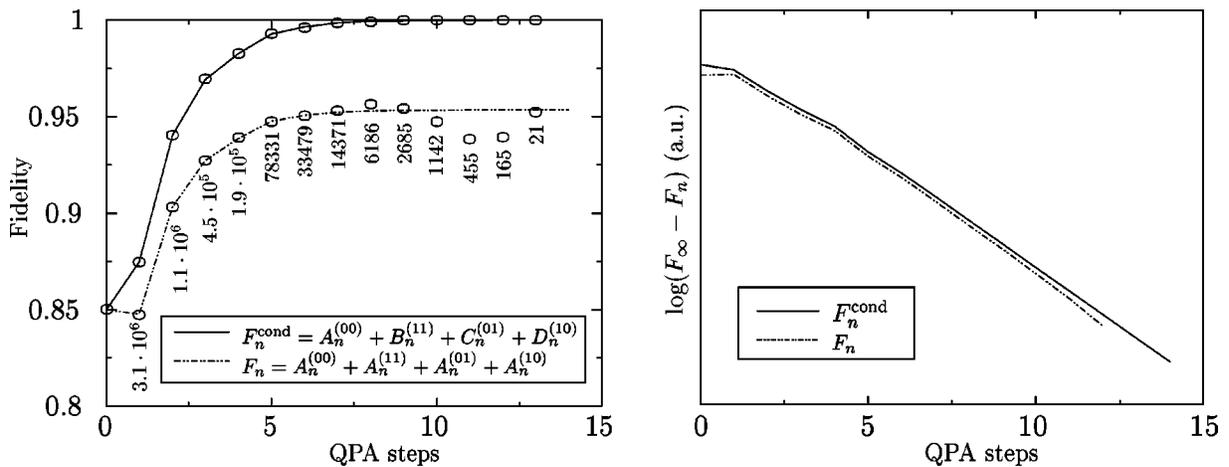$$0.8983 < f^{\text{crit,lower}} < f_0 < f^{\text{crit,upper}} < 0.8988.$$

FIG. 7. The fidelities F and F^{cond} as a function of the number of steps in the security regime of the entanglement distillation process [analytical results (lines) and Monte Carlo simulation (circles)]. The noise parameters for this plot were $f_{00} = 0.912\,791\,20$, $f_{0j} = f_{i0} = 0.011\,389\,6$, and $f_{ij} = 0.002\,096\,8$ for $i, j \in \{1, 2, 3\}$, corresponding to white noise with noise parameters $p_1 = 0.96$ and $p_2 = 0.968$ (see Fig. 6). The Monte Carlo simulation was started with $100\,000\,00$ pairs; the numbers indicate how many pairs are left after each step of the distillation process. This decreasing number is the reason for the increasing fluctuations around the analytical curves.
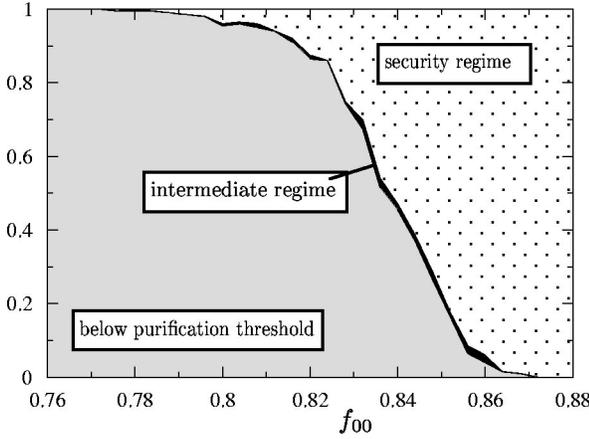
FIG. 8. The size and location of the three regimes of the distillation process. For fixed values of f_{00}, the remaining 15 noise parameters $f_{\mu\nu}$ have been chosen at random. Plotted is the relative frequency of finding the noise parameters in any of the three regimes as a function of f_{00}.

Note that the size of the intermediate regime is much smaller than in the case of binary pairs.

Regarding the efficiency of the distillation process, it is an important question how many initial pairs are needed to create one pair with fidelity F^{cond}, corresponding to the *security parameter* $\epsilon \equiv 1 - F^{\text{cond}}$. Both the number of required initial pairs (resources) and the security parameter scale exponentially with the number of distillation steps, so that we expect a polynomial relation between the resources and the security parameter ϵ. Figure 10 confirms this relation in a log-log plot for different noise parameters. The straight lines are fitted polynomial relations; the fit region is indicated by the lines themselves.
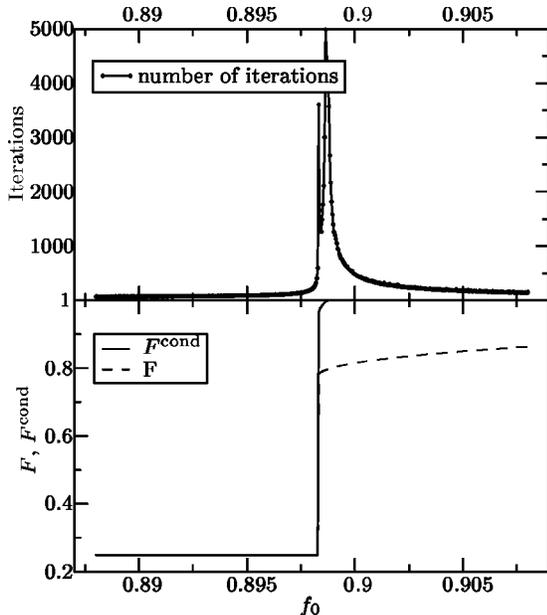

FIG. 9. The effect of one-qubit white noise on the fidelity F, the conditional fidelity F^{cond}, and the number of iterations required for the convergence up to an uncertainty $\epsilon = 10^{-12}$.
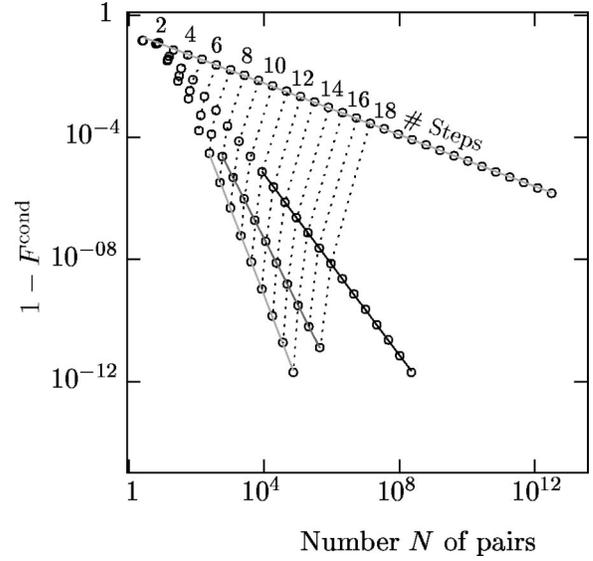

FIG. 10. Number N of pairs needed to create one pair with conditional fidelity F^{cond}. The initial state of the pairs was of the Werner type with fidelity $F_0 = 85\%$. One- and two-qubit white noises (see Fig. 6) have been assumed with the noise parameters $(p_1, p_2) = (0.9333, 0.9466)$, $(0.9733, 0.9786)$, $(0.9866, 0.9833)$, and $(0.9933, 0.9946)$ (from top to bottom).

E. Non-Bell-diagonal pairs

In the worst-case scenario, Eve generates an ensemble of N qubit pairs, which she distributes to Alice and Bob. For that reason, Alice and Bob are not allowed to make specific assumptions on the state of the pairs. Most generally, the state of the $2N$ qubits, of which Alice and Bob obtain N qubits each, can be written in the form

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

$$\times \langle \mathcal{B}_{\mu_1'}^{(a_1 b_1)} \cdots \mathcal{B}_{\mu_N'}^{(a_N b_N)} |. \tag{14}$$

Here, $|\mathcal{B}_{\mu_j}^{(a_j b_j)}\rangle$, $\mu_j = 00, 01, 10, 11$ denote the four Bell states associated with the two particles a_j and b_j and $j = 1, \ldots, N$. Specifically, $|\mathcal{B}_{00}\rangle \equiv |\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$, $|\mathcal{B}_{01}\rangle \equiv |\Psi^+\rangle = (|01\rangle + |01\rangle)/\sqrt{2}$, $|\mathcal{B}_{10}\rangle \equiv |\Phi^-\rangle = (|00\rangle - |11\rangle)/\sqrt{2}$, $|\mathcal{B}_{11}\rangle \equiv |\Psi^-\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$. In general, Eq. (14) will be an entangled state of $2N$ particles, which might moreover be entangled with additional quantum systems in Eve's hands; this allows for the possibility of so-called coherent attacks [41].

Upon reception of all pairs, Alice and Bob apply the following protocol to them. It consists of two steps, pre-1 and pre-2 of "preprocessing," which are followed by the standard purification process described in Sec. II A.

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

Steps 1 and 2 are required in order to treat correlated pairs correctly. Note that steps 1 and 2 would also be required—as "preprocessing" steps—for the ideal distillation process [6], if one requires that the process converges for arbitrary states of the form (14) to an ensemble of pure EPR states. While in Ref. [6] it is possible to check whether or not the process converges to the desired pure state, by measuring the fidelity of some of the remaining pairs, this is not possible when imperfect apparatus is used. Since the maximum attainable fidelity $F_{\max}$ is smaller than unity, there is no known way to exclude the possibility that the nonideal fidelity is due to correlations between the initial pairs. In both steps Alice and Bob discard the information which of the rotations and permutations, respectively, were chosen by their random number generator. Thus they deliberately lose some of the information about the ensemble, which is still available to Eve (as she can eavesdrop the classical information that Alice and Bob exchange to implement step 1). After step 1, their knowledge about the state is summarized by the density operator

$$\widetilde{\rho}_{AB} = \sum_{\mu_1 \cdots \mu_N} p_{\mu_1 \cdots \mu_N} |\mathcal{B}_{\mu_1}^{(a_1 b_1)} \cdots \mathcal{B}_{\mu_N}^{(a_N b_N)}\rangle$$
$$\times \langle \mathcal{B}_{\mu_1}^{(a_1 b_1)} \cdots \mathcal{B}_{\mu_N}^{(a_N b_N)}|, \tag{15}$$

which corresponds to a *classically correlated ensemble* of pure Bell states. Since the purification protocol that they are applying in the following steps maps Bell states onto Bell states, it is statistically consistent for Alice and Bob to assume after step 1 that they are dealing with a (numbered) ensemble of pure Bell states, where they have only limited knowledge about which Bell state a specific pair is in. The fact that the pairs are correlated means that the order in which they appear in the numbered ensemble may have some pattern, which may have been imposed by Eve or by the channel itself. By applying step 2, Alice and Bob (i) deliberately ignore this pattern and (ii) randomize the order in which the pairs are used in the subsequent purification steps [42]. For all statistical predictions made by Alice and Bob, they may consistently describe the ensemble by the density operator [43]

$$\widetilde{\widetilde{\rho}}_{AB} = \left(\sum_{\mu} p_{\mu} |\mathcal{B}_{\mu}\rangle\langle\mathcal{B}_{\mu}| \right)^{\otimes N} \equiv (\rho_{ab})^{\otimes N} \tag{16}$$

in which the p_{μ} describe the probability with which each pair is found in the Bell state $|\mathcal{B}_{\mu}\rangle$. 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 depends on the noise level introduced by their local apparatus. This test can be performed locally by statistical tests on a certain fraction of the pairs.

As Alice and Bob now own an ensemble of Bell diagonal pairs, they may proceed as described in the preceding Sec. II A [recursive application of the steps (1)–(3) described af-

ter Eq. (1)]. However, it is a reasonable question why Eve cannot take advantage of the additional information that she has about the state of the pairs: as she is allowed to keep the information about the twirl operations in steps 1 and 2, from her point of view all the pairs remain in an highly entangled $2N$-qubit state. Nevertheless, all predicions made by Eve must be statistically consistent with the predictions made by Alice and Bob (or, for that matter, their lab demon), which means that the state calculated by Eve must be the same as the state calculated by the lab demon, tracing out Eve's additional information. As the lab demon gets a pure state at the end of the entanglement distillation process, this must also be the result that Eve obtains using her additional information, simply due to the fact that no pure state can be written as a nontrivial convex combination of other states.

IV. HOW TO CALCULATE THE FLAG UPDATE FUNCTION

In this section, we analyze how errors are propagated in the distillation process. As was mentioned earlier, the state of a given pair that survives a given purification step in the distillation process depends on all errors that occured on pairs in earlier steps, which belong to the "family tree" of this pair. We will show that it is possible to summarize the effect of all errors in the family tree of each pair in an error flag, which consists of two classical bits. The values of the error flags can be calculated in a recursive scheme, and we call the recurrence relation the *flag update function*.

Each step of the distillation process consist of a number of unitary operations followed by a measurement, which we treat separately in the following two subsections.

A. Unitary transformations and errors

Consider an error U_{err} (i.e., a random unitary transformation) that is introduced before a unitary transformation U is performed on a state $|\psi\rangle$. Note that, without loss of generality, it is always possible to split up a noisy quantum operation close to a unitary operation U in two parts: first, a noisy operation close to identity, and afterwards the noiseless unitary operation U. For that reason, it only a matter of interpretation whether we think of a quantum operation that is accompanied by noise, e.g., as described by a master equation of the Lindblad form, or of the combination of some noise channel first and the noiseless quantum operation afterwards.

We call a transformation U_{corr} an *error corrector*, if the equation

$$U|\psi\rangle = U_{\text{corr}} U U_{\text{err}} |\psi\rangle \tag{17}$$

holds for all states $|\psi\rangle$. Equation (17) is obviously solved by $U_{\text{corr}} = U U_{\text{err}}^{-1} U^{-1}$.

We want to calculate the error corrector for the Pauli operators and the unitary operation $U_{\text{2-EPP}}$, which consists of the bilateral x rotations and the BC-NOT operation, as described in Sec. II.

In what follows, it is important to note that Pauli rotations and all the unitary operations used in the entanglement puri-

fication protocol map Bell states onto Bell states; it is thus expedient to write the four Bell states as

$$|\mathcal{B}_{ij}\rangle = \frac{1}{\sqrt{2}}(|0j\rangle + (-1)^i|1\bar{j}\rangle), \tag{18}$$

using the *phase bit i* and the *amplitude bit j* with $i,j \in \{0,1\}$ [5], which we have implicitly employed in Eq. (14). In this notation, we get (ignoring global phases): $\sigma_x|\mathcal{B}_{i,j}\rangle = |\mathcal{B}_{i,j\oplus1}\rangle$, $\sigma_y|\mathcal{B}_{i,j}\rangle = |\mathcal{B}_{i\oplus1,j\oplus1}\rangle$, and $\sigma_z|\mathcal{B}_{i,j}\rangle = |\mathcal{B}_{i\oplus1,j}\rangle$, where σ may act on either side of the pair. The $\oplus$ symbol indicates addition modulo 2. Consistent with this notation, σ_x is referred to as the amplitude flip operator, σ_z as the phase flip operator, and σ_y as the phase and amplitude flip operator.

The effect of the bilateral one-qubit rotation in the 2-EPP can be easily expressed in terms of the phase and amplitude bit,

$$U_x^A \otimes U_x^{B-1}|\mathcal{B}_{i,j}\rangle = |\mathcal{B}_{i,j\oplus i}\rangle, \tag{19}$$

and the same holds for the BC-NOT operation,

$$\text{BCNOT}|\mathcal{B}_{i,j}\rangle|\mathcal{B}_{i',j'}\rangle = |\mathcal{B}_{i\oplus i',j}\rangle|\mathcal{B}_{i',j\oplus j'}\rangle. \tag{20}$$

The effect of the unitary part of the 2-EPP onto two pairs in the states $|\mathcal{B}_{i,j}\rangle$ and $|\mathcal{B}_{i',j'}\rangle$ can be written in the form

$$U_{2\text{-EPP}}|\mathcal{B}_{i,j}\rangle|\mathcal{B}_{i',j'}\rangle = |\mathcal{B}_{i\oplus i',i\oplus j}\rangle|\mathcal{B}_{i',i'\oplus j'\oplus i\oplus j}\rangle, \tag{21}$$

where the first and second pair plays the role of the "source" and the "target" pair. Instead of Eq. (21), we will use an even more economic notation of the form $(i,j) \equiv |\mathcal{B}_{i,j}\rangle$. Equation (21) can then be written as

$$(i,j)(i',j') \overset{2-\text{EPP}}{\rightarrow} (i\oplus i',i\oplus j)(i',i'\oplus j'\oplus i\oplus j). \tag{22}$$

It is now straightforward to include the effect of the lab demon, Eq. (4). Applying Pauli rotations σ_{pa} and $\sigma_{p'a'}$ to the pairs before the unitary 2-EPP step ($\sigma_{00}=\text{id}, \sigma_{01}=\sigma_x, \sigma_{11}=\sigma_y, \sigma_{10}=\sigma_z$), we obtain

$$(i,j)(i',j') \overset{\sigma}{\rightarrow} (i\oplus p,j\oplus a)(i'\oplus p',j'\oplus a')$$

$$\overset{2-\text{EPP}}{\rightarrow} (i\oplus i'\oplus p\oplus p',i\oplus j\oplus p\oplus a)$$

$$\times(i'\oplus p',i'\oplus j'\oplus i\oplus j\oplus p'\oplus a'\oplus p\oplus a). \tag{23}$$

Comparing Eq. (22) and Eq. (23), we find that the error corrector for the error operation $\sigma_{p,a} \otimes \sigma_{p',a'}$ is given by

$$U_{\text{corr}} = \sigma_{p\oplus p',p\oplus a} \otimes \sigma_{p',p'\oplus a'\oplus p\oplus a}, \tag{24}$$

independent of the initial state of the pairs. This is the desired result.

B. Measurements and measurement errors

As the 2-EPP does not only consist of unitary transformations but also of measurements, it is an important question whether or not errors can be corrected after parts of the system have been measured, and how we can deal with measurement errors. It is important to note that whether a pair is kept or discarded in the 2-EPP depends on the measurement outcomes. This means that, depending on the level of noise in the distillation process, different pairs may be distilled, each with a different "family tree" of pairs. This procedure is conceptually very different from quantum error correction, in the following sense. In quantum error correction, it is necessary to correct for errors before performing a readout measurement on a logical qubit. Here, the situation is quite different: the lab demon performs all calculations only for bookkeeping purposes. *No* action is taken, and thus *no* error correction is performed, neither by the lab demon, nor by Alice and Bob.

In the analysis of the noisy entanglement distillation process [18,19], not only noisy unitary operations have been taken into account, but also noisy measurement apparatus, which is assumed to yield the correct result with the probability η, and the wrong result with the probability $1-\eta$. Surprisingly, if only the measurements are noisy (i.e., all unitary operations are perfect), the 2-EPP produces *perfect* EPR pairs, as long as the noise is moderate ($\eta > 63.5\%$). The reason for this property lies in the fact that $F=1$ is a fixpoint of the 2-EPP even with noisy measurements. For a physical understanding of this fact, it is useful to note that in the distillation process, while the fidelity of the pairs increases, it becomes more and more unlikely that a pair that should have been discarded is kept due to a measurement error. This means that the increasingly dominant effect of measurement errors is that pairs that should have been kept are discarded. However, this does not decrease the fidelity of remaining pairs, only the efficiency of the protocols is affected.

This fact is essential for our goal to extend the concept of error correctors to the entire 2-EPP, which actually includes measurements. As was shown in Sec. IV A, noise in the unitary operations can be accounted for with the help of error correctors, which can be used to keep track of errors through the entire distillation process; on the other hand, the measurement in the 2-EPP may yield wrong results due to noise that occured in an earlier (unitary) operation. This has, however, the same effect as a measurement error, of which we have seen that it does not jeopardize the entanglement distillation process.

C. The reset rule

From the preceding two sections, one can identify a first candidate for the flag update function. The idea is the following. The error corrector U_{corr} calculated in Sec. IV A describes how errors on the phase bit and amplitude bit are propagated by the 2-EPP. For the lab demon, this means that instead of introducing an error operaton $U_{\text{err}}=\sigma_{p,a}\otimes\sigma_{p',a'}$ *before* the unitary part of the 2-EPP, he could, with the same result, introduce the operation $U_{\text{corr}}^{-1}=U_{\text{corr}}=\sigma_{p\oplus p',p\oplus a} \otimes \sigma_{p',p'\oplus a'\oplus p\oplus a}$ as an error operation *afterwards*.

Let us assume, motivated by the preceding section, that the measurement that follows the unitary operation $U_{2\text{-EPP}}$ does not compromise the concept of error correctors (this assumption will have to be modified later). The lab demon can then consider the error corrector as an recursive update rule for errors on the phase bit and amplitude bit, i.e., for the phase and amplitude error bits that constitute the error flag, in the following way.

At the beginning of the destillation process, the lab demon assigns two classical bits to each of the pairs, both set to the value zero ("0"). Whenever he applies a phase flip or amplitude flip to a given pair, he inverts the first or the second bit of its error flag, respectively. For that reason, we call the two bits the *error phase bit* p_e and the *error amplitude bit* a_e.

If, for a given pair of pairs, the purification is successful, the source pair is kept. The error flag of the source pair is now calculated as a function of the previous error flag of both pairs, using the source-pair part of the error corrector: $(p_e,a_e)(p_e',a_e')\rightarrow(p_e\oplus p_e',p_e\oplus a_e)$.

In any case, the lab demon has to discard the target-pair part of the error corrector, as the target pair is measured and does no longer take part in the distillation process. The knowledge of the error flag of a specific pair implies that the lab demon could undo all errors introduced in the family tree of this pair. For example, if the error flag has the value (i,j), the lab demon could apply the Pauli operator $\sigma_{i,j}$ in order to undo the effect of all errors he introduced up to that point.

It is well known that the noiseless protocol asymptotically produces perfect EPR pairs in the state $\mathcal{B}_{0,0}$. It follows that—in the asymptotic limit—a pair with the error flag (i,j) must be in the state $\mathcal{B}_{i,j}$, i.e., the error flags and the states of the pairs are strictly correlated. This means, if the above assumption was true, then the flag update function would be given by $(p_e,a_e)(p_e',a_e')\rightarrow(p_e\oplus p_e',p_e\oplus a_e)$. However, as we will see, the assumption does not hold; for that reason we call this update function a *candidate* for the flag update function.

The candidate has already the important property that states with perfect correlations between the error flags (i.e., only the coefficients A_{00}, B_{11}, C_{01}, and D_{10} are nonvanishing) are mapped onto states with perfect correlations.

A serious deficiency of the candidate function as specified above is that perfect correlations between flags and pairs are not built up unless they exist from the beginning. By following the distillation process in a Monte Carlo simulation that takes the error flags into account, the reason for this is easy to identify. The population of pairs that carry an amplitude error becomes too large. Now, the amplitude bit (not the amplitude *error* bit) of a target pair is responsible for the coincidence of Alice's and Bob's measurement results; if the amplitude bit has the value zero, the measurement results coincide and the source pair will be kept, otherwise it will be discarded. If the target pair carries an amplitude error, a measurement error will occur, and there are two possibilities: either the source pair will be kept even though it should have been discarded, or *vice versa*, then the source pair will be discarded although it should have been kept. Obviously, the latter case does not destroy the convergence of the entanglement distillation process (but it does have an impact on its

efficiency); as Alice and Bob do not have any knowledge of the error flags, there is nothing that can be done in this case, and both pairs are discarded. The first case is more interesting. It is clear that for pairs with perfectly correlated error flags this case will not occur (due to the perfect correlations the amplitude error bit can only have the value one if the amplitude bit has the value one, which is just the second case). This means that we have the freedom to modify the error flags of the remaining pair *without* losing the property that perfectly correlated states get mapped onto perfectly correlated states. It turns out that *setting both the error amplitude bit and the error phase bit of the remaining pair* to zero (*reset rule*) yields the desired behavior of the flag update function, so that perfect correlations are being built up.

The amplitude error bit of the target pair is given by $p'\oplus a'\oplus p\oplus a$. The flag update function can thus be written as

$$(p,a)(p',a')\rightarrow\begin{cases}(p\oplus p',p\oplus a) & \text{if}\quad p'\oplus a'\oplus p\oplus a=0\\(0,0) & \text{otherwise}\end{cases}.$$
(25)

For convenience, the values of the flag update function are given in Table I.

Note that the reset rule is an *ad hoc* solution: even though the above arguments do not prove that the desired correlations are built up, we could calculate the recurrence relations (11) using the flag update function (25). Analytical considerations in the case of binary pairs with one-qubit noise (see Sec. III B) and numerical iterations of Eq. (11) for all other cases show the desired result, i.e., that strict correlations are in fact built up.

V. DISCUSSION

We have shown in Sec. III, that the two-way entanglement distillation process is able to disentangle any eavesdropper from an ensemble of imperfect EPR pairs distributed between Alice and Bob, even in the presence of noise, i.e., when the pairs can only be purified up to a specific maximum fidelity $F_{\text{max}}<1$. Alice and Bob may use these imperfectly purified pairs as a *secure* quantum communication channel. They are thus able to perform secure quantum communication, and, as a special case, secure classical communication (which is in this case equivalent to a key distribution scheme).

In order to keep the argument transparent, we have considered the case where noise of the form (4) is explicitly introduced by a fictitious lab demon, who keeps track of all error operations and performs calculations. However, using a simple indistinguishability argument (see Sec. III A), we could show that any apparatus with the noise characteristics (4) is equivalent to a situation where noise is introduced by the lab demon. This means that the security of the protocol does not depend on the fact whether or not anybody actually calculates the flag update function. It is sufficient to just use a noisy 2-EPP, in order to get a secure quantum channel.

For the proof, we had to make several assumptions on the

noise that acts in Alice's and Bob's entanglement purification device. One restriction is that we only considered noise that is of the form (4). However, this restriction is only due to technical reasons; we conjecture that our results are also true for most general noise models of the form (3). More generally, a regularization procedure (cf. Sec. III A) can be used to *actively* make any noise Bell-diagonal. We have also implicitly introduced the assumption that the eavesdropper has no additional knowledge about the noise process, i.e., Eve only knows the publicly known noise characteristics (4) of the apparatus. This assumption would not be justified, for example, if the lab demon was bribed by Eve, or if Eve was able to manipulate the apparatus in Alice's and Bob's laboratories, for example, by shining in light from an optical fiber. This concern is not important from a principal point of view, as the laboratories of Alice and Bob are considered secure by assumption. On the other hand, this concern has to be taken into account in a practical implementation.

ACKNOWLEDGMENTS

[1] B. Schumacher, Phys. Rev. A **54**, 2614 (1996).

[2] A. R. Calderbank and P. Shor, Phys. Rev. A **54**, 1098 (1996).

[3] A. M. Steane, Phys. Rev. Lett. **77**, 793 (1996).

[4] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).

[5] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).

[6] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).

[7] 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.

[8] A. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[9] A. K. Ekert, B. Huttner, G. M. Palma, and A. Peres, Phys. Rev. A **50**, 1047 (1994).

[10] C. A. Fuchs and A. Peres, Phys. Rev. A **53**, 2038 (1996).

[11] N. Lütkenhaus, Phys. Rev. A **54**, 97 (1996).

[12] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres, Phys. Rev. A **56**, 1163 (1997).

[13] D. Mayers, in *Advances in Cryptology*, Proceedings of Crypto '96, edited by Neal Koblitz (Springer-Verlag, New York, 1996), pp. 343–357; see also e-print quant-ph/9802025.

[14] E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhurny, in *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing* (ACM Press, New York, 2000), pp. 715–724; e-print quant-ph/9912053.

[15] H. Inamori, e-print quant-ph/0008064.

[16] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[17] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).

[18] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).

[19] W. Dür, H.-J. Briegel, J. I. Cirac, and P. Zoller, Phys. Rev. A **59**, 169 (1999).

[20] G. Giedke, H.-J. Briegel, J. I. Cirac, and P. Zoller, Phys. Rev. A **59**, 2641 (1999).

[21] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).

[22] While it would be interesting to extend our proof to the hashing protocol, we note that for noisy local operations the hashing protocol, which requires Alice and Bob to apply a large number of controlled-NOT operations in every distillation step, usually performs much worse that the recurrence protocols. The reason for this lies in the fact that the noise (i.e., information loss) introduced with every controlled-NOT operation accumulates and rapidly shatters the potential information that could ideally be gained from the parity measurement.

[23] C. Macchiavello, Phys. Lett. A **246**, 385 (1998).

[24] E. Knill, R. Laflamme, and W. Zurek, e-print quant-ph/9610011.

[25] J. Preskill, Proc. R. Soc. London, Ser. A **454**, 365 (1998).

[26] E. Knill and R. Laflamme, e-print quant-ph/9608012.

[27] A. Y. Kitaev, Russ. Math. Surveys **52**, 1191 (1997).

[28] E. Knill, R. Laflamme, and W. Zurek, Science **279**, 342 (1998).

[29] D. Aharonov and M. Ben-Or, e-print quant-ph/9611025.

[30] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).

[31] M. Zukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, Phys. Rev. Lett. **71**, 4287 (1993).

[32] J.-W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **80**, 3891 (1998).

[33] S. J. van Enk, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **78**, 4293 (1997).

[34] S. J. van Enk, J. I. Cirac, and P. Zoller, Science **279**, 205 (1998).

[35] H.-J. Briegel, W. Dür, J. Cirac, and P. Zoller, *The Physics of Quantum Information* (Springer, New York, 2000).

[36] We owe the term *private entanglement* to Charles Bennett.

[37] K. Kraus, Lect. Notes Phys. **190** (1983).

[38] We are grateful to C. H. Bennett for pointing out this possibility.

[39] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).

[40] B.-G. Englert, Z. Naturforsch., A: Phys. Sci. **54**, 11 (1999).

[41] J. I. Cirac and N. Gisin, Phys. Lett. A **229**, 1 (1997).

[42] This will prevent Eve from making use of any possibly prearranged order of the pairs, which Alice and Bob are meant to follow when performing the distillation process.

[43] While, strictly speaking, this equality holds only for $N \rightarrow \infty$, the subsequent arguments also hold for the exact but more complicated form of Eq. (16) for finite N.