Secure Key from Bound Entanglement

Karol Horodecki,[1] Michał Horodecki,[2] Paweł Horodecki,[3] and Jonathan Oppenheim[2,4,5]
[1]*Department of Mathematics, Physics and Computer Science, University of Gdańsk, Poland*
[2]*Institute of Theoretical Physics and Astrophysics, University of 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*
[5]*Racah Institute of Theoretical Physics, Hebrew University of Jerusalem, Givat Ram, Jerusalem 91904, Israel*
(Received 13 September 2003; published 26 April 2005)

We characterize the set of shared quantum states which contain a cryptographically private key. This allows us to recast the theory of privacy as a paradigm closely related to that used in entanglement manipulation. It is shown that one can distill an arbitrarily secure key from bound entangled states. There are also states that have less distillable private keys than the entanglement cost of the state. In general, the amount of distillable key is bounded from above by the relative entropy of entanglement. Relationships between distillability and distinguishability are found for a class of states which have Bell states correlated to separable hiding states. We also describe a technique for finding states exhibiting irreversibility in entanglement distillation.

DOI: 10.1103/PhysRevLett.94.160502 PACS numbers: 03.67.Dd, 03.65.Ud, 03.67.Mn

Recently, strong connections have been emerging between the amount of pure entanglement E_D and the private key K_D one can distill from a shared quantum state. For example, the security of key generation in Bennett-Brassard 1984 (BB84) [1] and Bennett 1992 (B92) [2] can be proven by showing its equivalence with entanglement distillation of singlets [3,4]. These proofs had their origin in the idea of *quantum privacy amplification* [5] where two parties (Alice and Bob) distill pure quantum entanglement until the quantum correlations are completely disentangled with an eavesdropper (Eve). Those correlations were represented by singlet states and were subsequently measured to obtain a classical private key to which Eve had no access. Very recently, the hashing inequality [6,7] was proven [8] by showing the equivalence between certain distillation protocols and one way secret key distillation.

An apparent equivalence between bound entangled states (states which require entanglement to create, but from which no pure entanglement can be distilled) and classical distributions which cannot be turned into a key was conjectured in [9]. Additionally, using techniques developed in entanglement theory, a gap similar to the one between entanglement cost and distillable entanglement was shown to exist classically for private keys [10]. It has also been shown that for two qubits, a state is one copy distillable iff it is cryptographically secure [11,12] (cf. [13,14]), and there are basic laws which govern the interplay of key generation in terms of sent quantum states [15].

In fact, the original Letters on entanglement distillation [6] used protocols which were derived from existing protocols for distilling privacy from classical probability distributions. Indeed, formal analogies between entanglement and secrecy exist [16]. The evidence to date strongly supports the widely held belief that privacy and entanglement distillation are strictly equivalent—that one can get a private key from a quantum state if and only if entanglement distillation is possible.

Surprisingly, this is not the case—we introduce a class of *bound entangled states* (no pure entanglement can be distilled from them), from which one can distill a private key. Examples of states that have one bit of perfect private key and at the some time arbitrarily small distillable entanglement are also provided.

Clearly, one always has $K_D \geq E_D$ since one can always distill singlets from a state, and then use these singlets to generate a private key [17]. Here, we prove that one can also have the strict inequality $K_D > E_D$, which sometimes holds even if $E_D = 0$. We also prove that the private key is generally bounded from above by the relative entropy of entanglement E_r [18] (regularized). This is sufficient to prove that one can have $K_D < E_c$ where E_c is the entanglement cost (the number of singlets required to prepare a state under LOCC). This enables one to easily find states for which $E_D < E_r$. In this Letter we state some of the results and present the full proofs in detail elsewhere [19].

We first introduce a wide class of states which are the most general *private states* in the sense that one can produce one bit of secure key from them even though an eavesdropper might hold the purification of the state. One can think of these states as being the equivalent of the singlet for key distillation. This allows us to recast all protocols of key distillation (classical or otherwise) in terms of distillation of private states using the distant labs paradigm used in entanglement theory, i.e., local operations and classical communication (LOCC). Next we show that these states can have arbitrarily little distillable entanglement while still retaining one bit of private key. We can relate this to the problem of distinguishability of states under LOCC. We then exhibit a bound entangled state from which a private key can be distilled. We then prove that $K_D \leq E_r$ and discuss the consequences.

Let us now introduce private states, i.e., $\gamma_{ABA'B'}$ where systems AB are both m qubits, and the measurement of AB in the computational basis gives m bits of perfect key. Systems AA' (BB') are held by Alice (Bob). We assume the usual scenario—that any part of the state which is not with Alice and Bob might be with an eavesdropper Eve. Thus Eve holds the purification of this state. We now provide their unique form. We first consider perfect security.

Theorem 1: *A state is private in the above sense iff it is of the following form:*

$$\gamma_m = U|\psi^+_{2^m}\rangle_{AB}\langle\psi^+_{2^m}| \otimes \varrho_{A'B'}U^\dagger, \tag{1}$$

where $|\psi^+_d\rangle = \sum_{i=1}^d |ii\rangle$ *and* $\varrho_{A'B'}$ *is an arbitrary state on* A', B'. *U is an arbitrary unitary controlled in the computational basis*

$$U = \sum_{i,j=1}^{2^m} |ij\rangle_{AB}\langle ij| \otimes U_{ij}^{A'B'}. \tag{2}$$

We call the operation (2) "twisting" (note that only $U_{ii}^{A'B'}$ matter here, yet it will be useful to consider general twisting later).

Proof: We prove for $m = 1$ (for higher m, the proof is analogous). Start with an arbitrary state held by Alice and Bob, $\rho_{AA'BB'}$, and include its purification to write the total state in the decomposition

$$\Psi_{ABA'B',E} = a|00\rangle_{AB}|\Psi_{00}\rangle_{A'B'E} + b|01\rangle_{AB}|\Psi_{01}\rangle_{A'B'E} + c|10\rangle_{AB}|\Psi_{10}\rangle_{A'B'E} + d|11\rangle_{AB}|\Psi_{11}\rangle_{A'B'E} \tag{3}$$

with the states $|ij\rangle$ on AB and Ψ_{ij} on $A'B'E$. Since the key is unbiased and perfectly correlated, we must have $b = c = 0$ and $|a|^2 = |d|^2 = 1/2$. Depending on whether the key is $|00\rangle$ or $|11\rangle$, Eve will hold the states

$$\varrho_0 = \mathrm{Tr}_{A'B'}|\Psi_{00}\rangle\langle\Psi_{00}|, \qquad \varrho_1 = \mathrm{Tr}_{A'B'}|\Psi_{11}\rangle\langle\Psi_{11}|. \tag{4}$$

Perfect security requires $\varrho_0 = \varrho_1$. Thus there exists unitaries U_{00} and U_{11} on $A'B'$ such that

$$|\Psi_{00}\rangle = \sum_i \sqrt{p_i}\,|U_0\phi_i^{A'B'}\rangle|\varphi_i^E\rangle,$$
$$|\Psi_{11}\rangle = \sum_i \sqrt{p_i}\,|U_1\phi_i^{A'B'}\rangle|\varphi_i^E\rangle. \tag{5}$$

After tracing out E, we thus get a state of the form Eq. (1), where $\varrho_{A'B'} = \Sigma_i p_i|\phi_i\rangle\langle\phi_i|$.

It is instructive to see the matrix of a general γ_1 state:

$$\gamma_1 = \begin{bmatrix} \sigma & 0 & 0 & X \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ X^\dagger & 0 & 0 & \sigma' \end{bmatrix}, \tag{6}$$

where the matrix is written in the computational basis on AB, i.e., $|00\rangle, |01\rangle, |10\rangle, |11\rangle$, and the trace norm of block X is $1/2$. Thus γ_1 looks like a Bell state with blocks instead of c numbers, and the condition on $\| X \|$ can be associated with the fact that Bell states have the corresponding element (coherence) equal to $1/2$.

Let us briefly sketch the situation where one demands only approximate security for $m = 1$. Consider in place of γ_1 an arbitrary state written in similar block form. One finds that the condition $\| X' \| \approx 1/2$, where X' is the upper right block, is equivalent to the state being close to γ_1 in norm. For the converse direction, one can verify that in terms of the fidelity $F(\varrho_0^E, \varrho_1^E) = \mathrm{Tr}|\sqrt{\varrho_0^E}\sqrt{\varrho_1^E}|$

$$\| X' \| = \sqrt{p_0 p_1} F(\rho_0^E, \rho_1^E), \tag{7}$$

where p_i are probabilities of Alice and Bob to obtain outcome ii, and ρ_i^E are the corresponding Eve's states. Thus having an approximate bit of key, i.e., uniformity $p_0 \approx p_1 \approx 1/2$ and security $F(\rho_1^E, \rho_2^E) \approx 1$ (implying $\rho_0^E \approx \rho_1^E$), is equivalent to sharing state close to γ_1. The result can be generalized to $m > 1$ [19], and thus the resulting state is close in norm to some γ_1.

This then completely recasts the drawing of key at a rate K_D under local operations and public communication (LOPC) in terms of distilling γ_m states (at a rate of K_γ under LOCC). Clearly $K_\gamma \leq K_D$ since distilling γ_m is a particular way of drawing key. Additionally, by Theorem 1, any secure protocol which distills K_D is also distilling γ_m with $K_\gamma = K_D$ when one considers all of Alice and Bob's laboratory as the $A'B'$ ancilla. That is, if one applies some protocol coherently (since the original LOPC protocol might be partly classical), one distills some γ_m at the full rate. We thus have equality of the two rates.

Before showing that one can have bound entangled states which give secure key, we provide examples of both strict and approximate γ states, which have an arbitrarily small amount of distillable entanglement, i.e., $K_D \gg E_D$.

Example 1.—Consider states

$$\varrho = p|\psi_+\rangle\langle\psi_+| \otimes \varrho_+ + (1-p)|\psi_-\rangle\langle\psi_-| \otimes \varrho_-, \tag{8}$$

where $\psi_\pm = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$ and $\varrho_\pm$ reside on orthogonal subspaces. One can verify that these states are particular examples of γ_1, and therefore produce at least one bit of private key. Eve (who holds the purification of the state) can learn the phase of the state on AB, i.e., whether Alice and Bob hold ψ_- or ψ_+. She can help Alice and Bob obtain one singlet by telling them which maximally entangled state they possess. Yet she can learn nothing about the key bit (i.e., whether they have $|00\rangle$ or $|11\rangle$). In a sense, Eve can hold one bit of information but it is the wrong bit of information. Such a situation is impossible classically (or with pure quantum states held by Alice and Bob).

To decrease the distillable entanglement, take $p = (1 + 1/d)/2$ and $\varrho_\pm$ to be two extreme Werner $d \otimes d$ states

$$\varrho_s = \frac{2}{d^2 + d} P_{\mathrm{sym}}, \qquad \varrho_a = \frac{2}{d^2 - d} P_{\mathrm{as}} \tag{9}$$

with P_{as} and P_{sym} the antisymmetric and symmetric projectors. The log-negativity E_N which is an upper bound on the distillable entanglement E_D [20] amounts in this case to $E_N(\varrho) = \log\frac{d+1}{d}$. Thus by increasing d one can have an arbitrarily small amount of distillable entanglement while keeping one bit of private key.

Example 2.—We take $\varrho_\pm$ to be two separable hiding states τ_0 and τ_1. We take here those given in [21]

$$\tau_0 = \varrho_s^{\otimes l}, \qquad \tau_1 = [(\varrho_a + \varrho_s)/2]^{\otimes l}. \tag{10}$$

By choosing d and l one can make them arbitrarily indistinguishable under LOCC and arbitrarily orthogonal [since $X = (\tau_1 - \tau_0)$, orthogonality of the τ's are needed for security, i.e., $\| X \|$, while hiding is needed for low distillability]. Choosing $p = 1/2$, one can show that distilling entanglement essentially reduces to Alice and Bob determining which maximally entangled state they possess by performing measurements on the hiding state τ. Choosing better and better hiding states decreases the distillable entanglement arbitrarily. Again we check this by the use of log negativity; one finds that $E_N(\varrho) = \| \tau_0^\Gamma - \tau_1^\Gamma \|$ where Γ stands for partial transpose. This quantity has been shown to be an upper bound for distinguishability of the hiding states, and for a suitable choice of l and d it can be made arbitrarily small [21].

Recently, strong connections have been emerging between the amount of pure entanglement E_D and the private key K_D one can distill from a shared quantum state. In both examples, however, the states do have nonzero distillable entanglement. For strict γ states, it is not hard to see that they are always distillable. It is then clear that any key from bound entangled states can be arbitrarily secure, but not perfectly secure.

Main result.—We now introduce a bound entangled state which can be shown to have $K_D > 0$. We simply take the preceding state, and introduce errors

$$\rho = \begin{bmatrix} \frac{p}{2}(\tau_0 + \tau_1) & 0 & 0 & \frac{p}{2}(\tau_1 - \tau_0) \\ 0 & (\frac{1}{2} - p)\tau_0 & 0 & 0 \\ 0 & 0 & (\frac{1}{2} - p)\tau_0 & 0 \\ \frac{p}{2}(\tau_1 - \tau_0) & 0 & 0 & \frac{p}{2}(\tau_0 + \tau_1) \end{bmatrix}. \tag{11}$$

One finds that for $p \leq 1/3$ and $l\sqrt{\frac{1-p}{p}}(d-1) \geq d$ the state has positive partial transpose (PPT) being therefore bound entangled [22].

Now, we take n copies and apply the recurrence distillation protocol of [23] without the twirling step. The off-diagonal block of the resulting state is given by $X = N^{-1}[p(\tau_1 - \tau_0)/2]^{\otimes n}$ with $N = 2p^n + 2(1/2 - p)^n$. To see that Alice and Bob have an arbitrarily secure key, we check that its trace norm tends to $1/2$:

$$\|X\| = \frac{1}{2}\left(1 - \frac{1}{2^l}\right)^n \left[1 + \left(\frac{1-2p}{2p}\right)^n\right]^{-1} \tag{12}$$

Now, for $p > 1/4$ the norm can be arbitrarily close to $1/2$ if we had previously taken l large enough, and now take large n. Given such l, one could always have initially chosen d to satisfy the PPT condition of the initial state (11), so that the state ρ' is PPT (as it is obtained from ρ by LOCC).

Remark.—Note that we need to use large l for security, large n for the state to approximate perfect key, and large d for the state to be PPT. Indeed, large d is needed for τ_i to be hiding states, and if they are not hiding, then the states would be distillable by distinguishing between them, and then distilling the correlated singlet.

Thus we have shown that we can get an arbitrarily secure bit from bound entangled states. The structure of our states sheds some light, perhaps for the first time, on the phenomenon of bound entanglement: they can contain singlets that are so "twisted" they cannot be distilled, but they can exhibit their quantum character through privacy. This explanation probably cannot be applied to low-dimensional bound entangled states.

Having shown that one can draw one bit of key, we now show that Alice and Bob can draw key at a nonzero asymptotic rate, using Lemma 1.

Lemma 1: *For any state $\psi_{ABA'BE}$ consider the state ϱ_{ABE} emerging after measurement on AB in the standard basis. The latter state does not change under twisting*. (The proof boils down to direct checking.)

Since the trace norm of the off-diagonal block (12) of the state is close to $1/2$, by the use of polar decomposition, one finds a twisting operation after which the *trace* of block X is equal to its trace norm. For such new state ρ'', by Lemma 1, Eve's states correlated with the outcomes of AB measurements that are still the same as for ρ'. Now, however, after tracing out $A'B'$, the state is close to singlet. Clearly, the problem is reduced to drawing key from outcomes of measurement, from a state close to singlet, which can be done, for example, by the protocol of Devetak and Winter [8]. As we have already noted, this draws γ states at the same rate as K_D when the corresponding classical protocol is applied coherently.

We now provide a general upper bound on K_D in terms of the relative entropy of entanglement $E_r(\rho) := \inf_{\sigma \in \mathrm{sep}} S(\rho \| \sigma)$, with $S(\rho \| \sigma) := \mathrm{Tr}[\rho(\ln\rho - \ln\sigma)]$ and "sep" being the set of separable states. Namely, we have Theorem 2.

Theorem 2: $K_D(\rho_{AB}) \leq E_r^\infty(\rho_{AB})$, *where E_r^∞ is the regularization of the relative entropy of entanglement $E_r^\infty(\rho) := \lim_{n\to\infty} E_r(\rho^{\otimes n})/n$.*

Our proof is inspired by the idea that transition rates are bounded by LOCC monotones [24], yet it needs essentially new techniques, mostly due to the possibility of large scaling of the size of the ancilla $A'B'$ with the number of obtained bits of key. We present it in [19].

Since we can have $E_r(\rho) < E_c(\rho)$, the above theorem implies that for some states, the key rate is strictly less than the entanglement cost, and, in fact, can be made arbitrarily small for fixed E_c. For example, for antisymmetric Werner state ϱ_a we have $E_c(\varrho_a) = 1$ [25] while $E_r^\infty(\varrho_a) = \log(d+2)/d$ which can be arbitrarily low.

In summary, we have found that, in general, $E_D \leq K_D \leq E_r^\infty \leq E_c$ with strict inequalities $E_D < K_D < E_c$ and $E_D < E_r^\infty$ also possible (the latter was shown previously in [26]; our result allows for easy construction of new examples). One can even have $K_D > 0$ for bound entangled states. This implies that the rate of distillable key is not only an operational measure of entanglement, but is also nontrivial in that it is not equal to other known operational measures: E_c and E_D. This is also likely to be true for the *quantum key cost* K_c which we define to be the minimum size m of γ_m required to form a state in the asymptotic limit. These results also put into question the possibility of "bound information" for bipartite systems conjectured in [9], although the phenomena may well exist for distributions derived from other bound entangled states. Our results also suggest that the qualitative equivalence between privacy and distillability in $2 \otimes 2$ [11] is likely to be due to the fact that in low dimensions, bound entanglement does not exist.

One could define a unit of privacy, by calling γ_1 *irreducible*, if one and only one bit of privacy can be obtained from it. An irreducible private state may therefore be thought of as the basic unit state of privacy, much as the singlet is the basic unit of entanglement theory (although not all γ states are equivalent to each other, thus one thinks of γ_m in its entirety). From Theorem 2 it follows that irreducibility can be imposed by demanding that γ_1 have a relative entropy of entanglement of one. However, we do not know if this condition is too strong.

Here our interest in privacy is motivated by the fundamental insight it gives into entanglement—there seems to exist a deep connection between the entanglement cost of PPT states, and privacy. In terms of cryptographic protocols, the states considered here can be incorporated into an actual scheme by performing a suitably randomized tomography protocol on the obtained states to verify that they are, indeed, close to the expected form. Such a protocol is highly inefficient, but appears to be secure for binding entanglement channels, although the scaling of security parameters may be qualitatively different than in BB84. Determining how efficient such a protocol could be is an interesting open problem.

This work is supported by EU grants RESQ (IST-2001-37559), QUPRODIS (IST-2001-38877), and PROSECCO (IST-2001-39227), and J. O. additionally acknowledges 129/00-1 of the ISF, and a grant from the Cambridge-MIT Institute. We thank A. Acin, R. Horodecki, A. Winter, and N. Lütkenhaus for helpful feedback and T. Eggeling for sending us an advance copy of the sequel to Ref. [21].

[1] C. Bennett and G. Brassard, in *Proceedings of the IEEE Conference on Computers, Systems and Signal Processing* (IEEE Computer Society Press, New York, 1984), pp. 175–179.
[2] C. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[3] P. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[4] K. Tamaki, M. Koashi, and N. Imoto, Phys. Rev. Lett. **90**, 167904 (2003).
[5] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).
[6] C. H. Bennett, D. P. DiVincenzo, J. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[7] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **85**, 433 (2000).
[8] I. Devetak and A. Winter, Phys. Rev. Lett. **93**, 080501 (2004).
[9] N. Gisin and S. Wolf, in *Proceedings of CRYPTO 2000, Lecture Notes in Computer Science* (Springer-Verlag, Berlin, 2000), Vol. 1880, p. 482.
[10] R. Renner and S. Wolf, in *Advances in Cryptology—EUROCRYPT '03, Lecture Notes in Computer Science* (Springer-Verlag, Berlin, 2003).
[11] A. Acin, L. Massanes, and N. Gisin, quant-ph/0303053.
[12] In the case where the eavesdropper measures her states before privacy amplification.
[13] N. Gisin and S. Wolf, Phys. Rev. Lett. **83**, 4200 (1999).
[14] D. Bruss, M. Christandl, A. Ekert, B. Englert, D. Kaszlikowski, and C. Macchiavello, quant-ph/0303184.
[15] J. Oppenheim and M. Horodecki, quant-ph/0306161.
[16] D. Collins and S. Popescu, Phys. Rev. A **65**, 032321 (2002).
[17] A. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[18] V. Vedral and M. B. Plenio, Phys. Rev. A **57**, 1619 (1998).
[19] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim (to be published).
[20] G. Vidal and R. Werner, Phys. Rev. A **65**, 032314 (2002).
[21] T. Eggeling and R. Werner, Phys. Rev. Lett. **89**, 097905 (2002).
[22] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **80**, 5239 (1998).
[23] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. Smolin, and W. K. Wootters, Phys. Rev. Lett. **78**, 2031 (1997).
[24] M. Horodecki, Quantum Inf. Comput. **1**, 3 (2001).
[25] K. Matsumoto and F. Yura, J. Phys. A **37**, L167 (2004).
[26] A. Acin, G. Vidal, and J. Cirac, Quantum Inf. Comput. **3**, 55 (2003).