

Equivalence between Two-Qubit Entanglement and Secure Key Distribution

Antonio Acín,^{1,2} Lluís Masanes,³ and Nicolas Gisin¹

¹*GAP-Optique, University of Geneva, 20, Rue de l'École de Médecine, CH-1211 Geneva 4, Switzerland*

²*Institut de Ciències Fotòniques, Jordi Girona 29, Edifici Nexus II, 08034 Barcelona, Spain*

³*Department of ECM, University of Barcelona, Diagonal 647, 08028 Barcelona, Spain*

(Received 1 April 2003; revised manuscript received 31 July 2003; published 13 October 2003)

We study the problem of secret key distillation from bipartite states in the scenario where Alice and Bob can perform measurements only at the single-copy level and classically process the obtained outcomes. Even with these limitations, secret bits can be asymptotically distilled by the honest parties from any two-qubit entangled state, under any individual attack. Our results point out a complete equivalence between two-qubit entanglement and secure key distribution: a key can be established through a one-qubit channel if and only if it allows one to distribute entanglement. These results can be generalized to a higher dimension for all those states that are one-copy distillable.

DOI: 10.1103/PhysRevLett.91.167901

PACS numbers: 03.67.Dd, 03.65.Ud, 03.67.Hk, 03.67.Mn

Quantum correlations or entanglement is the basic ingredient for many applications of quantum information theory [1]. By exploiting the correlations of entangled states, one can perform tasks that are impossible in classical information theory. Quantum cryptography [2], or more precisely quantum key distribution, is the most successful quantum information application, due to its experimental feasibility with present-day technology. Although entanglement is not required for a secure key distribution [3], there exist proposals using entangled states [4]. Indeed, it is unclear which role entanglement plays in quantum cryptography protocols. In this work, we analyze the problem of secret key extraction in the following scenario: after a distribution stage, two honest parties, Alice and Bob, share a quantum state. This state is translated into a probability distribution by local measurements at the single-copy level, and the obtained outcomes are processed in order to distill a secret key. We denote by SIMCAP this *single-copy measurements plus classical processing* scenario. This is a common scenario in quantum information applications, where useful correlations are distributed between two or more parties by means of entangled states. For two-qubit systems and individual attacks, we prove that Alice and Bob can distill a key by a SIMCAP protocol if and only if they initially share an entangled state. Thus, two-qubit entanglement is indeed equivalent to secure key distribution.

Our result links the security of one-qubit channels with their entanglement capability. In the usual formulation of quantum cryptography, first a protocol for key distribution is proposed and later possible eavesdropping attacks on it are analyzed. However, one can reverse this standard presentation and, after specifying an eavesdropping attack, look for a secure key distribution protocol. This is indeed closer to what happens in a practical situation: the honest parties are connected by a given channel, denoted by Y , that is fixed and known. It depends on experimental parameters such as, for instance, dark counts or optical imperfections, and is the only nonlocal quantum resource

Alice and Bob share. From the quantum cryptography point of view, it is conservatively assumed that Eve has total access to the channel. This means that the definition of the quantum channel is equivalent to specify Eve's interaction with the sent states. When does a given channel allow the honest parties to securely establish a secret key in the SIMCAP scenario? Our results imply that a one-qubit channel is secure as soon as it allows entanglement distribution. Moving to a higher dimension, our results immediately hold for all those bipartite states, and corresponding channels, that are one-copy distillable. Thus, they suggest a complete equivalence between distillable entanglement and secure key distribution.

Let us start with the simplest case of two qubits. A two-qubit entangled state is locally prepared by Alice and one of the two qubits is sent to Bob through a quantum channel. Since the channel is not perfect, Alice and Bob end with a two-qubit mixed state, ρ_{AB} [5]. They attribute the channel to the eavesdropper, Eve, who interacts with the sent qubits. We assume, as is often done in many works on quantum cryptography, that Eve applies an individual attack: she lets independent auxiliary systems interact with each qubit and measures each system before the key extraction process [6]. Since Eve has perfect control on her interaction, the global state of the system is pure, $|\Psi_{ABE}\rangle$. The state shared by Alice and Bob is $\rho_{AB} = \text{tr}(|\Psi_{ABE}\rangle\langle\Psi_{ABE}|)$, while the global pure state including Eve reads

$$|\Psi_{ABE}\rangle = \sum_{i=1}^r \sqrt{r_i} |i\rangle |i_e\rangle, \quad (1)$$

where $|\Psi_{ABE}\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^r$, $\{r_i, |i\rangle\}$ define the spectrum of ρ_{AB} , r is its rank, and $|i_e\rangle$ is an orthonormal basis on Eve's space. By computing the Schmidt decomposition with respect to the partition $AB - E$, one can easily see that any other state $|\tilde{\Psi}_{ABE}\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^{d_E}$, where $d_E \geq r$, such that $\text{tr}_E(|\tilde{\Psi}_{ABE}\rangle\langle\tilde{\Psi}_{ABE}|) = \rho_{AB}$, is completely equivalent to $|\Psi_{ABE}\rangle$.

If ρ_{AB} is entangled, one can consider the following *fully quantum* protocol for key distribution. The honest parties run a quantum distillation protocol [7] that transforms many copies of the initial entangled state into fewer copies of a maximally entangled state [8]. In this way, Eve becomes uncorrelated to Alice and Bob, who can safely measure in one basis, say z , and obtain the secret key. Note that in these protocols the honest parties must be able to perform quantum operations on several copies of their local states. This is in strong contrast to the SIMCAP scenario where all the collective actions are performed at the classical level, while quantum physics is used only for the correlation distribution. Does this limit the possibility of distilling a key?

It is worth mentioning here that the experimental requirements for the SIMCAP protocols are definitely less stringent for quantum distillation protocols. In particular, no quantum memory is needed, avoiding decoherence problems. Moreover, our scenario reflects precisely what is feasible with current technology, in contrast to joint operations and quantum memories, which are impossible on a large scale even in the near future.

Theorem: *Consider the situation in which Alice and Bob share unlimited many instances of a two-qubit state, ρ_{AB} . Under individual attacks, they can distill a secret key from them by measurements at the single-copy level and classical processing of the outcomes if and only if ρ_{AB} is entangled.*

Proof: It was shown in [9] that there exists a unique local filtering operation, $F_A \otimes F_B$ with $F_A^\dagger F_A \leq \mathbb{1}_2$ and $F_B^\dagger F_B \leq \mathbb{1}_2$, mapping with some probability any two-qubit state into a state diagonal in a Bell basis [10],

$$\rho'_{AB} = \Lambda_1 |\Phi^+\rangle\langle\Phi^+| + \Lambda_2 |\Psi^+\rangle\langle\Psi^+| + \Lambda_3 |\Psi^-\rangle\langle\Psi^-| + \Lambda_4 |\Phi^-\rangle\langle\Phi^-|. \quad (2)$$

The local bases can be chosen such that $|\Phi^+\rangle$ is the eigenvector associated with the largest eigenvalue, $\Lambda_1 = \max\{\Lambda_i\}$. This transformation maps entangled states into entangled Bell diagonal states [9]. After applying this filtering operation to ρ_{AB} , the honest parties share a Bell diagonal state (2), while the global state is

$$|\Psi'_{ABE}\rangle = \lambda_1 |\Phi^+\rangle|1\rangle + \lambda_2 |\Psi^+\rangle|2\rangle + \lambda_3 |\Psi^-\rangle|3\rangle + \lambda_4 |\Phi^-\rangle|4\rangle, \quad (3)$$

with $\lambda_i = \sqrt{\Lambda_i}$. Since the positivity of the partial transposition [11] is a necessary and sufficient condition for separability in $\mathbb{C}^2 \otimes \mathbb{C}^2$ systems, ρ'_{AB} is entangled if and only if

$$\Lambda_1 > \Lambda_2 + \Lambda_3 + \Lambda_4 = 1 - \Lambda_1. \quad (4)$$

After a successful local filtering, Alice and Bob measure ρ'_{AB} in the z basis, obtaining a partially correlated list of symbols, $\{a_i\}$ and $\{b_i\}$. The measurements in the z basis

terminate the measurement step in the SIMCAP distillation protocol [12]. From Eq. (3), Eve's non-normalized states, $|e_{AB}\rangle$, depending on Alice and Bob's results are, where $R = 0, 1, \dots$,

$$\begin{aligned} |e_{RR}\rangle &= \frac{1}{\sqrt{2}} [\lambda_1 |1\rangle + (-1)^R \lambda_4 |4\rangle], \\ |e_{R(1-R)}\rangle &= \frac{1}{\sqrt{2}} [\lambda_2 |2\rangle + (-1)^R \lambda_3 |3\rangle]. \end{aligned} \quad (5)$$

Note that Eve knows in a deterministic way whether Alice and Bob differ in their measurement outcomes (which implies $I_{AE} = I_{BE}$). This happens with probability

$$\epsilon_B = \|e_{01}\|^2 + \|e_{10}\|^2 = \Lambda_2 + \Lambda_3, \quad (6)$$

which is Bob's error probability.

In order to classically distill a key, Alice and Bob will now apply the advantage distillation protocol described in Ref. [13] to their measurement outcomes. If the state is close to $|\Phi^+\rangle$, the mutual information between the honest parties, I_{AB} , is larger than Eve's information, $I_E = \min(I_{AE}, I_{BE})$. Then, no advantage distillation protocol is, in principle, required, since privacy amplification [14], a more efficient key distillation protocol, suffices. Nevertheless, we deal with advantage distillation protocols because they allow us to extract a key even in situations where $I_{AB} \leq I_E$ [15]. The advantage distillation protocol works as follows: if Alice wants to establish the bit x with Bob, she randomly takes N items from her list of symbols, $\vec{a} = (a_1, a_2, \dots, a_N)$, and sends to Bob the vector \vec{x} such that $a_i + x_i = x \pmod{2}$, $\forall i = 1, \dots, N$, plus the information about the chosen symbols. Bob computes $b_i + x_i$, and whenever he obtains the same result, $b_i + x_i = y$, $\forall i$, he accepts the bit. If not, the symbols are discarded and the process is repeated for a new vector of length N . Bob's error probability is now [13]

$$\epsilon_{BN} = \frac{(\epsilon_B)^N}{(1 - \epsilon_B)^N + (\epsilon_B)^N} \leq \left(\frac{\epsilon_B}{1 - \epsilon_B} \right)^N, \quad (7)$$

that tends to an equality for $N \rightarrow \infty$.

Notice that for large N , $x = y$ with very high probability. Hence we concentrate on the states $|e_i\rangle \equiv |e_{ii}\rangle / \|e_{ii}\|$ and denote E_i the corresponding projectors. Eve applies generalized measurements (positive-operator-valued measurements) of M outcomes, $\sum_i M_i = \mathbb{1}_2$ with $M_i > 0$, trying to acquire information about these states. Indeed, since \vec{a} is chosen at random, we assume Eve's measurement to be the same for all qubits without losing generality. Moreover, any generic measurement can be seen as a measurement consisting of rank-one operators where some of the outcomes are later combined, so we can take $M_i = |m_i\rangle\langle m_i|$, $\forall i$, with $\|m_i\| \leq 1$. After the measurements, Eve uses all the information collected from the N symbols for guessing x . From \vec{x} , she knows that the bit string was equal to $\vec{a} = (a_1, a_2, \dots, a_N)$ or to $\vec{a}' = (1 - a_1, 1 - a_2, \dots, 1 - a_N)$, corresponding to

$1 - x$. Independently of her decision strategy, there are instances where she will make an error. For example, when the number of zeros in \vec{a} is the same as the number of ones (the same holds for \vec{a}'), and the number of times any measurement outcome has been obtained is the same for zeros and ones [16]. These events do not give her any information about x , so she is forced to guess and makes a mistake with probability $1/2$. Therefore, her error probability is bounded by

$$\epsilon_{EN} \geq \frac{1}{2} \frac{1}{2^N} \sum_{n_1, \dots, n_M} \frac{N!}{(2n_1)! \dots (2n_M)!} \binom{2n_1}{n_1} \text{tr}(E_0 M_1)^{n_1} \text{tr}(E_1 M_1)^{n_1} \dots \binom{2n_M}{n_M} \text{tr}(E_0 M_M)^{n_M} \text{tr}(E_1 M_M)^{n_M}, \quad (8)$$

with $2\sum_i n_i = N$. The factor $1/2^N$ takes into account the number of possible vectors \vec{a} , while the combinatorial terms count the number of vectors satisfying our requirements. When N is large, one can approximate the combinatorial term $(2n_i)!/(n_i!)^2 \approx 2^{2n_i}$ and then

$$\epsilon_{EN} \geq \frac{1}{2} \sum_{n_i} \frac{N!}{(2n_1)! \dots (2n_M)!} \prod_{i=1}^M [\text{tr}(E_0 M_i) \text{tr}(E_1 M_i)]^{n_i}. \quad (9)$$

In the same limit, this sum is equal to

$$\epsilon_{EN} \approx \frac{1}{2} \frac{1}{2^{M-1}} \left(\sum_{i=1}^M \sqrt{\text{tr}(E_0 M_i) \text{tr}(E_1 M_i)} \right)^N. \quad (10)$$

Since M_i are rank-one operators,

$$\sum_{i=1}^M \sqrt{\text{tr}(E_0 M_i) \text{tr}(E_1 M_i)} = \sum_{i=1}^M |\langle e_0 | M_i | e_1 \rangle| \geq |\langle e_0 | e_1 \rangle|, \quad (11)$$

where in the last step we used that $\{M_i\}$ is a resolution of the identity. These equations imply that, for large N , Eve's error probability is bounded by an exponential term $|\langle e_0 | e_1 \rangle|^N$. This bound is tight: a simple measurement in the x [i.e., $(|1\rangle \pm |4\rangle)/\sqrt{2}$] basis attains it (see Fig. 1).

Now, Alice and Bob can establish a key whenever

$$\frac{\epsilon_B}{1 - \epsilon_B} < |\langle e_1 | e_0 \rangle|, \quad (12)$$

since then [see Eq. (7)] Bob's error probability decreases exponentially faster than Eve's, and this condition is known to be sufficient for key distillation [17]. More precisely, if Eq. (12) is satisfied, there exists a finite N such that Alice and Bob, starting from the raw data and using this protocol, end with a smaller list of symbols where $I_{AB} > I_E$. Then, they can apply privacy amplification techniques [14] and distill a key. Using Eqs. (5) and (6), condition (12) can be shown to be equivalent to Eq. (4). Since Alice and Bob cannot establish a key when the state ρ_{AB} is separable [18], we conclude that a secret key can be distilled in the SIMCAP scenario if and only if the initially shared state is entangled. \square

Our results imply the equivalence between entanglement and security for qubit channels: if a one-qubit channel, \mathcal{Y} , allows one to distribute entanglement, key distribution is possible. Indeed, this means that there exists a bipartite state, $|\Phi\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$, such that

$$\rho_{AB}^\Phi = (\mathbb{1}_2 \otimes \mathcal{Y})(|\Phi\rangle) \quad (13)$$

is entangled. Alice can then prepare the state $|\Phi\rangle$ locally and send half of it to Bob through the noisy channel \mathcal{Y} . After this distribution stage, the honest parties run the presented SIMCAP protocol and distill a secret key from ρ_{AB}^Φ . Two points deserve to be mentioned here. First, note that if one places the state preparation on Alice's side, she can start with the state "as if it had passed her filter." And second, there is actually no need of entanglement in the protocol. Indeed, it can be translated into an equivalent protocol without entanglement using the ideas of Ref. [3]. Alice's measurement can be incorporated into the state preparation, before the state distribution. Then, she sends through the channel, with probability $1/2$, one of the two states $|\psi_B^\pm\rangle \in \mathbb{C}^2$, where

$$|\psi_B^\pm\rangle = \sqrt{2}(|\pm z\rangle \otimes \mathbb{1}_2)|\Phi\rangle. \quad (14)$$

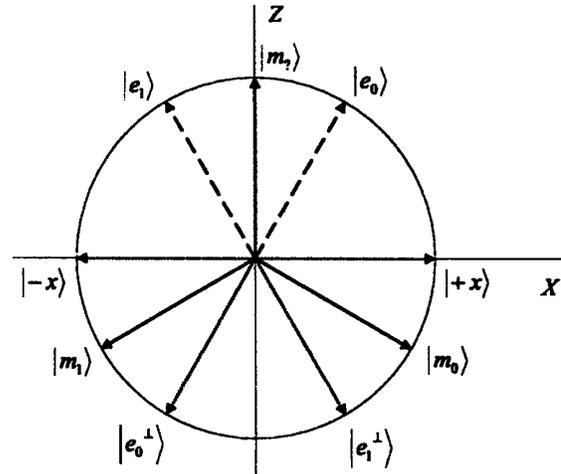


FIG. 1. Example of measurement attaining the bound of Eq. (11), where the first outcome, $|m_0\rangle$, is associated to 0, the second, $|m_1\rangle$, symmetric to $|m_0\rangle$ with respect to the z axis, to 1, and the third, $|m_2\rangle = |+z\rangle$, to an inconclusive result. The weight of $|m_2\rangle$ is minimized. One can consider similar three-outcome measurements, just changing the angle between $|m_0\rangle$, or $|m_1\rangle$, and the z axis. All the measurements such that $|m_0\rangle$ is between $|+x\rangle$ and $|e_1^\perp\rangle$ saturate the exponential bound. This does not mean that ϵ_{EN} is the same for all of them. The limiting cases, $|m_0\rangle = |e_1^\perp\rangle$ and $|m_0\rangle = |+x\rangle$, correspond to the optimal measurements for unambiguous discrimination and for maximizing Eve's information.

Bob receives the states $\rho_B^\pm = Y(|\psi_B^\pm\rangle)$. He applies the filter F_B and measures in the z basis. Of course, the obtained probabilities are exactly the same as in the SIMCAP protocol using $|\Phi\rangle$, so Alice and Bob can securely distill a key without using any entanglement.

For all the protocols, with and without entanglement, it is assumed that the channel is fixed. Note that for some channels, the states $|\psi_B^\pm\rangle$ may be orthogonal and form a basis. Eve could then replace her interaction by an intercept-resend attack: she measures in that basis and prepares a new state for Bob. But this would dramatically change the channel. Thus, Alice and Bob should randomly interrupt the key distribution and switch to a check stage where they monitor the channel. Entanglement is not required for this stage either. Those channels that do not allow one to distribute entanglement are called *entanglement breaking*. They can be written as [19]

$$Y(|\psi\rangle) = \sum_k \text{tr}(L_k |\psi\rangle\langle\psi|) \rho_k, \quad (15)$$

where ρ_k are density matrices and $\{L_k\}$ define a generalized measurement; i.e., $L_k \geq 0$ and $\sum_k L_k = \mathbb{1}_2$. From a cryptography point of view, this just represents an intercept-resend attack, as the one described above.

To conclude, we have seen that, under arbitrary individual attacks, a secret key can be established in the SIMCAP scenario if and only if the two-qubit state shared by Alice and Bob is entangled. This gives a one-to-one correspondence between two-qubit entanglement and secure key distribution: any one-qubit channel that is not entanglement breaking is secure. It would be interesting to extend our results to higher dimensional systems (preliminary results can be found in Ref. [20]), where there are entangled states, known as bound entangled [21], that are not quantum distillable. Our analysis can be trivially extended to the so-called one-copy distillable states, those states for which there exist local projections onto two-dimensional subspaces such that the resulting two-qubit state is entangled. The honest parties should simply include these projections as a first step in the measurement part of the distillation protocol. This fact suggests a complete equivalence between distillable entanglement and key distribution. According to it, the so-called entanglement binding channels, those channels through which only bound entanglement can be established [22], would be useless for key distribution, although this remains unproven. A related open question is the conjectured existence of a classical analog of bound entanglement, known as *bound information* [18], that seems to appear in some probability distributions $P(a, b, e)$ derived from bound entangled states.

This work has been supported by the ESF, by the Swiss NCCR, "Quantum Photonics," and by OFES within the

EU project RESQ (IST-2001037559), by Spanish Grant No. 2002FI-00373 UB and by the Generalitat de Catalunya.

-
- [1] See, for instance, M.A. Nielsen and I.L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
 - [2] N. Gisin *et al.*, *Rev. Mod. Phys.* **74**, 145 (2002).
 - [3] C.H. Bennett, G. Brassard, and N.D. Mermin, *Phys. Rev. Lett.* **68**, 557 (1992).
 - [4] A. Ekert, *Phys. Rev. Lett.* **67**, 661 (1991).
 - [5] Usually, Alice sends half of a maximally entangled state to Bob. Here, we aim to discuss the most general situation, with no constraints on ρ_{AB} . This is equivalent to the case where the state is prepared by an insecure source.
 - [6] This assumption excludes unconditional security.
 - [7] C.H. Bennett *et al.*, *Phys. Rev. Lett.* **76**, 722 (1996); D. Deutsch *et al.*, *Phys. Rev. Lett.* **77**, 2818 (1996).
 - [8] It was proven in M. Horodecki, P. Horodecki, and R. Horodecki, *Phys. Rev. Lett.* **78**, 574 (1997) that all two-bit entangled states are distillable.
 - [9] A. Kent, N. Linden, and S. Massar, *Phys. Rev. Lett.* **83**, 2656 (1999); F. Verstraete, J. Dehaene, and B. DeMoor, *Phys. Rev. A* **64**, 010101(R) (2001).
 - [10] The Bell basis is defined by the four orthonormal two-qubit maximally entangled states $|\Phi^\pm\rangle = (|00\rangle \pm |11\rangle)/\sqrt{2}$ and $|\Psi^\pm\rangle = (|01\rangle \pm |10\rangle)/\sqrt{2}$.
 - [11] A. Peres, *Phys. Rev. Lett.* **77**, 1413 (1996); M. Horodecki, P. Horodecki, and R. Horodecki, *Phys. Lett. A* **223**, 1 (1996). Given an operator on $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$, the partial transposition of O with respect to the first subsystem in the basis $\{|1\rangle, \dots, |d_1\rangle\}$ is $O^{T_1} \equiv \sum_{i,j=1}^{d_1} |i\rangle\langle j| O |j\rangle\langle i|$.
 - [12] The filter plus the z measurement can be seen as a single local measurement of three outcomes: 0, 1, and reject.
 - [13] N. Gisin and S. Wolf, *Phys. Rev. Lett.* **83**, 4200 (1999).
 - [14] I. Csiszár and J. Körner, *IEEE Trans. Inf. Theory* **24**, 339 (1978).
 - [15] U. M. Maurer, *IEEE Trans. Inf. Theory* **39**, 733 (1993).
 - [16] For large N , the first requirement is naturally satisfied by all the typical sequences.
 - [17] U. Maurer and S. Wolf, *IEEE Trans. Inf. Theory* **45**, 499 (1999).
 - [18] N. Gisin and S. Wolf, in *Proceedings of CRYPTO 2000*, Lecture Notes in Computer Science Vol. 1880 (Springer-Verlag, Heidelberg, 2000), p. 482.
 - [19] See M. Horodecki, P.W. Shor, and M. B. Ruskai, quant-ph/0302031, and references therein.
 - [20] A. Acín, N. Gisin, and V. Scarani, quant-ph/0303009; D. Bruß *et al.*, *Phys. Rev. Lett.* **91**, 097901 (2003).
 - [21] M. Horodecki, P. Horodecki, and R. Horodecki, *Phys. Rev. Lett.* **80**, 5239 (1998).
 - [22] P. Horodecki, M. Horodecki, and R. Horodecki, *J. Mod. Opt.* **47**, 347 (2000).