Quantum Correlations and Secret Bits

Antonio Acín[1] and Nicolas Gisin[2]

[1]*ICFO-Institut de Ciències Fotòniques, Jordi Girona 29, Edifici Nexus II, E-08034 Barcelona, Spain*
[2]*GAP-Optique, University of Geneva, 20, Rue de l'École de Médecine, CH-1211 Geneva 4, Switzerland*

(Received 21 October 2003; published 18 January 2005)

It is shown that (i) all entangled states can be mapped by single-copy measurements into probability distributions containing secret correlations, and (ii) if a probability distribution obtained from a quantum state contains secret correlations, then this state has to be entangled. These results prove the existence of a two-way connection between secret and quantum correlations in the process of preparation. They also imply that either it is possible to map any bound entangled state into a distillable probability distribution or bipartite bound information exists.

DOI: 10.1103/PhysRevLett.94.020501 PACS numbers: 03.67.Dd, 03.65.Ud, 03.67.Hk

Entanglement and secret correlations are fundamental resources in quantum information theory and cryptography, respectively. They both share the property of being *monogamous* [1], in the sense that the more two parties share quantum or secret correlations, the less they are correlated to the outside world. This fact suggests that these two concepts are closely related.

In the past years, several authors analyzed the link between quantum and secret correlations. Already in 1991, Ekert [2] proposed a cryptography protocol whose security was based on the violation of a Bell inequality [3]. More recently, this link has been exploited for proving the security of most of the existing quantum cryptography protocols, e.g., the Shor-Preskill proof [4] of the security of the Bennett-Brassard 1984 scheme [5]. Further relations were later analyzed in [6,7]. A qualitative equivalence between entanglement and key distillability has been shown in the cases of two-qubit and of one-copy distillable states [8]. There even exist quantitative analogies: the rates of entanglement and of secret-key distillability for some one-way communication protocols are equal [9]. All these results suggested the existence of a correspondence between entanglement and secret-key distillability, in the sense that a quantum state could be transformed into a private key if and only if it was distillable. However, the recent results of [10] have proven this statement to be false: there are nondistillable quantum states, also known as bound entangled, that are useful for establishing a secret key.

Up to now, the connection between quantum and secret correlations has mainly been analyzed from the point of view of distilling or extracting these resources from quantum states. However, very little is known about the process of preparation, i.e., about the resources required for the formation of a quantum state or a probability distribution. Recall that a state of a composite quantum system is entangled if and only if it cannot be prepared by local operations and classical communication (LOCC), that is, iff it requires truly quantum correlations (i.e., classical correlations are not sufficient for its preparation). In a similar way, for a given probability distribution, one may wonder what the cost of its distribution is, in terms of secret bits, when only classical resources are used. Following [11], we say that a probability distribution contains secret correlations if and only if it cannot be distributed using only local operations and public communication, that is, iff it requires the use of a private channel (i.e., public communication is not sufficient for its distribution).

In this work we study those probability distributions derived from single-copy measurements on bipartite quantum systems. We prove that (i) all entangled states can be mapped by single-copy measurements into probability distributions containing secret correlations and (ii) if a probability distribution containing secret correlations can be derived from a state ρ_{AB}, then ρ_{AB} has to be entangled. Accordingly, in strong contrast to the case of distillability, in the preparation process there exists a one-to-one relation between secret and quantum correlations. As far as we know, this result represents the first two-way connection between these two resources, entanglement and secret correlations. In particular, our results imply that all bound entangled states are useful to distribute secret correlations [12], a task that is impossible using only LOCC. But let us start reviewing some basic facts about entanglement and secret correlations.

In the modern theory of quantum correlations, the usual scenario consists of two parties, Alice and Bob, sharing a quantum state ρ_{AB} in a system $\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$. The impurity of the state is due to the coupling to the environment. The basic unit of entanglement is the entangled bit, or *ebit,* represented by a singlet state or a maximally entangled state of two qubits, $|\Psi^-\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$. Given ρ_{AB}, one would like to know (i) how many ebits are required for its preparation, and (ii) how many ebits can be extracted from it by LOCC. These two fundamental questions define the separability and distillability problems. Associated with them, there exist two entanglement measures, the so-called entanglement cost, E_c [13], and distillable entan-

glement, E_D [14]. Those states for which $E_c > 0$ require ebits for being prepared; they contain quantum correlations. Separable states can be prepared by LOCC [15], so $E_c = 0$.

Moving to secret correlations, the usual scenario consists of two honest parties, Alice and Bob, and an eavesdropper, Eve, having access to independent realizations of three random variables, X, Y, and Z, characterized by a probability distribution $P(X, Y, Z)$. Alice and Bob's symbols have some correlations, and they are also partially correlated with Eve. The basic unit is now the *secret bit,* that is, a probability distribution $P(X, Y, Z) = P(X, Y)P(Z)$ where X and Y are binary and locally random, $P(X = Y) = 1$, and Eve's symbols are decoupled from Alice and Bob's result. Similarly as above, given $P(X, Y, Z)$, one can look for the amount of secret bits (i) needed for its preparation and (ii) that can be extracted from it by local operations and public classical communication [6,7]. The corresponding measures are the so-called information of formation, $I_{\text{form}}(X; Y|Z)$, proposed in [11] as the classical analog of E_c, and the secret-key rate, $S(X; Y||Z)$, introduced in [16]. As for the entanglement scenario, a positive information of formation means that the correlations $P(X, Y, Z)$ cannot be distributed using only local operations and public communication—secret bits are needed. Therefore, $P(X, Y, Z)$ contains secret correlations iff $I_{\text{form}}(X; Y|Z) > 0$ [12].

All these measures, E_C and E_D as well as $S(X; Y||Z)$ and $I_{\text{form}}(X; Y|Z)$, have been defined from an operational point of view and are hard to compute. For our purpose, it is necessary to have bounds on these quantities. In the case of secret correlations, it is known that the so-called intrinsic information, $I(X; Y \downarrow Z)$, provides a lower bound to the information of formation [11] and an upper bound to the secret-key rate [16],

$$S(X; Y||Z) \leq I(X; Y \downarrow Z) \leq I_{\text{form}}(X; Y|Z). \tag{1}$$

This function, originally introduced in [16], is defined as follows: from $P(X, Y, Z)$ one can compute for any Z the conditioned probability distribution $P(X, Y|Z) = P(X, Y, Z)/P(Z)$. The total mutual information between X and Y conditioned on Z, $I(X; Y|Z)$, is the mutual information of $P(X, Y|Z)$ averaged over all Z. The intrinsic information then reads

$$I(X; Y \downarrow Z) = \min_{Z \to \bar{Z}} I(X; Y|\bar{Z}), \tag{2}$$

the minimization running over all the channels $Z \to \bar{Z}$.

In order to link quantum and secret correlations, we need two more remarks.

First, the adversary, Eve, appears in the quantum case in a less explicit way than in cryptography, where her presence is essential for the problem to be meaningful. If Alice and Bob share a state ρ_{AB}, the natural way of including Eve is to add a third system purifying it, in such a way that the global state of the three parties is $|\Psi_{ABE}\rangle \in \mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B} \otimes \mathbb{C}^{d_E}$ and $\rho_{AB} = \text{tr}_E(|\Psi_{ABE}\rangle\langle\Psi_{ABE}|)$. Thus, all the environment is conservatively associated with the adversary. Given ρ_{AB}, $|\Psi_{ABE}\rangle$ is uniquely specified up to an irrelevant unitary transformation on Eve's space [17].

Next, measurements are required for mapping the potential quantum correlations into probability distributions. We denote by M_Z the positive operators defining Eve's measurement, where $\sum_Z M_Z = \mathbb{1}_E$, and in a similar way M_X and M_Y define Alice and Bob's measurements. Thus, given a state $|\Psi_{ABE}\rangle$ and measurements for each party, the corresponding probability distribution is

$$P(X, Y, Z) = \text{tr}(M_X \otimes M_Y \otimes M_Z |\Psi_{ABE}\rangle\langle\Psi_{ABE}|), \tag{3}$$

while Alice and Bob's probability distribution is

$$P(X, Y) = \sum_Z P(X, Y, Z) = \text{tr}(M_X \otimes M_Y \rho_{AB}). \tag{4}$$

Notice that the map (3) is not one to one, since there may be many choices of measurements and states leading to the same probability distribution. And even if the measurements by Alice, Bob, and Eve are fixed, there may be many states compatible with Eq. (3). Therefore, $P(X, Y, Z)$ together with M_X, M_Y, and M_Z define equivalence classes in the space of states $|\Psi_{ABE}\rangle$ [18].

We have now introduced all the main ideas and can concentrate on the case where Alice and Bob perform local measurements M_X and M_Y on an unknown state ρ_{AB}. Assume that they can infer from their data $P(X, Y)$ that the state ρ_{AB} is entangled. Recall that the detection of entanglement through local measurements can always be done by means of an entanglement witness W, i.e., by measuring an observable in $\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$ such that for all product states $|ab\rangle$, $\langle ab|W|ab\rangle \geq 0$. Recall furthermore that all operators can be decomposed into a linear combination of product operators: $W(c_{XY}) = \sum_{X,Y} c_{XY} M_X \otimes M_Y$. Accordingly, whenever a linear combination of Alice and Bob local measurements provides an entanglement witness W, they can compute its expectation value from their data: $\text{tr}(W(c_{XY})\rho_{AB}) = \sum_{X,Y} c_{XY} P(X, Y)$. And whenever this expectation value is negative, Alice and Bob can conclude that the state ρ_{AB} they share is entangled. In such a case we say that the probability distribution, $P(X, Y)$, for the measurements M_X and M_Y *is incompatible with any separable state.* Actually, it was proven in [18] that Alice and Bob can discard any separable state as the origin of the observed correlations iff they can construct from their data an entanglement witness such that $\text{tr}(W(c_{XY})\rho_{AB}) < 0$. We can now state our main result.

Let $|\Psi_{ABE}\rangle$ be a quantum state shared by Alice, Bob, and Eve. The following two statements are equivalent: (1) Alice and Bob's state, ρ_{AB}, is entangled. (2) There exist measurements by Alice and Bob, M_X and M_Y, such that for any measurement by Eve, M_Z, the corresponding probability distribution $P(A, B, E)$ (3) contains secret correlations. This result is indeed a corollary of the following theorem.

Theorem.—Let $P(X, Y)$ be a probability distribution shared by Alice and Bob after measuring M_X, M_Y on a unknown state. Then, (i) $P(X, Y)$, for the measurements M_X and M_Y, is incompatible with any separable state (4) *if and only if* (ii) for all the purifications $|\Psi_{ABE}\rangle$, compatible with the observed data (4), and for all measurements M_Z by Eve, $P(X, Y, Z)$ contains secret correlations.

Proof: For the (i) $\Rightarrow$ (ii) part, assume that Alice and Bob detect the entanglement of the unknown state ρ_{AB} used for the correlation distribution by means of an entanglement witness $W(c_{XY}) = \sum_{X,Y} c_{XY} M_X \otimes M_Y$ built from their measurements, i.e., $\mathrm{tr}(W\rho_{AB}) < 0$. The proof proceeds by contradiction. Assume that there is a global state $|\Psi_{ABE}\rangle$ and a measurement by Eve, M_Z, such that the corresponding probability distribution $P(X, Y, Z) = \mathrm{tr}(M_X \otimes M_Y \otimes M_Z |\Psi_{ABE}\rangle\langle\Psi_{ABE}|)$ admits $P(X, Y)$ as marginal, but does not contain any secret correlations. This implies $I(X; Y \downarrow Z) = 0$ for $P(X, Y, Z)$; hence there is a channel $P(\bar{Z}|Z)$ such that $I(X; Y|\bar{Z}) = 0$, i.e.,

$$P(X, Y|\bar{Z}) = P(X|\bar{Z})P(Y|\bar{Z}). \tag{5}$$

Denote by ρ_Z the state shared by Alice and Bob when Eve's result is Z,

$$\rho_Z = \frac{1}{P(Z)} \mathrm{tr}_E(\mathbb{1} \otimes M_Z |\Psi_{ABE}\rangle\langle\Psi_{ABE}|), \tag{6}$$

where $P(Z) = \mathrm{tr}(\mathbb{1} \otimes M_Z |\Psi_{ABE}\rangle\langle\Psi_{ABE}|)$, and by $\rho_{\bar{Z}}$ the state after Eve's classical processing

$$\rho_{\bar{Z}} = \frac{1}{P(\bar{Z})} \sum_Z P(Z)P(\bar{Z}|Z)\rho_Z, \tag{7}$$

where $P(\bar{Z}) = \sum_Z P(Z)P(\bar{Z}|Z)$ and the positive operators $M_{\bar{Z}} = \sum_Z P(\bar{Z}|Z)M_Z$ define another measurement, since $\sum_{\bar{Z}} M_{\bar{Z}} = \mathbb{1}_E$ [19]. From Eq. (5) we have that $\forall\ X, Y$,

$$\mathrm{tr}(M_X \otimes M_Y \rho_{\bar{Z}}) = \mathrm{tr}(M_X \rho_{A\bar{Z}})\mathrm{tr}(M_Y \rho_{B\bar{Z}}), \tag{8}$$

where $\rho_{A\bar{Z}}$ ($\rho_{B\bar{Z}}$) denotes the state after tracing Bob (Alice) out in $\rho_{\bar{Z}}$. Define the separable state $\rho^S_{AB} = \sum P(\bar{Z})\rho_{A\bar{Z}} \otimes \rho_{B\bar{Z}}$. Using $\rho_{AB} = \sum_Z P(Z)\rho_Z = \sum_{\bar{Z}} P(\bar{Z})\rho_{\bar{Z}}$, it follows from Eq. (8) that

$$\mathrm{tr}(W\rho_{AB}) = \mathrm{tr}(W\rho^S_{AB}) < 0, \tag{9}$$

which is a contradiction with the assumption that W is an entanglement witness. Therefore, $I_{\mathrm{form}}(X; Y|Z) \geq I(X; Y \downarrow Z) > 0$ for all the states $|\Psi_{ABE}\rangle$ and all Eve's measurements. This concludes the (i) $\Rightarrow$ (ii) part of the proof.

For the (ii) $\Rightarrow$ (i) part, we proceed again by contradiction (see also [6,18]). Assume that there exists a separable state ρ_{AB} compatible with the observed data $P(X, Y)$. Since ρ_{AB} is separable, it can be expressed as

$$\rho_{AB} = \sum_{Z=1}^{n_Z} P(Z)|a_Z b_Z\rangle\langle a_Z b_Z|. \tag{10}$$

Consider the purification

$$|\Psi_{ABE}\rangle = \sum_{i=1}^{n_Z} \sqrt{P(Z)}\, |a_Z b_Z\rangle|Z\rangle, \tag{11}$$

where $|\Psi_{ABE}\rangle \in \mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B} \otimes \mathbb{C}^{n_Z}$ and $|Z\rangle$ are n_Z orthonormal vectors. If Eve applies the measurement defined by $M_Z = |Z\rangle\langle Z|$, we have that for all Alice and Bob's measurements

$$\begin{aligned} P(X, Y|Z) &= \mathrm{tr}(M_X \otimes M_Y |a_Z b_Z\rangle\langle a_Z b_Z|) \\ &= \mathrm{tr}(M_X |a_Z\rangle\langle a_Z|)\mathrm{tr}(M_Y |b_Z\rangle\langle b_Z|) \\ &= P(X|Z)P(Y|Z). \end{aligned} \tag{12}$$

Now, it is clear that these correlations could be generated as well using public communication. The random variables X and Y are locally generated according to one of the n_Z probability distributions $P(X|Z)$ and $P(Y|Z)$. The choice among these probability distributions is made according to the probability distribution $P(Z)$. Alice and Bob correlate this choice through the message Z that one of the parties generates and sends to the other through a public channel (or a source to both parties). This classical message is accessible to Eve. No secret bits are required for this distribution, thus $I_{\mathrm{form}} = 0$, which contradicts statement (ii). Hence there is no separable state ρ_{AB} compatible with the observed data $P(X, Y)$. □

Corollary.—Consider an entangled state $\rho_{AB} = \mathrm{tr}_E(|\Psi_{ABE}\rangle\langle\Psi_{ABE}|)$, where $|\Psi_{ABE}\rangle$ denotes the global state including Eve. There always exist measurements by Alice and Bob mapping this state into a probability distribution containing secret correlations, independently of Eve's measurement.

Proof: This easily follows from the previous theorem together with two known results: (i) any entangled state is detected by an entanglement witness [20], and (ii) any entanglement witness can be decomposed in terms of a tensor product of operators defining local measurements; i.e., it can be computed by local measurements [21]. □

These statements prove the announced "if and only if" connection between secret and quantum correlations in the process of preparation. Note that all the proofs have been derived using single-copy measurements. This fact allows one to easily translate our conclusions from entanglement based to prepare and measure protocols using the same ideas as in [22] (see also [18]). In the following lines, several implications of the results are discussed.

First, the presented connection is as strong as it could be. Consider that Alice and Bob are connected by an unknown quantum channel (share an unknown state). As soon as their measurement outcomes detect that the channel allows one to distribute entanglement, they know to share secrecy, no matter what Eve does [12]. Alice and Bob may not have enough information from the obtained measurement results to completely determine their channel. Still, if their data are only compatible with entanglement, the observed distribution contains secret bits. On the other hand, if the

measured correlations are compatible with a separable state, no secret key can be extracted from them [18]. Indeed, from the observed data Alice and Bob cannot exclude that $I(X;Y \downarrow Z) = 0$, which implies $S(X;Y||Z) = 0$. Thus, any entangling channel can be seen as a source of privacy.

Next, all this discussion is independent of the distillability properties of quantum states. Indeed, the previous corollary provides a systematic way of mapping bound entangled states into a probability distribution containing secrecy. An interesting open question is whether all these probability distributions are distillable into a perfect key (cf. [10]). It follows from our results that at least one of the two following possibilities must be true [23]: (i) all bound entangled states can be mapped into distillable probability distributions, or (ii) there exist classical probability distributions having nondistillable secret correlations. In this case, they would provide examples of bipartite probability distributions with bound information, the cryptographic analog of bound entanglement conjectured in [6] (see also [24]).

Finally, our results also shed light on what the differences between bound entangled states and the set of LOCC operations are. It is known that these states do not improve the fidelity of teleportation compared to LOCC [25]. On the other hand, there are examples of bound entangled states violating some inequalities for the variance of observables that are satisfied by separable states [26]. Moving to secret correlations, there exist bound entangled states that are useful for key distribution [10]. Here, it is proven that all bound entangled states can be transformed into probability distributions that, from the point of view of its secrecy features, can never be established by LOCC.

To conclude, in this work we have shown the correspondence between secret and quantum correlations in the process of preparation. Given a probability distribution, its formation using quantum resources needs entangled states if and only if an alternative preparation using classical resources requires secret bits.

This work is supported by the Swiss NCCR, ''Quantum Photonics,'' and OFES within the European project RESQ (IST-2001-37559), the Spanish MCyT, under ''Ramón y Cajal'' grant, and Generalitat de Catalunya.

[1] B. M. Terhal, IBM J. Res. Dev. **48**, 71 (2004).
[2] A. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[3] J. S. Bell, Physics **1**, 195 (1964).
[4] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[5] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.
[6] N. Gisin and S. Wolf, in *Proceedings of CRYPTO 2000*, Lecture Notes in Computer Science Vol. 1880 (Springer-Verlag, Berlin, 2000), p. 482.
[7] D. Collins and S. Popescu, Phys. Rev. A **65**, 032321 (2002).
[8] A. Acín, Ll. Masanes, and N. Gisin, Phys. Rev. Lett. **91**, 167901 (2003).
[9] I. Devetak and A. Winter, Phys. Rev. Lett. **93**, 080501 (2004).
[10] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, quant-ph/0309110.
[11] R. Renner and S. Wolf, in *Proceedings of Advances in Cryptology—EUROCRYPT 2003: International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, 2003*, Lecture Notes in Computer Science (Springer-Verlag, Berlin, 2003).
[12] Whether these secret correlations can be extracted or distilled into perfect secret bits, a key is a different, though related, problem that we do not consider here.
[13] P. M. Hayden, M. Horodecki, and B. M. Terhal, J. Phys. A **34**, 6891 (2001).
[14] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[15] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).
[16] U. Maurer and S. Wolf, IEEE Trans. Inf. Theory **45**, 499 (1999).
[17] L. P. Hughston, R. Josza, and W. K. Wootters, Phys. Lett. A **183**, 14 (1993).
[18] M. Curty, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. Lett. **92**, 217903 (2004).
[19] Note that the classical postprocessing, $P(\bar{Z}|Z)$, can always be included in Eve's measurement.
[20] M. Lewenstein, B. Kraus, J. I. Cirac, and P. Horodecki, Phys. Rev. A **62**, 052310 (2000).
[21] O. Guehne *et al.*, J. Mod. Opt. **50**, 1079 (2003).
[22] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
[23] Both possibilities can be true since (i) one can derive many probability distribution containing secret correlations from any bound entangled state, and (ii) bound information could be proven for probability distributions not associated with quantum states.
[24] The existence of bound information in a multipartite scenario has been shown in A. Acín, J. I. Cirac, and Ll. Masanes, Phys. Rev. Lett. **92**, 107903 (2004). The proof for the case of two honest parties still remains elusive.
[25] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. A **60**, 1888 (1999).
[26] H. F. Hofmann, Phys. Rev. A **68**, 034307 (2003); O. Gühne, Phys. Rev. Lett. **92**, 117903 (2004).