Locking Entanglement with a Single Qubit

Karol Horodecki,[1] Michał Horodecki,[2] Paweł Horodecki,[3] and Jonathan Oppenheim[4]
[1]Department of Mathematics Physics and Computer Science, University of Gdańsk, 80–952 Gdańsk, Poland
[2]Institute of Theoretical Physics and Astrophysics, University of Gdańsk, 80–952 Gdańsk, Poland
[3]Faculty of Applied Physics and Mathematics, Technical University of Gdańsk, 80–952 Gdańsk, Poland
[4]Department of Applied Mathematics and Theoretical Physics, University of Cambridge, Cambridge, United Kingdom

(Received 20 April 2004; revised manuscript received 28 January 2005; published 26 May 2005)

We study the loss of entanglement of a bipartite state subjected to discarding or measurement of one qubit. Examining behavior of different entanglement measures, we find that entanglement of formation, entanglement cost, logarithmic negativity, and one-way distillable entanglement are *lockable* measures in that they can decrease arbitrarily after measuring one qubit. We prove that any convex and asymptotically *noncontinuous* measure is lockable. As a consequence, all the convex-roof measures can be locked. The relative entropy of entanglement is shown to be a nonlockable measure.

DOI: 10.1103/PhysRevLett.94.200501 PACS numbers: 03.67.Mn, 03.65.Ud

Quantum information, unlike classical information, exhibits various superadditivities. An example of superadditivity was found in [1] where, with a single bit, one can lock (unlock) an arbitrary amount of classical correlations contained in a quantum state (according to a physically significant measure of classical correlations). One can ask if similar effects can be found for entanglement. The basic question is the following: How much can entanglement of any bipartite or multipartite system change when one qubit is discarded? The answer clearly depends on the measure of entanglement. In this Letter we show that the effect of locking holds for the entanglement of formation E_F and cost E_c, the distillable entanglement when only one-way classical communication is allowed $E_D^{\rightarrow}$, as well as a computable measure of entanglement—the logarithmic negativity E_N [2] (cf. [3]). More specifically, we show that for some state, measuring (or dephasing) one qubit can change the entanglement from an arbitrary large value to zero. We analyze other entanglement measures. We argue that if a measure is convex but not too much, then it does not admit locking. We show, for example, that relative entropy of entanglement can change at most by two upon discarding one qubit. Moreover, we link the effect of locking with the postulate that is often adopted in the case of manipulations of many copies of a quantum state—"asymptotic continuity." An entanglement measure is asymptotically continuous, if its entanglement per qubit is continuous. The importance of asymptotically continuous measures is that they give rise to "macroparameters" describing entanglement. That is, entanglement would be a measure that changes little if the state changes little. The effect of locking is a form of discontinuity, since by removing just one qubit many ebits are destroyed. This raises the question of whether locking is connected to asymptotic continuity. We confirm this by proving that a convex measure that is not asymptotically continuous admits locking. Our proof is constructive: from the states on which a function is discontinuous, one can build a state exhibiting locking. Examples are entanglement measures built by the convex-roof method [4].

Entanglement cost and logarithmic negativity.—We shall show that an *arbitrary large* E_c and E_N of a given state can be reduced to zero by a measurement on a single qubit. Consider the state on the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B \sim C^{d+2} \otimes C^{d+2}$

$$\rho_{AB} = \frac{1}{2}\begin{bmatrix} \sigma & 0 & 0 & \frac{1}{d}W^T \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \frac{1}{d}(\bar{W}) & 0 & 0 & \sigma \end{bmatrix}. \tag{1}$$

Here $W = \sum_{i,j=0}^{d-1} u_{ij}|ii\rangle\langle jj|$ where u_{ij} are elements of unitary matrix U on C^d and the state $\sigma = \sum_i \frac{1}{d}|ii\rangle\langle ii|$ is a separable maximally correlated state, also defined on C^d. The matrix is written in the computational basis $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ of a pair of qubits each with one of two parties Alice and Bob. Clearly after one party measures in the computational basis, the state will decohere, and the off-diagonal elements will go to zero—thus the state will be separable. However, before the measurement, the state has an arbitrarily large entanglement cost; i.e., it requires an arbitrarily large number of singlets shared between Alice and Bob to create, even in the asymptotic limit. To see this, we take the purification of the state

$$\psi_{ABE} = \frac{1}{\sqrt{2d}} \sum_{i=0}^{d-1} \{|i\rangle|0\rangle\}_A \{|i\rangle|0\rangle\}_B |i\rangle_E + \{|i\rangle|1\rangle\}_A \times \{|i\rangle|1\rangle\}_B U|i\rangle_E \tag{2}$$

with the third subsystem denoted as E for Eve (we call the state ρ_{AE} *dual* to ρ_{AB}). One sees that Eve gets a bit string X of length $\log d$ encoded in one of two bases. The basis is complementary if U is taken to be $H^{\otimes \log d}$ with H the Hadamard transform. This is precisely the situation for locking classical information between one party and another (here Eve). In [1] it was shown that Eve can learn at most $\frac{1}{2}\log d$ bits of X. Thus, for Eve's optimal measurement, the entropy of Alice will be greater than $\frac{1}{2}\log d$. But this is precisely a definition of E_F, i.e.,

$$E_F(\rho_{AB}) = \inf_{A_i} \sum_i p_i S(\rho_i), \tag{3}$$

where the infimum is taken over all measurements with outcomes A_i performed on the purification of ρ_{AB} and resulting in states ρ_i with Alice. This quantity is obviously achievable by a measurement in basis $\{|i\rangle\}$ which gives $E_f = 1 + \frac{1}{2}\log d$. However, since accessible information is additive as shown by Wootters [5], we get that also $E_c = 1 + \frac{1}{2}\log d$, so that it is arbitrarily large. The log-negativity can also be calculated, and it is $E_N = \log(1 + \sqrt{d})$; thus it too can be locked. Note that here we have used only two unitaries (I or U)—one can clearly get even greater entanglement locking by using more unitaries [6] and the results of [7].

Let us consider another example for locking E_N which is motivated by the results of [8]. To this aim, consider the state defined on the Hilbert space $\mathcal{H}_A^{(n)} \otimes \mathcal{H}_B^{(n)}$ in such a way that $\mathcal{H}_A^{(n)} \sim \mathcal{H}_B^{(n)} \sim C^2 \otimes (C^d)^{\otimes n}$ with parameters n and α,

$$\begin{aligned}\varrho_{AB}^{(n)} = \tfrac{1}{2}[&|00\rangle\langle 00| \otimes \tau_0^{\otimes n} + |11\rangle\langle 11| \otimes \tau_1^{\otimes n} \\ &+ \alpha^n |00\rangle\langle 11| \otimes (\tau_1^\Gamma - \tau_0^\Gamma)^{\otimes n} \\ &+ \alpha^n |11\rangle\langle 00| \otimes (\tau_1^\Gamma - \tau_0^\Gamma)^{\otimes n}].\end{aligned} \tag{4}$$

Here we use the *hiding states* from [9], $\tau_0 = \varrho_s^{\otimes l}$ and $\tau_1 = (\frac{\varrho_s + \varrho_a}{2})^{\otimes l}$, where ϱ_s and ϱ_a are fully symmetric and antisymmetric Werner states on $C^d \otimes C^d$. Note that $\rho_{AB}^{(n)}$ is a state for any $|\alpha| \le 1$ since it can be reproduced by specific local operations and classical communication (LOCC) recurrence protocol [8] from $\varrho^{(1)}$ defined by the formula above. $\varrho^{(1)}$ can be easily checked to be a state. The log negativity of $\varrho^{(n)}$ for given n is

$$E_N(\varrho^{(n)}) = \log_2[1 + \alpha(2 - 2^{-l+1})^n], \tag{5}$$

which goes to infinity with n when $|\alpha| > (2 - 2^{-l+1})^{-1}$ (since orthogonality of ϱ_s and ϱ_a implies $\|\tau_0 - \tau_1\| = 2 - 2^{-l+1}$). On the other hand, measurement of Alice's qubit in the $|i\rangle$ basis leads to the state $\frac{1}{2}\sum_{i=0}^{1}(|i\rangle\langle i|)^2 \otimes (\tau_i)^n$, which is completely separable. Hence, we have that measurement on a single qubit has locked completely an arbitrary high amount of entanglement.

Relative entropy of entanglement.—Let us now examine the relative entropy of entanglement (E_r) [10]. We show that it is not lockable. More precisely, two solutions are presented, exhibiting that after tracing out one qubit of the state ρ_{AB}, $E_r(\rho_{AB})$ can decrease at most by two, and after a complete von Neumann measurement on one qubit, E_r can decrease at most by one.

Proposition I.—For any bipartite state $\rho_{AA':B} \equiv \rho$ and any complete von Neumann measurement Λ_A on the one qubit system A there holds

$$E_r(\rho) - E_r(\Lambda_A \otimes \mathrm{I}_{A'B}(\rho)) \le 1, \tag{6}$$

$$E_r(\rho) - E_r(\mathrm{Tr}_A(\rho)) \le 2, \tag{7}$$

where Tr_A denotes a partial trace over system A.

Proof: Both statements of this theorem are the consequence of the following property of the relative entropy of entanglement [11] (see [12] in this context):

$$\sum_i p_i E_r(\rho_i) - E_r\Big(\sum_i p_i \rho_i\Big) \le S\Big(\sum_i p_i \rho_i\Big) - \sum_i p_i S(\rho_i), \tag{8}$$

where S stands for the von Neumann entropy of the state.

For the first part of the proof, it suffices to notice that any complete measurement can be implemented as a dephasing of the system. To dephase one qubit, one can add a local random ancilla $\tau = \frac{1}{2}[|0\rangle\langle 0| + |1\rangle\langle 1|]$ and perform the controlled unitary operation $U = \sum_{i=0}^{1} |i\rangle\langle i|_{\mathrm{anc}} \otimes \sigma_A^{(i)}$ with $\sigma^{(0)} = I_A$ and $\sigma^{(1)} = \sigma_z$—a Pauli matrix, followed by tracing out τ. One can easily check that random unitaries put phases which zero the coherences of the state:

$$\mathrm{T\,r}_{\mathrm{anc}}[U(\tau \otimes \rho)U^\dagger] = \Lambda_A \otimes I_{A'B}(\rho) \equiv \rho_{\mathrm{meas}}. \tag{9}$$

Taking now in (8) $\rho_i = \sigma_i \otimes I_{A'B}(\rho)$ and $p_i = \frac{1}{2}$, one gets

$$E_r(\rho) - E_r\Big(\sum_i p_i \rho_i\Big) \le S\Big(\sum_i p_i \rho_i\Big) - \sum_i p_i S(\rho_i), \tag{10}$$

since local unitary transformations do not change E_r. For such choices of ρ_i and p_i the state $\sum_i p_i \rho_i$ is equal to state ρ after dephasing, and by (9) it is the same as the one after a complete measurement, which gives us

$$E_r(\rho) - E_r(\rho_{\mathrm{meas}}) \le S\Big(\sum_i p_i \rho_i\Big) - \sum_i p_i S(\rho_i). \tag{11}$$

It is known [13] that the right hand side does not exceed $H(p)$, i.e., the Shannon entropy of the "mixing" distribution $\{p_i\}$. In our case this distribution is homogeneous, so $S(\sum_i p_i \rho_i) - \sum_i p_i S(\rho_i) \le 1$, which leads us to the first part of the theorem.

The second part of the theorem can be proven in a similar vein. Instead of tracing out, we apply total dephasing, which is equivalent to the substitution of a qubit by the maximally mixed one, uncorrelated with the rest of the state. To this end, we a need bigger random ancilla system $\tau^{\otimes 2}$ and the controlled unitary composed from all four Pauli matrices: $U = \sum_{i=0}^{3} |i\rangle\langle i|_{\mathrm{anc}} \otimes \sigma_A^{(i)}$ [14,15].

Now the state after the transformation U and tracing out the ancilla $\tau^{\otimes 2}$ is the following: $\frac{I_A}{4} \otimes \mathrm{Tr}_A \rho_{AA'B}$. The relative entropy of entanglement of this state is the same as for $\mathrm{Tr}_A \rho_{AA'B}$, because it cannot increase after tracing out $\frac{I_A}{4}$ for this is a local operation, and it cannot decrease, since this qubit is product with the rest of the state. In this case, the right hand side of the inequality (11) is bounded by $H(p) = 2$ which completes the proof.

Although it seems to be intuitive, we are not able to show that both complete measurement and tracing out of a qubit decrease E_r by the same amount. That is, for tracing out, we were able to prove only a bound of 2 rather than 1 for the change of E_r. Were this tighter bound to be proven, one would have an interesting complementarity relation between measuring and forgetting. Clearly, measuring a qubit can decrease the entanglement by one ebit. Likewise, forgetting the result of a measurement can also decrease entanglement also by one ebit. An example of the latter is the measurement result which tells one whether one has a singlet, or some other Bell state. Since tracing out a qubit is equivalent to measuring and then forgetting the result, we would have that if a measurement decreases entanglement by one, then forgetting this result cannot change the entanglement and vice versa. Note that our proof also holds for the relative entropy distance to any convex set closed under local unitaries, e.g., the distance to the set of positive partial transpose states.

Locking and asymptotic continuity.—Let us now proceed to the connection between asymptotic continuity and locking. We first provide a general result on asymptotic continuity, which is inspired by results of Alicki and Fannes [16] on quantum conditional entropy.

Proposition 2. —Any function f satisfying (1) "approximate affinity" $|pf(\rho) + (1-p)f(\sigma) - f[p\rho + (1-p)\sigma]| \leq c$, and (2) "subextensivity" $|f(\rho)| \leq M\log d$, where c and M are constants, is asymptotically continuous; i.e., it satisfies

$$|f(\rho_1) - f(\rho_2)| \leq M \parallel \rho_1 - \rho_2 \parallel \log d + 4c. \tag{12}$$

Remark: For our purpose (asymptotic regime), it is only important that c is constant. However, to have also the usual continuity, it should be that for small p, c is small. [For example, for f being a von Neumann entropy, we have $c \leq H(p)$.]

To prove the proposition, we need the following lemma of [17] (cf. [16]).

Lemma 1.—For any two states $\rho_1 \neq \rho_2$, there exist states σ, γ_1, and γ_2 such that

$$\sigma = \frac{1}{(1+\delta)}\rho_1 + \frac{\delta}{(1+\delta)}\gamma_1 = \frac{1}{(1+\delta)}\rho_2 + \frac{\delta}{(1+\delta)}\gamma_2, \tag{13}$$

where $2\delta = \parallel \rho_1 - \rho_2 \parallel$.

Proof of the lemma: One takes states $\gamma_{1(2)} = \omega_\pm/\mathrm{Tr}\omega_\pm$, where $\omega_\pm$ are positive and negative parts of $\rho_1 - \rho_2$.

Proof of proposition: Let us denote $x_i = \frac{1}{(1+\delta)}f(\rho_i) + \frac{\delta}{(1+\delta)}f(\gamma_i) - f(\sigma)$. The x_i's show how the function f departs from the affinity on the considered states. A positive x_i means convexity, and a negative x_i means concavity. Of course, $c \geq |x_i|$, because c bounds the departure from affinity for any states. Using (13) we get

$$f(\rho_1) - f(\rho_2) = \delta[f(\gamma_1) - f(\gamma_1)] + (1+\delta)(x_2 - x_1); \tag{14}$$

hence due to subextensivity we get

$$\begin{aligned}|f(\rho_1) - f(\rho_2)| &\leq \delta|f(\gamma_1) - f(\gamma_2)| + (1+\delta)(|x_1| + |x_2|)\\ &\leq 2\delta M\log d + 4c.\end{aligned}$$

This ends the proof. ■

Now let us exhibit what happens when a function is subextensive, but is not asymptotically continuous. To this end, consider a subextensive function f; i.e., let $f(\rho) \leq M\log d$, where ρ acts on a d-dimensional Hilbert space. Let us assume that f is not asymptotically continuous. This means that we have a sequence of states $\rho_1^{(n)}$ and $\rho_2^{(n)}$ approaching each other in a trace distance and acting on a Hilbert space of increasing dimension d_n, such that

$$\frac{|f(\rho_1^{(n)}) - f(\rho_2^{(n)})|}{\log d_n} \geq \Delta, \tag{15}$$

where Δ is some positive constant. We now consider states $\sigma^{(n)}$, $\gamma_1^{(n)}$, $\gamma_2^{(n)}$ given by lemma, $\delta^{(n)} = \frac{1}{2} \parallel \rho_1^{(n)} - \rho_2^{(n)} \parallel$, and $x_i^{(n)}$ being analogues of x_i. The formula (14) applied to those states together with (15) implies that $|x_1 - x_2| \geq (\Delta - 2\delta^{(n)}M)\log d_n$. Thus we see that at least one of the x_i must have an arbitrary large modulus for large n (i.e., small $\delta^{(n)}$). Without a loss of generality, we can assume it is x_1. Then we get that one of two possibilities holds: (i) $x_1 \leq (-\Delta/2 + \delta^{(n)}M)\log d_n$, or (ii) $x_1 \geq (\Delta/2 - \delta^{(n)}M)\log d_n$. In case (i) the function is too concave, while in case (ii) it is too convex. In both cases, the function upon mixing two states can be arbitrarily different from the average of the function.

In the first case we have a situation where upon mixing two states (i.e., forgetting whether one has $\rho_1^{(n)}$ or $\rho_2^{(n)}$), a function can go up an arbitrary amount—this can be regarded as a type of *activation.* In case (ii), we have that upon mixing, the function goes arbitrarily down. If f is convex, then, of course, only (ii) can occur, and together with convexity, it gives *locking.* We have then the following.

Proposition 3.—A convex LOCC monotone E that satisfies $E(\rho) \leq M\log d$ for some constant M, and that is not asymptotically continuous, admits locking.

Proof: From assumptions it follows that there must exist states ρ_1 and γ_1 and weights $1-\epsilon$ and ϵ such that the difference

$$x = [\epsilon E(\rho_1) + (1-\epsilon)E(\gamma_1)] - E[\epsilon\rho_1 + (1-\epsilon)\gamma_1] \tag{16}$$

can be arbitrarily large. Now let us note that a convex entanglement measure satisfies

$$\begin{aligned}&E(p\rho_{AB} \otimes |0\rangle\langle 0|_{A'} +\\ &\quad (1-p)\tilde{\rho}_{AB} \otimes |1\rangle\langle 1|_{A'}) = pE(\rho) + (1-p)E(\tilde{\rho}).\end{aligned} \tag{17}$$

One way follows from convexity and from nonincreasing E under tracing out a local qubit. The second follows from the fact that the state on the left hand side of the inequality can be transformed into the ensemble $\{(p, \rho), (1 - p, \tilde{\rho})\}$. Consider now the state

$$\rho_{ABA'} = (1 - \epsilon)\rho_1 \otimes |0\rangle\langle 0|'_A + \epsilon\tilde{\gamma}_1 \otimes |1\rangle\langle 1|'_{A'}, \qquad (18)$$

where A' is one qubit system. Its reduction is given by

$$\rho_{AB} = (1 - \epsilon)\rho_1 + \epsilon\tilde{\gamma}_1. \qquad (19)$$

Hence following (16) we obtain that the difference

$$E(\rho_{ABA'}) - E(\rho_{AB}) \qquad (20)$$

can be arbitrarily large, which is locking.

Examples.—Consider the so-called convex-roof measures [4], based on Renyi entropy with $0 \leq \alpha < 1$. Such measures are convex by definition, and on pure states they are equal to the Renyi entropy $S_\alpha = \frac{1}{1-\alpha} \log\mathrm{Tr}\rho^\alpha$ of the subsystem. For our choice of α the Renyi entropy is greater than the von Neumann entropy. It is easy to check that, for a compressed version of state $\rho^{\otimes n}$ (denote it by ρ_{typ}) where only typical eigenvalues are kept, the Renyi entropy for large n tends to the von Neumann entropy $nS(\rho)$. On the other hand, for the original state, it is equal to $nS_\alpha(\rho)$. As we know, the states ρ_{typ} and $\rho^{\otimes n}$ converge to each other. However, for the Renyi entropy we obtain that $\Delta = S_\alpha(\rho) - S(\rho)$. Thus Renyi entropy is not asymptotically continuous, and since we pointed out states on which it diverges, we can construct the states, on which we have a locking effect.

Let us mention that the above theorem does not say anything about measures that are asymptotically continuous. Thus the cases of E_r [18] and E_c which are asymptotically continuous had to be treated separately. Also the theorem does not say anything about measures that are not subextensive. Therefore the case of negativity was also treated separately. Whether distillable entanglement is lockable or not remains an open problem. However, if we restrict the parties to only one-way communication, $E_D^{\rightarrow}$ turns out to be lockable.

One-way distillable entanglement and classical capacity.—An example of $E_D^{\rightarrow}$ locking is the state [19] $\frac{1}{2}|\psi_+\rangle_{AB}\langle\psi_+| \otimes |0\rangle_{A'}\langle 0| + \frac{1}{2}\frac{I_{AB}}{d^2} \otimes |1\rangle_{A'}\langle 1|$. The state has $E_D^{\rightarrow} = E_D = \frac{1}{2}\log d$. After removing flags, it has $E_D^{\rightarrow} = 0$, by the standard no-cloning (or monogamy) argument [20].

One can also ask whether the channel capacity can be locked by not using part of the input. In the case of classical capacity, the answer is yes. The example comes right from the state ρ_{CB}, which produces the locking of accessible information. The channel acts as follows: the input consists of a control bit and n other qubits. The control bit decides whether or not U is applied to the other qubits. Then all qubits are measured on a computational basis. If we choose $U = H^{\otimes n}$, then the sender cannot use a control bit (where instead the random bit is input), the classical capacity of the channel drop to $\log d$, while initially it was of order of d. For quantum capacity is it also lockable, as the example of $D^{\rightarrow}$ shows.

Finally, we propose a definition of the nonlockable version of the entanglement measure.

Definition.—For any entanglement measure $E(\rho)$ the reduced entanglement measure $E\downarrow(\rho)$ is defined as

$$E\downarrow(\rho) = \inf_{\Lambda\in\mathrm{CLOCC}} E[\Lambda(\rho) + \Delta S]. \qquad (21)$$

Here CLOCC is a class of LOCC operations in a closed system and $\Delta S = S(\Lambda(\rho)) - S(\rho)$ is the increase of entropy produced by measurement. In fact, this is the quantum analogue of the reduced intrinsic information defined in [21]. One can also consider other versions of such a reduction, choosing maps Λ, e.g., to be local bistochastic ones or local dephasings.

We thank Ryszard Horodecki and Matthias Christandl for helpful discussion. This work is supported by MNiI, Grant No. PBZ-MIN-008/P03/2003, EU grants RESQ (IST-2001-37559), QUPRODIS (IST-2001-38877), and PROSECCO (IST-2001-39227). J. O. additionally acknowledges the Cambridge-MIT Institute.

[1] D. P. DiVincenzo *et al.*, Phys. Rev. Lett. **92**, 067902 (2004).
[2] G. Vidal and R. F. Werner, Phys. Rev. A **65**, 032314 (2002).
[3] K. Zyczkowski *et al.*, Phys. Rev. A **58**, 883 (1998)..
[4] G. Vidal, J. Mod. Opt. **47**, 355 (2000).
[5] D. P. DiVincenzo, D. W. Leung, and B. M. Terhal, IEEE Trans. Inf. Theory **48**, 580 (2002).
[6] This was also noted by Debbie Leung (private communication).
[7] P. Hayden *et al.*, Commun. Math. Phys. **250**, 371 (2004).
[8] K. Horodecki *et al.*, Phys. Rev. Lett. **94**, 160502 (2005).
[9] T. Eggeling and R. F. Werner, Phys. Rev. Lett. **89**, 097905 (2002).
[10] V. Vedral *et al.*, Phys. Rev. Lett. **78**, 2275 (1997).
[11] N. Linden *et al.*, quant-ph/9912039.
[12] J. Eisert *et al.*, Phys. Rev. Lett. **84**, 1611 (2000).
[13] M. Ohya and D. Petz, *Quantum Entropy and Its Use* (Springer, New York, 1993).
[14] P. Boykin and V. Roychowdhury, Phys. Rev. A **67**, 042317 (2003).
[15] M. Mosca, A. Tapp, and R. de Wolf, quant-ph/0003101.
[16] R. Alicki and M. Fannes, J. Phys. A **37**, L55 (2004).
[17] H. Araki and H. Moriya (unpublished).
[18] M. Donald and M. Horodecki, Phys. Lett. A **264**, 257 (1999).
[19] This example was found during discussions with Andreas Winter and Reinhard Werner.
[20] C. H. Bennett, D. P. DiVincenzo, and J. A. Smolin, Phys. Rev. Lett. **78**, 3217 (1997).
[21] R. Renner and S. Wolf, in *Advances in Cryptology—EUROCRYPT '03*, Lecture Notes in Computer Science (Springer, Berlin, 2003).