# Nonsecret correlations can be used to distribute secrecy

Joonwoo Bae,[1] Toby Cubitt,[2] and Antonio Acín[3,4]
[1]*School of Computational Sciences, Korea Institute for Advanced Study, Seoul 130-012, Korea*
[2]*Department of Mathematics, University of Bristol, University Walk, Bristol, BS8 1TW, United Kingdom*
[3]*ICFO-Institut de Ciències Fotòniques, Mediterranean Technology Park, 08860 Castelldefels (Barcelona), Spain*
[4]*ICREA-Institució Catalana de Recerca i Estudis Avançats, Lluis Companys 23, 08010 Barcelona, Spain*
(Received 17 June 2008; published 5 March 2009)

A counterintuitive result in entanglement theory was shown by Cubitt *et al.* [Phys. Rev. Lett. **91**, 037902 (2003)], namely, that entanglement can be distributed by sending a separable state through a quantum channel. In this work, following an analogy between the entanglement and secret-key distillation scenarios, we derive its classical analog: secrecy can be distributed by sending nonsecret correlations through a private channel. This strengthens the close relation between entanglement and secrecy.

DOI: 10.1103/PhysRevA.79.032304 PACS number(s): 03.67.Dd, 03.67.Mn, 03.65.Ud

## I. INTRODUCTION

Entangled and secret bits are different information resources that turn out to be closely connected. An entangled bit, or ebit, corresponds to a maximally entangled state of two qubits,

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \tag{1}$$

and represents the basic unit of bipartite entanglement [1]. A standard problem in entanglement theory is, given an arbitrary bipartite quantum state, $\rho_{AB}$, to determine how many ebits are required for its formation or can be distilled out of it by local operations and classical communication (LOCC).

On the other hand, secret bits are the basic unit of classical secret correlations. These arise when two honest parties, Alice and Bob, share correlated random variables, $A$ and $B$, whereas the eavesdropper, Eve, holds a third random variable $E$. The total correlations are then described by a tripartite probability distribution, $P(A,B,E)$. This distribution is a perfect secret bit whenever

$$P(A=B=0) = P(A=B=1) = \frac{1}{2},$$

$$P(A,B,E) = P(A,B)P(E).$$

Note that the Alice and Bob variables are perfectly correlated, while Eve gets no information whatsoever about them from her outcome. Similar to the case of quantum states, a basic question is to quantify the number of secret bits that are required to create a given tripartite probability distribution $P(A,B,E)$ or that can be distilled out of it by local operations and *public* communication (LOPC).

There exist several analogies between the entanglement properties of quantum states and the cryptographic properties of the classical probability distributions derived from them by local measurements [2,3]. In order to construct these analogies, one has to explicitly introduce a third party in the quantum scenario. This can easily be done by noting that any bipartite mixed state $\rho_{AB}$ can be seen as a tripartite pure state $|\psi\rangle_{ABE}$, such that $\mathrm{Tr}_E|\psi\rangle\langle\psi|_{ABE}=\rho_{AB}$. Indeed, the environment (that is, the part of the global system that is not under the honest party control) can naturally be associated with an adversary party, the eavesdropper. The goal is then to connect the entanglement properties of $\rho_{AB}$ to the cryptographic properties of those probability distributions $P(A,B,E)$ that can be written as

$$P(A,B,E) = \mathrm{Tr}(M_A \otimes M_B \otimes M_E|\psi\rangle\langle\psi|_{ABE}). \tag{2}$$

$M_A$, $M_B$, and $M_E$ are positive operators defining a quantum measurement in each local space, i.e., $\Sigma_i M_i = \mathbb{1}_i$ with $i=A,B,E$. Of course, the same rule can be applied in a multipartite scenario, where the quantum state $\rho_{ABC\ldots}$ is shared among $N$ parties.

A first rather trivial analogy follows from the fact that one secret bit can directly be obtained by measuring one ebit in, say, the computational basis. This simple observation is behind some of the security proofs of quantum key distribution protocols [4]. Beyond this basic analogy, other classical analogs of quantum information phenomena have been derived and vice versa. For instance, the results of [5] on the existence of what is called negative quantum information were translated into the classical scenario, obtaining analogous results for the secret-key rate [6]. In [7], a systematic way of mapping any entangled state onto a probability distribution containing secret correlations was derived. One of the nicest concepts in this direction is the existence of a cryptographic analog of bound entanglement, known as bound information, first conjectured in [3]. Recall that a quantum state is bound entangled when, despite being entangled, it is impossible to distill pure ebits out of it by LOCC. The existence and activation of nondistillable secret correlations has been demonstrated in [8] for the multipartite scenario, adapting some known results for multipartite bound entangled states. The existence of bipartite bound information remains an open question. Other results have followed the opposite direction, going from classical to quantum: the so-called squashed entanglement is an entanglement measure whose construction was inspired by a known upper bound on the secret-key rate [9]. In general, the connection between entangled states and secret correlations is a useful tool in the study of ebits and secret bits since it provides much insight into these two fundamental resources. Note, however, that this analogy is not a strict correspondence; there are "exceptions," such as the ex-

 

istence of bound entangled states that can be mapped into distillable probability distributions [10].

A remarkable result in entanglement theory was obtained in [11], where it was shown that entanglement can be distributed by sending a separable nonentangled state through a quantum channel. The scope of this work is to study whether a similar result holds for probability distributions. Following the analogy between ebits and secret bits, we indeed prove that this is the case; secret correlations can be distributed by sending nonsecret correlations through a private channel.

This paper is structured as follows. In Sec. II, we introduce the basic rules that apply when translating results from the quantum to the classical scenario and vice versa. Section III briefly reviews the results of [11], showing how to entangle two distant parties by sending a separable state. The main results are given in Sec. IV, where we show how to distribute secrecy by sending nonsecret correlations. Finally, we discuss some relevant issues and conclude.

## II. ENTANGLEMENT VERSUS SECRET CORRELATIONS

A standard scenario in entanglement theory consists of $N$ distant parties, $A,B,C\ldots$, who share quantum correlations described by a state $\rho$. The state may be mixed due to coupling to the environment, $E$, the overall state being $|\Psi\rangle$, where $\rho=\mathrm{Tr}_E|\Psi\rangle\langle\Psi|$. The two main questions in this scenario are the following: (i) is the preparation of $\rho$ possible by LOCC? (ii) If not, can pure ebits be distilled from $\rho$ by LOCC? These two questions define the separability and distillability problems. When considering the key-agreement scenario, many similarities appear (see for instance [2,3]). Now, $N$ distant honest parties and an eavesdropper share correlated random variables, described by a probability distribution $P(A,B,C,\ldots,E)$. The corresponding questions are the following: (i) can these correlations be established by LOPC? (ii) If not, can pure secret bits be distilled by LOPC?

Most of the analogies between the two scenarios can be summarized as follows:

| quantum entanglement | secret correlations |
|---|---|
| quantum communication | private communication |
| classical communication | public communication |
| local operations | local actions |

Here a private channel is a classical channel that is only accessible to the honest parties. Using these intuitive rules, one can often adapt results from entanglement theory to the secret correlation scenario and vice versa. For instance, a state is bound entangled whenever its formation by LOCC is impossible but nevertheless it cannot be transformed into pure ebits by LOCC. The corresponding concept for secret correlations, known as bound information, is simply given by a probability distribution that despite its formation by LOPC being impossible, it cannot be transformed into pure secret bits by LOPC.

More quantitative statements can be made in the bipartite case. In the case of quantum states, the ebit represents the basic unit of entanglement. The number of ebits per copy that can be distilled out of the copies of a given quantum state by LOCC defines the distillable entanglement, $E_D$ [12]. The corresponding classical analog is the secret-key rate $S(A:B\|E)$ which gives the number of secret bits distillable from $P(A,B,E)$ by LOPC [13]. In a similar way, the number of ebits required per copy for the formation of an entangled state defines the entanglement cost, $E_C$. The so-called information of formation, $I_c(A;B|E)$, introduced in [14], represents its classical analog. A probability distribution contains secret correlations if, and only if, its information of formation is nonzero [14].

A useful upper bound for $S(A:B\|E)$ is given by the so-called intrinsic information [13]. The intrinsic information between $A$ and $B$ given $E$ is defined as

$$I(A:B\downarrow E)=\min_{E\to\tilde{E}} I(A:B|\tilde{E}), \tag{3}$$

where the minimization runs over all possible stochastic maps $P(\tilde{E}|E)$ defining a new random variable $\tilde{E}$. The quantity $I(A:B|E)$ is the mutual information between $A$ and $B$ conditioned on $E$. It can be written as

$$I(A:B|E)=H(A,E)+H(B,E)-H(A,B,E)-H(E),$$

where $H(X)$ is the Shannon entropy of the random variable $X$. It also gives a lower bound on the information of formation [14], thus

$$S(A:B\|E)\leq I(A:B\downarrow E)\leq I_c(A;B|E). \tag{4}$$

In fact, $I_c(A;B|E)>0$ if, and only if, $I(A:B\downarrow E)>0$ [14]. The intrinsic information plays a key role in the proof of our results.

## III. QUANTUM SCENARIO

Before presenting our results, we summarize the findings of Ref. [11] on the distribution of entanglement by means of a separable state. The scenario consists of two initially uncorrelated distant parties who are connected by a classical and a quantum channel [15]. In order to entangle two distant qubits, $A$ and $B$, the parties must use the quantum channel since no entanglement can be created by LOCC. Thus one of the parties, say Alice, should prepare an additional qubit, $C$, and send it to Bob. Clearly, a sufficient condition for entanglement distribution is that the mediating quantum particle $C$ is entangled with Alice's quantum system $A$ so that Bob becomes entangled with her after receiving it. Intuitively, one would expect that this is also a necessary condition. Remarkably, this is not the case, as shown in Ref. [11], where an explicit counterexample is provided in which Alice distributes entanglement to Bob by sending a qubit $C$ through the quantum channel that is never entangled across the partition $C-AB$.

The example works as follows. Alice holds two qubits, $A$ and $C$, while Bob has one qubit, $B$, in the initial state

$$\rho_{ABC}=\frac{1}{6}\sum_{k=0}^{3}|\Psi_k,\Psi_{-k},0\rangle\langle\Psi_k,\Psi_{-k},0|+\sum_{i=0}^{1}\frac{1}{6}|i,i,1\rangle\langle i,i,1|, \tag{5}$$

where $|\Psi_k\rangle=(|0\rangle+e^{i\pi k/2}|1\rangle)/\sqrt{2}$. This state is fully separable across all partitions, so it can be prepared by LOCC. Alice now applies a controlled-NOT (CNOT) operation to her qubits, where $A$ ($C$) is the control (target) qubit, resulting in the state

$$\sigma_{ABC}=\frac{1}{3}|\Psi_{GHZ}\rangle\langle\Psi_{GHZ}|+\sum_{i,j,k=0}^{1}\beta_{ijk}|ijk\rangle\langle ijk|, \tag{6}$$

where $|\Psi_{GHZ}\rangle_{ABC}=(|000\rangle+|111\rangle)/\sqrt{2}$, $\beta_{001}=\beta_{010}=\beta_{101}=\beta_{110}=1/6$, and all other $\beta_{ijk}=0$. This state is still separable across the $C-AB$ partition [16]. Alice now sends $C$ to Bob, who applies a CNOT with $B$ ($C$) as the control (target) qubit. After all these steps, Alice and Bob share a state

$$\tau_{ABC}=\frac{1}{3}|\Phi^+\rangle\langle\Phi^+|_{AB}\otimes|0\rangle\langle 0|_C+\frac{2}{3}\mathbb{1}_{AB}\otimes|1\rangle\langle 1|_C, \tag{7}$$

where Bob has both $B$ and $C$. This state is distillable. Indeed, by measuring particle $C$ in the computational basis, the Alice and Bob systems are projected into a maximally entangled state of two qubits with a probability of 1/3.

## IV. TRANSLATED CLASSICAL SCENARIO

We now translate the previous quantum result to the key-agreement scenario. Namely, we show that secret correlations can be distributed by sending through the private channel a random variable that does not have secret correlations with either Alice or Bob. For the construction of the example, we can follow the "rules" given in Sec. II. Following Eq. (2), the initial quantum state (5) is replaced by the probability distribution obtained by measuring in the computational bases:

| $A$ | $B$ | $C$ | $E$ | $P(A,B,C,E)$ |
|---|---|---|---|---|
| 0 | 0 | 0 | $e_0$ | 1/6 |
| 0 | 1 | 0 | $e_{01}$ | 1/6 |
| 1 | 0 | 0 | $e_{10}$ | 1/6 |
| 1 | 1 | 0 | $e_0$ | 1/6 |
| 0 | 0 | 1 | $f_0$ | 1/6 |
| 1 | 1 | 1 | $f_1$ | 1/6 |

. (8)

Recall that for any separable state there exists an optimal measurement by Eve such that the intrinsic information for the obtained distribution (2) is zero for all choices of measurements by Alice and Bob [3]. However, Eve's optimal measurement is not necessarily in the computational basis. Thus, it is not immediate that distribution (8) contains no secret correlations. However, it is possible to prove that this is indeed the case; the distribution has zero intrinsic information across the bipartition $AC-B$, since $I(AC:B\downarrow E)=0$, which *does* imply that Alice and Bob do not share secret correlations.

Indeed, this can be seen more directly. Consider the following protocol. First, Alice tosses a biased coin that gives tails with a probability of 2/3 and heads with a probability of 1/3, and announces the result publicly. This establishes the value for the random variable $C$, namely, 0 stands for tails and 1 for heads. If the result was tails, Alice and Bob independently and privately each toss a fair coin, writing down the value 1 for heads and 0 for tails. If the biased coin came up heads, Alice tosses a fair coin, announces the result publicly, and Alice and Bob both write down 1/0 for heads/tails. Now, if Eve has eavesdropped on all the public communication, this results in something similar to distribution(8) but without the subscripts on Eve's labels $e$. Clearly, since it was created by LOPC, Alice and Bob cannot share any secret correlations at the end of this protocol. But the resulting distribution is even stronger than distribution (8) in the sense that Eve has even less information; by giving Eve the additional information about Alice and Bob's bits when $C=0$ and $A+B=1$, which certainly cannot increase the secret correlations between Alice and Bob, we arrive at distribution (8), which therefore also contains no shared secrecy.

Having prepared this distribution, Alice now performs the (classical) CNOT operation on $A$ and $C$, and sends $C$ through the private channel to Bob, who performs the CNOT operation on $B$ and $C$. Note that this is the *only* use of the private channel required by Alice and Bob yet it will turn out that $C$ does not carry any secrecy. After Alice's CNOT, the probability distribution is

| $A$ | $B$ | $C$ | $E$ | $P(A,B,C,E)$ |
|---|---|---|---|---|
| 0 | 0 | 0 | $e_0$ | 1/6 |
| 0 | 1 | 0 | $e_{01}$ | 1/6 |
| 1 | 0 | 1 | $e_{10}$ | 1/6 |
| 1 | 1 | 1 | $e_0$ | 1/6 |
| 0 | 0 | 1 | $f_0$ | 1/6 |
| 1 | 1 | 0 | $f_1$ | 1/6 |

. (9)

This distribution has zero intrinsic information across the partition $C-AB$. Indeed, consider the map $E\rightarrow\bar{E}$ in which Eve replaces $f_0$ and $f_1$ by $e_0$ but leaves everything else untouched. The resulting probability distribution has $I(A:B|\bar{E})=0$, thus $I(AB:C\downarrow E)=0$ for (9). That is, since $C$ would still share no secret correlations with $A$ and/or $B$ even if Eve were to throw away some of her information, the $C$ that is sent through the private channel cannot possibly share any secret correlations with $A$ and/or $B$.

The final probability distribution between Alice and Bob, after Bob's CNOT, is

| $A$ | $B$ | $C$ | $E$ | $P(A,B,C,E)$ |
|---|---|---|---|---|
| 0 | 0 | 0 | $e_0$ | 1/6 |
| 0 | 1 | 1 | $e_{01}$ | 1/6 |
| 1 | 0 | 1 | $e_{10}$ | 1/6 |
| 1 | 1 | 0 | $e_0$ | 1/6 |
| 0 | 0 | 1 | $f_0$ | 1/6 |
| 1 | 1 | 1 | $f_1$ | 1/6 |

. (10)

We now show how Alice and Bob can distill one secret bit from this distribution. Bob holds two of the random variables, $B$ and $C$. He receives $C=0$ and $C=1$ with probabilities 1/3 and 2/3, respectively. By LOPC, Alice and Bob keep their outcome whenever $C=0$, otherwise they reject the instance. Thus, with probability 1/3, Alice and Bob (and Eve) are correlated according to:

| $A$ | $B$ | $C$ | $E$ | $P(A,B,C,E)$ |
|---|---|---|---|---|
| 0 | 0 | 0 | $e_0$ | 1/2 |
| 1 | 1 | 0 | $e_0$ | 1/2 |

which defines a perfect secret bit. Thus, Alice and Bob are able to distribute distillable secret correlations by sending a random variable, which does not itself have secret correlations, through a private channel.

## V. CONCLUDING REMARKS

In this work, we have constructed the cryptographic analog of the distribution of (distillable) entanglement by a separable state: (distillable) secrecy can be distributed by sending nonsecret correlations. This result is completely equivalent to its entanglement analog: the use of the quantum (private) channel is essential for the successful entanglement (secrecy) distribution, even though the mediating particle (random variable) never has quantum (secret) correlations with the sender and/or receiver.

At first sight, the existence of this cryptographic analog suggests some interesting possibilities. For instance, one might imagine that secrecy could be distributed by an untrusted messenger, Charlie, who after transmitting the relevant information could not break the established secret key. Clearly, this is not the case if the transmitter can later collaborate with the eavesdropper. Indeed, since the information is classical, Charlie can keep a perfect copy of the transmitted random variable, $C$, and give it to Eve. The channel is no longer private, and it is known that the distribution of secret correlations by LOPC is impossible.

One could however consider a less restrictive scenario, in which the transmitter is still untrusted, but it is assumed that he does not collaborate with Eve. Can Alice and Bob use the above protocol to distill a secret key against Eve and Charlie separately? Indeed, they can. However, a much simpler protocol already achieves this. Alice, Bob, and Eve initially share a public perfectly correlated bit, $P(a=b=e=0)=P(a=b=e=1)=1/2$. Of course, no key extraction is possible. Then, Alice generates a random bit which she sends to Bob via the messenger Charlie. Charlie leaves and may try to break the key, but he is not allowed to collaborate with Eve. When he delivers the random bit, Alice, Bob, and Charlie also share a perfectly correlated bit. It is clear that Alice and Bob can distill a key against Charlie and Eve (if they do not collaborate) by taking the Boolean XOR of their two bits.

## ACKNOWLEDGMENTS

This work was supported by the EU QAP project, the Spanish MEC under Grant No. FIS2007-60182, and Consolider-Ingenio QOIT projects, the Caixa Manresa, the Generalitat de Catalunya, the IT R&D program of MKE/IITA (Grant No. 2008-F-035-02), and the Korea Research Foundation (Grant No. KRF-2008-313-C00185).

[1] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, Phys. Rev. A **53**, 2046 (1996).
[2] D. Collins and S. Popescu, Phys. Rev. A **65**, 032321 (2002).
[3] N. Gisin, R. Renner, and S. Wolf, Algorithmica **34**, 389 (2002).
[4] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[5] M. Horodecki, J. Oppenheim, and A. Winter, Nature (London) **436**, 673 (2005).
[6] J. Oppenheim, R. Spekkens, and A. Winter, e-print arXiv:quant-ph/0511247, Phys. Rev. Lett. (to be published).
[7] A. Acín and N. Gisin, Phys. Rev. Lett. **94**, 020501 (2005).
[8] A. Acín, J. I. Cirac, and Ll. Masanes, Phys. Rev. Lett. **92** 107903 (2004); Ll. Masanes and A. Acín, IEEE Trans. Inf. Theory **52**, 4686 (2006).
[9] M. Christandl and A. Winter, J. Math. Phys. **45**, 829 (2004).
[10] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, Phys. Rev. Lett. **94**, 160502 (2005).
[11] T. S. Cubitt, F. Verstraete, W. Dür, and J. I. Cirac, Phys. Rev. Lett. **91**, 037902 (2003).
[12] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[13] U. Maurer and W. Wolf, IEEE Trans. Inf. Theory **45**, 499 (1999).
[14] R. Renner and W. Wolf, *Advances in Cryptology, EUROCRYPT 2003*, Lecture Notes in Computer Science Vol. 2656 (Springer-Verlag, Berlin, 2003), p. 562.
[15] This artificial distinction between the channels is made for the sake of clarity. Indeed, classical information can be sent through the quantum channel.
[16] W. Dür and J. I. Cirac, J. Phys. A **34**, 6837 (2001).