Multipartite classical and quantum secrecy monotones

N. J. Cerf,[1] S. Massar,[1,2] and S. Schneider[3]
[1]*Ecole Polytechnique, CP 165, Université Libre de Bruxelles, 1050 Brussels, Belgium*
[2]*Service de Physique Théorique, CP 225, Université Libre de Bruxelles, 1050 Brussels, Belgium*
[3]*Department of Chemistry, University of Toronto, Toronto, Ontario, Canada M5S 3H6*
(Received 19 February 2002; published 15 October 2002)

In order to study multipartite quantum cryptography, we introduce quantities which vanish on product probability distributions, and which can only decrease if the parties carry out local operations or public classical communication. These ''secrecy monotones'' therefore measure how much secret correlation is shared by the parties. In the bipartite case we show that the mutual information is a secrecy monotone. In the multipartite case we describe two different generalizations of the mutual information, both of which are secrecy monotones. The existence of two distinct secrecy monotones allows us to show that in multipartite quantum cryptography the parties must make irreversible choices about which multipartite correlations they want to obtain. Secrecy monotones can be extended to the quantum domain and are then defined on density matrices. We illustrate this generalization by considering tripartite quantum cryptography based on the Greenberger-Horne-Zeilinger state. We show that before carrying out measurements on the state, the parties must make an irreversible decision about what probability distribution they want to obtain.

DOI: 10.1103/PhysRevA.66.042309 PACS number(s): 03.67.Dd, 89.70.+c

I. INTRODUCTION

Quantum cryptography uses the uncertainty principle of quantum mechanics to allow two parties to communicate secretly [1]. It has been extensively studied during the last decade both theoretically and experimentally (see, e.g., [2] for a review). The basic idea of a quantum cryptographic protocol is that two parties, Alice and Bob, use a quantum communication channel to exchange an entangled state Ψ_{AB}. Local measurements yield correlated results and allow them to obtain a certain number of shared secret bits P^2_{AB} uncorrelated with Eve, defined by the probability distribution $P^2_{AB}(0,0)=P^2_{AB}(1,1)=1/2$. These resulting secret bits can then be used for secure cryptography, using, e.g., the one-time pad scheme. An eavesdropper, Eve, will necessarily disturb the quantum state Ψ_{AB} when attempting to get information on the secret bits, and will therefore be detected by Alice and Bob. A central problem of quantum cryptography is to establish the maximum rate at which Alice and Bob can establish a secret key for a given level of disturbance by Eve.

Independently of quantum cryptography, Maurer has introduced a paradigm for classical cryptography based on probabilistic correlations between two parties, Alice and Bob, and an eavesdropper Eve [3]. Specifically, suppose that Alice, Bob, and Eve have several independent realizations of their three random variables, each distributed according to the probability distribution P_{ABE}. The goal is for Alice and Bob to distill, from these realizations, a maximal number of shared secret bits P^2_{AB}. The tools available to Alice and Bob to perform this distillation are local operations and classical public communications (LOPC). An important question is to estimate the maximum rate at which the parties can generate the secret bits. Bounds on this secret bits distillation rate have been obtained in [4].

Quantum cryptography and Maurer's cryptographic paradigm are closely related. Indeed, after measuring their quantum bits, the parties *A*, *B*, and *E* end up in exactly the situation considered by Maurer. Therefore, distillation protocols used in Maurer's cryptographic scheme can be adapted to the quantum situation [5]. Moreover, ideas from quantum cryptography and quantum information theory have illuminated the structure of Maurer's cryptographic scheme [6].

In this paper, we will consider multipartite cryptography both from the point of view of Maurer's classical cryptographic scheme and from the point of view of quantum cryptography. As in the papers mentioned above, these two approaches are complementary. We show that putting ideas from these two approaches together provides insights into multipartite cryptography. Let us first consider the extension of Maurer's cryptographic scenario to more than two parties. One supposes that the different parties $A_1, A_2, \ldots, A_n, E$ possess independent realizations of $n+1$ random variables distributed according to the multipartite probability distribution $P_{A_1 A_2 \cdots A_n E}$, where *E* denotes the eavesdropper, as before. In this case, however, it is not obvious what the goal of the parties should be. For instance, in the case of three parties, one possible aim of the distillation process could be to maximize the resulting number of random bits shared between pairs of parties $P^2_{AB}P^2_{BC}P^2_{CA}$. Another goal could be to generate efficiently the tripartite probability distribution P^3 defined by $P^3_{ABC}(0,0,0)=P^3_{ABC}(1,1,1)=1/2$. This probability distribution allows any one of the parties to encrypt a message (by XORing it with his random variable and publicly communicating the result) in such a way that it can be decrypted by both the other parties independently. A third possibility could be to generate the probability distribution P^x_{ABC} in which any two random variables are independent random bits, while the third one is the XOR of the other two bits, $P^x_{ABC}(0,0,0)=P^x_{ABC}(1,1,0)=P^x_{ABC}(1,0,1)=P^x_{ABC}(0,1,1)=1/4$. This probability distribution allows any one of the parties to encrypt a message (by XORing it with his random variable and publicly communicating the result) in such a

way that it can only be decrypted if the other two parties get together and compute the XOR of their two random bits. This is known as secret sharing, see [7] for a discussion of quantum secret sharing.

One main result of the present paper is to show that in the multipartite case, the parties must decide before they start the distillation protocol which probability distribution they want to obtain. Making the wrong choice entails an irreversible loss. For instance, the parties will, in general, obtain more triplets P^3 if they directly distill to P^3 than if they first distill to another kind of probability distribution, say shared random bits between pairs of parties $P_{AB}^2 P_{BC}^2 P_{CA}^2$, and subsequently try to generate P^3 from these pairs of random bits. More generally, we address in this paper the question of the convertibility, using LOPC, of one multipartite probability distribution into another one.

As mentioned above, these issues can be generalized to quantum-mechanical systems in the context of quantum cryptography. We thus aim at addressing the same questions of convertibility between quantum multipartite density operators in this paper. An important potential application of this extension is to provide bounds on the yields of multipartite quantum cryptography. Indeed, in quantum cryptography, the parties start with a quantum state (in general, a mixed state) and, by carrying out local operations, measurements, and classical communication, they aim at obtaining a multipartite classical probability distribution (which can of course be viewed as a particular kind of mixed quantum state). Bounds on the interconvertibility of multipartite quantum states have been studied by several authors (see, for instance, [8–11]), but most of this work has focused on pure states. The interconvertibility of mixed states, and, in particular, applications to multipartite cryptography, have so far been relatively little studied. As an illustration, we consider in detail the case of quantum cryptography based on the Greenberger-Horne-Zeilinger (GHZ) state $\Psi_{GHZ}=(|000\rangle+|111\rangle)/\sqrt{2}$. By measuring Ψ_{GHZ} in the z basis the parties can obtain the probability distribution P^3, while by measuring in the x basis, they can obtain the probability distribution P^x. We show that the parties cannot obtain more than one P^3 or one P^x distribution per GHZ state. Combining this with the bounds stated above, we see that when extracting correlations from the GHZ state, the parties must make an irreversible choice of what kind of tripartite correlations they want to obtain.

In order to study these interconvertibility issues, we have developed a tool that we call *secrecy monotones*. These are functions of the multipartite probability distributions (or, more generally, of the quantum density operators) that can only *decrease* under local operations and public classical communication. Therefore, comparing the value of the monotone on the initial and the target probability distribution allows one to obtain an upper bound on the number of realizations of the target probability distribution that can be obtained from the initial probability distribution. In fact, the upper bounds obtained in [3] and in [4] on the secret key distillation rate in the bipartite case can be reexpressed in terms of the existence of certain bipartite secrecy monotones.

Monotones have proved to be extremely useful for the study of quantum entanglement (see, for instance, [12]), in which context they are called entanglement monotones. Our study of secrecy monotones is closely inspired by these works on entanglement monotones. Entanglement monotones are positive and vanish on unentangled density matrices, which implies that they measure the amount of entanglement in a density matrix. In a similar way, secrecy monotones are positive and vanish on product probability distributions (or product density operators), so that they measure the amount of both classical and quantum correlations between the parties. In the present paper, we introduce two information-theoretic multipartite secrecy monotones (called S_n and T_n), which can be viewed as the multipartite extension of the (classical or quantum) mutual information of a bipartite system. The definition of the quantum mutual information was discussed in [13], and its use in the context of quantum channels was investigated in detail in [14]. Here, this quantity is shown to be a monotone and is extended to multipartite systems. In particular, we discuss several applications of these monotones to the special case of three parties.

The paper is organized as follows. The initial sections of the paper are devoted exclusively to the classical secrecy monotones. We begin in Sec. II by giving a general definition of classical secrecy monotones and studying the implications of this definition. In Sec. III we introduce two specific multipartite secrecy monotones S_n and T_n, which are the multipartite generalization of the bipartite mutual entropy. Most of this section is devoted to proving that these functions obey all the properties of a secrecy monotone. In Sec. IV, we use these two secrecy monotones to study the particular case of tripartite cryptography. In particular we address the question raised above concerning the interconvertibility under LOPC of the probability distributions P_{AB}^2, P_{BC}^2, P_{CA}^2, P_{ABC}^3, and P_{ABC}^x. Finally, in Sec. V, we study the generalization of the classical secrecy monotones to quantum mechanics. In particular, we show that the monotones S_n and T_n have natural quantum analogs that have important applications to multipartite quantum cryptography. As an illustration, we study bounds on quantum cryptography based on the GHZ state.

II. PROPERTIES OF SECRECY MONOTONES

A. Defining properties

A secrecy monotone is a function M defined on multipartite probability distributions $P_{A_1A_2\ldots A_nE}$ which obeys a series of properties, which we now review and explain. (We restrict ourselves to the classical case, the quantum case will be analyzed in Sec. V.) We will denote the monotone by either $M(P_{A_1A_2\cdots A_nE})$ or $M(A_1{:}A_2{:}\cdots{:}A_n{:}E)$ where the semicolons separate the different parties.

The first two properties ensure that M provides a measure of the amount of correlation between the parties.

(a) *Semi-positivity*.

$$M(P_{A_1A_2\cdots A_nE})\geqslant 0. \tag{1}$$

(b) *Vanishing on product probability distributions*.

$$\text{If} \quad P_{A_1A_2\cdots A_nE} = P_{A_1E}P_{A_2E}\cdots P_{A_nE},$$

$$\text{then} \quad M(P_{A_1E}P_{A_2E}\cdots P_{A_nE}) = 0. \tag{2}$$

The next two properties express the monotonicity of M under LOPC, namely, the fact that M can only decrease if one of the parties performs some local operation (e.g., randomization) or publicly discloses (partly or completely) the value of his variable. Thus, these monotonicity properties imply that M describes the amount of correlation not shared with Eve. They also make M useful for studying the convertibility of one probability distribution into another.

(c) *Monotonicity under local operations*. Suppose that party A_j carries out a local transformation that modifies A_j to $\overline{A_j}$ according to the conditional probability distribution $P_{\overline{A_j}|A_j}$. Then M can only decrease:

$$\text{if} \quad P_{A_1\cdots\overline{A_j}\cdots A_nE} = P_{\overline{A_j}|A_j}P_{A_1\cdots A_j\cdots A_nE},$$

$$\text{then} \quad M(P_{A_1\cdots\overline{A_j}\cdots A_nE}) \leqslant M(P_{A_1\cdots A_j\cdots A_nE}). \tag{3}$$

(d) *Monotonicity under public communication*. Suppose that party j publicly discloses the value of $\overline{A_j}$, where $\overline{A_j}$ depends on j's variable A_j according to the conditional probability distribution $P_{\overline{A_j}|A_j}$. Then M can only decrease on average:

$$M(P_{A_1\cdots A_j\cdots A_nE|\overline{A_j}}) \leqslant M(P_{A_1\cdots A_j\cdots A_nE}). \tag{4}$$

The next two properties are important if the secrecy monotone is to provide information on the asymptotic rate of convertibility of one probability distribution into another. By this, we mean that the parties initially have a large number n of realizations of the probability distribution P^1 and want to obtain a large number m of realizations of the probability distribution P^2. Property (e) ensures that one can use the monotone M to study the asymptotic limit $n,m\to\infty$. Property (f) allows one to study the situation where one does not want to obtain the exact probability distribution $(P^2)^{\otimes m}$, but only a probability distribution that is close to $(P^2)^{\otimes m}$.

(e) *Additivity*.

$$M(P^1\otimes P^2) = M(P^1) + M(P^2). \tag{5}$$

Note that one may also impose only the weaker condition $M(P^{\otimes n}) = nM(P)$ (see [12] for a motivation for considering only this weaker condition in the case of entanglement).

(f) *Continuity*. $M(P)$ is a continuous function of the probability distribution P. We will not make more explicit the condition that this imposes on M since the monotones we will explicitly describe below are highly smooth functions of P. We refer to [12] where a weak continuity condition is introduced and motivated in the context of entanglement.

Finally, we introduce two additional properties which are natural to impose if the monotone is to measure the amount of secrecy shared by the parties $A_1\cdots A_n$, with E viewed as a hostile party. Indeed, these final properties express the fact that the secrecy can only increase if E looses information either by performing some local operation or by publicly disclosing (in part or totally) his variable.

(g) *Monotonicity under local operations by Eve*. Suppose that Eve carries out a local transformation which modifies E to $\overline{E}$ according to the conditional probability distribution $P_{\overline{E}|E}$. Then M can only increase:

$$\text{if} \quad P_{A_1\cdots A_n\overline{E}} = P_{\overline{E}|E}P_{A_1\cdots A_nE},$$

$$\text{then} \quad M(P_{A_1\cdots A_n\overline{E}}) \geqslant M(P_{A_1\cdots A_nE}). \tag{6}$$

(h) *Monotonicity under public communication by Eve*. Suppose that Eve publicly discloses the value of $\overline{E}$, where $\overline{E}$ depends on Eve's variable E according to the conditional probability distribution $P_{\overline{E}|E}$. Then M can only increase on average:

$$M(P_{A_1\cdots A_nE|\overline{E}}) \geqslant M(P_{A_1\cdots A_nE}). \tag{7}$$

B. Consequences of the defining properties

1. Upper bound on the yield

The most important consequence of the above properties is that a monotone allows one to obtain a bound on the rate at which a multipartite probability distribution P^1 can be converted into another probability distribution P^2 using LOPC. Suppose that the parties are able, using LOPC, to convert n realizations of P^1 into some realization of a probability distribution $P^{2'}$ which is close to m independent realizations of the desired probability distribution P^2:

$$(P^1)^{\otimes n} \underset{\text{LOPC}}{\to} P^{2'} \simeq (P^2)^{\otimes m}. \tag{8}$$

The yield of this distillation protocol is defined as

$$Y_{P^1\to P^2} = \frac{m}{n}. \tag{9}$$

The existence of a secrecy monotone M allows us to put a bound on the yield. Indeed, from Eq. (8), we have

$$M((P^1)^{\otimes n}) = nM(P^1) \geqslant M(P^{2'}) \simeq mM(P^2), \tag{10}$$

where we have used the defining properties of M (additivity, monotonicity, and continuity). Hence, using the positivity of M, we obtain

$$Y_{P^1\to P^2} \leqslant \frac{M(P^1)}{M(P^2)}. \tag{11}$$

2. Monotones that do not involve Eve

In practice, it is much easier to construct a restricted type of monotones M that are only defined on probability distributions $P_{A_1A_2\cdots A_n}$ that do not depend on E. These simple monotones are therefore applicable only to the cases where

Eve initially has no information about the probability distribution. It is these monotones which we will consider in most of this paper.

Importantly, one can easily extend such monotones M to more general monotones M defined on probability distributions $P_{A_1A_2\cdots A_nE}$ that also include initial correlations with Eve. The simplest way to carry out this extension is to calculate the probability distributions $P_{A_1A_2\cdots A_n|E}$ conditional on Eve's variable E, and then to average the value of M over the conditional probability distribution. This yields a monotone M_1:

$$M_1(P_{A_1A_2\cdots A_nE})=\sum_E P(E)M(P_{A_1A_2\cdots A_n|E}).$$

The monotone M_1 thus constructed obeys property (h), but in general does not obey property (g) [4].

In order to obtain a monotone that obeys both properties (g) and (h), before computing the conditional probability distribution $P_{A_1A_2\cdots A_n|E}$, we first need to take the minimum over Eve's operations. This transforms the variable E into $\overline{E}$ according to $P(\overline{E}|E)$. This procedure yields a new monotone $M_\downarrow$:

$$M_\downarrow(P_{A_1A_2\cdots A_nE})=\min_{P(\overline{E}|E)}\sum_{\overline{E}} P(\overline{E})M(P_{A_1A_2\cdots A_n|\overline{E}}). \tag{12}$$

Note that it is this second procedure that was used in [4] to obtain a strong upper bound on the rate of distillation of a secret key.

3. Extending monotones to more parties

A monotone defined on an n-partite probability distribution can be extended in a natural way to a monotone on a m-partite probability distribution with $m>n$. Let us illustrate this procedure in the case of a bipartite monotone $M_2(A:B)$ extended to a tripartite case. An example of a tripartite monotone for the variables A, B, and C is simply $M_2(AB:C)$ and can be interpreted as the bipartite monotone which would be obtained if parties A and B get together. We can of course group the parties in many different ways, and therefore $M_2(AC:B)$ and $M_2(BC:A)$ are two other independent tripartite monotones. These three monotones are distinct from the genuinely tripartite monotones that can be constructed on P_{ABC}, as we will show later on, and lead to independent conditions on the convertibility of tripartite distributions.

III. TWO CLASSICAL MULTIPARTITE SECRECY MONOTONES

We now introduce two information-theoretic multipartite secrecy monotones for n parties $A_1,\ldots,A_n$ (with $n\geqslant 2$) sharing some classical probability distribution $P_{A_1\cdots A_n}$. We shall suppose that Eve initally has no knowledge about the probability distribution. The generalization to the case where the probability distribution depends on E can, in principle, be done as discussed in Sec. II B 2, although we do not know of a systematic way to carry out the minimization over Eve's operations used to obtain the monotone $M_\downarrow$ in Eq. (12).

A. Amount of shared randomness between the parties: S_n

The first multipartite secrecy monotone is denoted by S_n and is defined by

$$S_n(A_1:\cdots:A_n)=H(A_1\cdots A_n)-\sum_{i=1}^{n} H(A_i|A_1\cdots A_{i-1}A_{i+1}\cdots A_n), \tag{13}$$

where $H(A)$ denotes the Shannon entropy of variable A distributed as P_A, that is, $H(A)=-\Sigma_a p_a\log_2 p_a$. Here $H(A|B)$ denotes the conditional entropy and is defined as $H(A|B)=H(AB)-H(B)$.

In order to provide a physical interpretation to S_n, we note that the first term on the right-hand side of Eq. (13) is the total randomness of the probability distribution $P_{A_1\cdots A_n}$, whereas the subtracted terms are the amounts of randomness that are purely local to each party. Thus S_n measures the number of bits of shared randomness between the n parties (irrespective of them being shared between two, three, or more parties, but not including the local randomness). On the basis of this interpretation it is natural that if one of the parties publicly reveals some of his data, this will decrease S_n since the total number of bits of shared randomness has decreased. This remark suggests that S_n should be a secrecy monotone. That this is indeed the case will be proven below.

We begin by introducing two alternative expressions for S_n:

$$S_n(A_1:\cdots:A_n)=\sum_{i=1}^{n} H(A_1\cdots A_{i-1}A_{i+1}\cdots A_n)-(n-1)H(A_1\cdots A_n) \tag{14}$$

and

$$S_n(A_1:\cdots:A_n)=I(A_1:A_2A_3\cdots A_n)+\sum_{i=2}^{n-1} I(A_i:A_{i+1}\cdots A_n|A_1\cdots A_{i-1}), \tag{15}$$

where $I(A:B)=H(A)+H(B)-H(AB)$ is the mutual information between A and B, while $I(A:B|C)=H(AC)+H(BC)-H(C)-H(ABC)$ is the conditional mutual information between A and B given C. The proof of these different equivalent expressions follows from the following recurrence relation for S_n:

$$S_n(A_1:\cdots:A_n)=S_{n-1}(A_1:\cdots:A_{n-1}A_n)+I(A_{n-1}:A_n|A_1\cdots A_{n-2}). \tag{16}$$

These expressions allow us to derive the following simple properties of S_n:

(1) S_n is symmetric under the interchange of any two parties A_i and A_j. This follows from Eq. (13).

(2) S_n is semipositive. This follows from Eq. (15) and from the positivity of the conditional mutual entropy, $I(A:B|C) \geqslant 0$, which itself follows from the strong subbadditivity of Shannon entropies. [Thus S_n statisfies condition (a) for a secrecy monotone.]

(3) S_n is additive [thus it satisfies condition (e) for a secrecy monotone].

(4) S_n vanishes on the product probability distribution $P = P_{A_1} P_{A_2} \ldots P_{A_n}$ [thus it satisfies condition (b) for a secrecy monotone].

(5) For two parties S_2 is the mutual information,

$$S_2(A:B) = H(A) + H(B) - H(AB) = I(A:B). \tag{17}$$

(6) S_n is a continuous function of $P_{A_1 \cdots A_n}$ [thus property (f) of secrecy monotones is satisfied].

B. Local increase in entropy to erase all correlations: T_n

The second secrecy monotone is defined as

$$T_n(A_1 : \cdots : A_n) = \sum_{i=1}^{n} H(A_i) - H(A_1 \cdots A_n). \tag{18}$$

In order to interpret this quantity we note that it is equal to the minimum relative entropy between the probability distribution $P_{A_1 \cdots A_n}$ and any product probability distribution $Q_{A_1} Q_{A_2} \cdots Q_{A_n}$ (with the minimum being attained when the Q_{A_i} are equal to the local distributions P_{A_i}):

$$\begin{aligned} T_n(A_1 : \cdots : A_n) &= D(P_{A_1 \cdots A_n} || P_{A_1} P_{A_2} \cdots P_{A_n}) \\ &= \min_{Q_{A_1} Q_{A_2} \cdots Q_{A_n}} D(P_{A_1 \cdots A_n} || Q_{A_1} Q_{A_2} \cdots Q_{A_n}), \end{aligned} \tag{19}$$

where $D(P_A || Q_A) = \Sigma_a P(a) \log_2 [P(a)/Q(a)]$ is the relative entropy between the distributions P and Q. In order to give an interpretation to T_n, we turn to the recent work of Vedral [15] (see also the review [16]), who gave an interpretation of a related quantity, the relative entropy of entanglement, as the minimum increase of entropy of *classically correlated* environments needed to erase all correlations between the parties sharing an entangled state. (The relative entropy of entanglement is the minimum relative entropy between the entangled state and any separable state.) This argument can easily be extended to the present situation whereupon one finds that T_n is the minimum increase of entropy of local *uncorrelated* environments if the parties erase all correlations between them by interacting locally with their environment.

To proceed, we note that T_n obeys the recurrence relation

$$T_n(A_1 : \cdots : A_n) = T_{n-1}(A_1 : \cdots : A_{n-1}) + I(A_n : A_1 \cdots A_{n-1}), \tag{20}$$

which allows us to derive the following expression:

$$T_n(A_1 : \cdots : A_n) = I(A_1 : A_2) + \sum_{i=2}^{n-1} I(A_1 \cdots A_i : A_{i+1}). \tag{21}$$

These expressions allow us to derive the following simple properties of T_n:

(1) T_n is symmetric under the interchange of any two parties A_i and A_j. This follows from Eq. (18).

(2) T_n is semipositive. This follows from Eq. (21).

(3) T_n is additive.

(4) T_n vanishes on product probability distribution $P = P_{A_1} P_{A_2} \cdots P_{A_n}$.

(5) For two parties T_2 is the mutual information,

$$T_2(A:B) = H(A) + H(B) - H(AB) = I(A:B). \tag{22}$$

(6) T_n is a continuous function of the probability distribution $P_{A_1 \cdots A_n}$.

C. Relation between S_n and T_n

For two parties, S_n and T_n coincide and are equal to the mutual entropy between the parties. Thus, S_n and T_n can be viewed as two (generally distinct) multipartite extensions of the mutual information of a bipartite system. That these two generalizations are generally distinct follows from the following relation between the two monotones:

$$\begin{aligned} &S_n(A_1 : \cdots : A_n) + T_n(A_1 : \cdots : A_n) \\ &\quad = \sum_{i=1}^{n} I(A_i : A_1 \cdots A_{i-1} A_{i+1} \cdots A_n). \end{aligned} \tag{23}$$

This expression will prove important in the interpretation of the monotones in the quantum case.

Let us note that linear combinations of T_n and S_n of the form

$$M_n = \lambda S_n + (1 - \lambda) T_n, \tag{24}$$

with $0 \leqslant \lambda \leqslant 1$, are monotones as well. For the case of three parties, we will prove below that *only* for this range of λ is M_n a monotone.

We have already shown that S_n and T_n satisfy the requirements (a),(b),(e),(f) for being a secrecy monotone. Let us now show that they also satisfy conditions (c) and (d). [Conditions (g) and (h) will not be considered, since initially Eve has no information about the probability distribution.]

D. Monotonicity of S_n and T_n under local operations

We now prove that S_n can only decrease under local operations. Local operations by party j correspond to carrying out a local transformation which modifies A_j to $\overline{A_j}$ according to the conditional probability distribution $P_{\overline{A_j}|A_j}$. For example, let us choose A_n to undergo such a transformation. We want to prove first that

$$S_n(A_1:\cdots:A_n) \geqslant S_n(A_1:\cdots:\overline{A}_n). \tag{25}$$

Using Eqs. (20) and (23), we find

$$S_n(A_1:\cdots:A_n) = -T_{n-1}(A_1:\cdots:A_{n-1}) + \sum_{i=1}^{n-1} I(A_i:A_1\cdots A_{i-1}A_{i+1}\cdots A_{n-1}A_n). \tag{26}$$

Clearly, only the second term on the right-hand side is affected by the local operation on A_n. As a consequence of the data processing inequality (see, e.g., [17]), one can show that each term of the summation can only decrease under the transformation $A_n \to \overline{A}_n$,

$$I(A_i:A_1\cdots A_{i-1}A_{i+1}\cdots A_{n-1}A_n) \geqslant I(A_i:A_1\cdots A_{i-1}A_{i+1}\cdots A_{n-1}\overline{A}_n). \tag{27}$$

For example, consider the term $i=1$ and write the mutual information $I(A_1:A_2\cdots A_n\overline{A}_n)$ in two equivalent ways:

$$I(A_1:A_2\cdots A_{n-1}\overline{A}_n) + I(A_1:A_n|A_2\cdots A_{n-1}\overline{A}_n) = I(A_1:A_2\cdots A_n) + I(A_1:\overline{A}_n|A_2\cdots A_n). \tag{28}$$

We have $I(A_1:\overline{A}_n|A_2\cdots A_n)=0$ since A_1 and $\overline{A}_n$ are conditionally independent given A_n. Using strong subadditivity $I(A_1:A_n|A_2\cdots A_{n-1}\overline{A}_n)\geqslant 0$, we conclude that $I(A_1:A_2\cdots A_n)\geqslant I(A_1:A_2\cdots A_{n-1}\overline{A}_n)$. Finally, as S_n is symmetric in all A_j, this proof is actually valid for local operation performed by all parties.

In order to prove the monotonicity of T_n under local operations, we assume, as above, that A_n undergoes a local transformation to $\overline{A}_n$, and prove that

$$T_n(A_1:\cdots:A_n) \geqslant T_n(A_1:\cdots:\overline{A}_n). \tag{29}$$

Using Eq. (20), we have

$$T_n(A_1:\cdots:A_{n-1}:\overline{A}_n) = T_{n-1}(A_1:\cdots:A_{n-1}) + I(\overline{A}_n:A_1\cdots A_{n-1}). \tag{30}$$

Again, due to the data processing inequality, the second term on the right-hand side cannot increase as a result of the local transformation on A_n, while the first term remains unchanged. This proves Eq. (29). Consequently, as T_n is symmetric in all A_j's, it can only decrease under local operations of any party.

E. Monotonicity of S_n and T_n under public classical communication

Now, let us consider the monotonicity of S_n and T_n under classical communications. Here, classical communication means that one party makes its probability distribution (partly or completely) known to all the other parties. Say, we choose the party A_1 to make $\overline{A}_1$ known to the public, where $\overline{A}_1$ is drawn from the conditional probability distribution $P_{\overline{A}_1|A_1}$. We want to prove that S_n is a monotone, that is,

$$S_n(A_1:\cdots:A_n) \geqslant S_n(A_1:\cdots:A_n|\overline{A}_1), \tag{31}$$

with the right-hand side term being the monotone S_n calculated from the probability distribution $P_{A_1\cdots A_n|\overline{A}_1=a}$, averaged over all values a of $\overline{A}_1$, or

$$S_n(A_1:\cdots:A_n|\overline{A}_1) = \sum_{i=1}^{n} H(A_1\cdots A_{i-1}A_{i+1}\cdots A_n|\overline{A}_1) - (n-1)H(A_1\cdots A_n|\overline{A}_1). \tag{32}$$

Using Eq. (15), we have

$$S_n(A_1:\cdots:A_n|\overline{A}_1) = I(A_1:A_2\cdots A_n|\overline{A}_1) + \sum_{i=2}^{n-1} I(A_i:A_{i+1}\cdots A_n|A_1\cdots A_{i-1}\overline{A}_1). \tag{33}$$

The knowledge of $\overline{A}_1$ clearly only changes a conditional mutual information if A_1 is *not* given. This is only the case in the first term on the right-hand side of the above equation. Finally, we can prove that this term only decreases under classical communication by writing the mutual information $I(A_1\overline{A}_1:A_2\cdots A_n)$ in two equivalent ways,

$$I(A_1:A_2\cdots A_n) + I(\overline{A}_1:A_2\cdots A_n|A_1) = I(\overline{A}_1:A_2\cdots A_n) + I(A_1:A_2\cdots A_n|\overline{A}_1). \tag{34}$$

We have $I(\overline{A}_1:A_2\cdots A_n|A_1)=0$ since $\overline{A}_1$ is independent of $A_2\cdots A_n$ conditionally on A_1. Then, using $I(\overline{A}_1:A_2\cdots A_n)\geqslant 0$, we find that

$$I(A_1:A_2\cdots A_n) \geqslant I(A_1:A_2\cdots A_n|\overline{A}_1), \tag{35}$$

which proves that S_n is a monotone when party A_1 makes $\overline{A}_1$ public. Since S_n is symmetric in all parties, we have also proven that it decreases on average under classical communication between all parties.

Let us finally prove the monotonicity of T_n under classical communications. If one of the parties, say A_1, makes $\overline{A}_1$ public, then T_n changes according to

$$T_n(A_1:\cdots:A_n) \geqslant T_n(A_1:\cdots:A_n|\overline{A}_1), \tag{36}$$

with the right-hand side term being the monotone T_n for the probability distribution $P_{A_1\cdots A_n|\overline{A}_1=a}$, averaged over all values a of $\overline{A}_1$, or

$$T_n(A_1:\cdots:A_n|\overline{A}_1) = \sum_{i=1}^{n} H(A_i|\overline{A}_1) - H(A_1\cdots A_n|\overline{A}_1). \tag{37}$$

Using Eq. (21), we have

$$T_n(A_1:\cdots:A_n|\overline{A}_1)=\sum_{i=1}^{n-1} I(A_1\cdots A_i:A_{i+1}|\overline{A}_1). \quad (38)$$

As proven above, we have for all the terms on the right-hand side,

$$I(A_1\cdots A_i:A_{i+1})\geqslant I(A_1\cdots A_i:A_{i+1}|\overline{A}_1), \quad (39)$$

which proves that T_n can only decrease under public communication of one party. This is true for all parties since T_n is a symmetric quantity.

IV. TRIPARTITE CLASSICAL SECRECY MONOTONES

A. Five independent tripartite secrecy monotones

For three parties *A*, *B*, and *C*, we have a closer look at the above secrecy monotones for classical probability distributions. We start by writing the monotones explicitly in terms of entropies or mutual informations:

$$S_3(A:B:C)=H(AB)+H(BC)+H(AC)-2H(ABC)$$
$$=I(A:BC)+I(B:C|A), \quad (40)$$

$$T_3(A:B:C)=H(A)+H(B)+H(C)-H(ABC)$$
$$=I(A:B)+I(AB:C). \quad (41)$$

In addition to these two tripartite monotones, we also have three other monotones $S_2(A:BC)=I(A:BC)$, $S_2(B:AC)=I(B:AC)$, and $S_2(C:AB)=I(C:AB)$, which consist of evaluating the bipartite monotone S_2 on the probability distribution obtained by grouping together any two of the three parties. Thus, there is a total of five tripartite secrecy montones. These monotones are not all linearly independent as Eq. (23) shows. However, none of these monotones can be written as a linear combination of the other monotones with only positive coefficients. For this reason these five monotones give independent constraints on the transformations that are possible under LOPC.

B. Five particular probability distributions

We begin by using these five tripartite monotones to investigate in detail five particular tripartite probability distributions. These five probability distributions play a particular role since they are, in a sense made precise below, the extreme points in a convex set. These five distributions consist of three bipartite distributions

$$P^2_{AB}(0,0)=P^2_{AB}(1,1)=1/2, \quad (42)$$

$$P^2_{AC}(0,0)=P^2_{AC}(1,1)=1/2, \quad (43)$$

$$P^2_{BC}(0,0)=P^2_{BC}(1,1)=1/2 \quad (44)$$

and two tripartite distributions

$$P^3_{ABC}(0,0,0)=P^3_{ABC}(1,1,1)=1/2 \quad (45)$$

TABLE I. Values of the secrecy monotones S_2, S_3, T_3 in the case of the joint probabilities P^2, P^3, P^x.

	$S_2(A:BC)$	$S_2(B:AC)$	$S_2(C:AB)$	$S_3(ABC)$	$T_3(ABC)$
P^2_{AB}	1	1	0	1	1
P^2_{AC}	1	0	1	1	1
P^2_{BC}	0	1	1	1	1
P^3_{ABC}	1	1	1	1	2
P^x_{ABC}	1	1	1	2	1

and

$$P^x_{ABC}(0,0,0)=P^x_{ABC}(1,1,0)=P^x_{ABC}(1,0,1)=P^x_{ABC}(0,1,1)$$
$$=1/4. \quad (46)$$

The first three probability distributions, Eqs. (42)–(44), are perfectly correlated shared random bits between two of the three parties; the fourth probability distribution, Eq. (45), is one shared random bit between the three parties; and the last probability distribution, Eq. (46), corresponds to the case where two parties have independent random bits while the third party has the exclusive OR (XOR) of these bits.

Table I lists for each of these probability distributions the values of the five tripartite monotones.

C. Converting a probability distribution into another

We can use this table to study which probability distributions can be converted into which others, and with what yield. The first thing we note from the table is that it forbids the conversion of a probability distribution P^x_{ABC} into a probability distribution P^3_{ABC} and vice versa, as $S_3(P^x_{ABC})>S_3(P^3_{ABC})$ and $T_3(P^3_{ABC})>T_3(P^x_{ABC})$. This can be understood in the following way. The number of shared random bits underlying the distribution P^x_{ABC} is two (two parties must have uncorrelated random bits), while it is only one for the distribution P^3_{ABC} (where the three parties share one common bit). Since the number of shared bits S_3 is a monotone, one cannot go from P^3_{ABC} to P^x_{ABC}. On the other hand, the number of bits that must be forgotten (or put in the environment) in order to get three independent bits is equal to two for the distribution P^3_{ABC} (two parties, say *B* and *C*, must randomize their bits), while it is only one for the distribution P^x_{ABC} (where it is enough that party *C* forgets its bit in order to get three independent bits). Since the number T_3 of bits that must be forgotten to get independent distributions is a monotone, one cannot go from P^x_{ABC} to P^3_{ABC}.

The above table also suggests that distillation procedures of the form $P^x_{ABC}\rightarrow P^2_{AB}$ or $P^3_{ABC}\rightarrow P^2_{AB}$ are possible. This is indeed the case: starting from P^x_{ABC}, the party *C* simply has to make its bit public in order to get P^2_{AB}, thereby reducing by one the number of shared bits S_3. If we start with P^3_{ABC} instead, the party *C* has to forget its bit, i.e., send it through a channel that completely randomizes it. Thus, one bit must be forgotten, reducing by one the monotone T_3.

The transformations $P_{ABC}^{3\otimes 2}\to P_{ABC}^{x}$ and $P_{ABC}^{x\otimes 2}\to P_{ABC}^{3}$ are also allowed by the above table of monotones, and we can check that they can actually be achieved. If the probability distribution is $P_{ABC}^{3\otimes 2}$ and the parties want to convert it into P_{ABC}^{x}, then A has to forget the first of the two bits it has, B has to forget the second, and C just takes the sum of the two bits it has, forgetting the individual values. Thus, three bits must be forgotten, reducing the value of T_3 from 4 to 1. To convert $P_{ABC}^{x\otimes 2}$ into P_{ABC}^{3} is a little bit more complicated. We start with A having the bits x and x', B having the bits y and y', and C having the bits $x+y$ and $x'+y'$. Now A makes x public and B makes y' public. From this, C can calculate y as well as x'. Then, C makes $y+x'$ public, which allows A (who still has x') to calculate y. Thus, every party knows the secret bit y, so we have got P_{ABC}^{3}. Here, three bits must have been made public, reducing the value of S_3 from 4 to 1.

The above table leaves open the question whether the conversion

$$P_{ABC}^{x}\otimes P_{ABC}^{3}\rightleftharpoons P_{AB}^{2}\otimes P_{BC}^{2}\otimes P_{AC}^{2} \tag{47}$$

is possible. We have not been able to devise a protocol that carries out this transformation. Such a protocol should not make any bit public, nor should the parties be allowed to forget a bit in order to keep the values of S_n and T_n constant. Ruling out this possibility would probably require an additional independent monotone, and the five monotones listed above are the only ones we know at present.

Let us note that in order to carry out the above conversions, we sometimes had to suppose that one of the parties forgets some of his information. In practice, this is obviously a stupid thing to do. Why to forget something you know? However, there may be an accident, say an irrecoverable hard disk crash, such that one of the parties has lost part or all of his data. In this case, the monotone T_n constrains how much secrecy is left among the parties. It would be interesting and important to study the restricted class of transformations in which the parties never forget their data (they would only be allowed to communicate classically). This would impose another constraint on the transformations that are possible.

D. Extremality of the five tripartite probability distributions

The above discussion raises the general question of the *reversible* conversion of one probability distribution into another. By this we mean that, in the limit of a large number of draws, it is possible to go from one probability distribution P_1 to another P_2 and back with negligible losses. In particular, in the tripartite case, one can enquire whether there are yields $y_1,\ldots,y_5$ such that the reversible conversion

$$P_{ABC}\rightleftharpoons P_{AB}^{2\otimes y_1}\otimes P_{BC}^{2\otimes y_2}\otimes P_{AC}^{2\otimes y_3}\otimes P_{ABC}^{x\otimes y_4}\otimes P_{ABC}^{3\otimes y_5} \tag{48}$$

is possible. Let us show that the five secrecy monotones introduced above leave open the possibility of the reversible distillation of Eq. (48). Whether this is possible in practice is an open question.

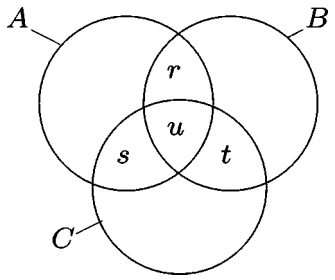

FIG. 1. Venn diagram for a tripartite probability distribution.

To prove this, let us introduce the following notation:

$$r=I(A{:}B|C),$$

$$s=I(B{:}C|A),$$

$$t=I(C{:}A|B),$$

$$u=I(A{:}B)-I(A{:}B|C). \tag{49}$$

Let us note that u is symmetric between the three parties and can also be written as $u=I(B{:}C)-I(B{:}C|A)=I(C{:}A)-I(C{:}A|B)$. These different quantities can be represented graphically as in Fig. 1.

Given these quantities we can express S_3 and T_3 as

$$S_3=r+s+t+u, \tag{50}$$

$$T_3=r+s+t+2u. \tag{51}$$

We note that u is not positive definite, but the additivity and strong subadditivity of Shannon entropies impose the positivity conditions

$$r\geqslant 0,$$

$$s\geqslant 0,$$

$$t\geqslant 0,$$

$$r+u\geqslant 0,$$

$$s+u\geqslant 0,$$

$$t+u\geqslant 0. \tag{52}$$

Using these conditions, one can show that if $u=0$, then the reversible conversion

$$P_{ABC}\rightleftharpoons P_{AB}^{2\otimes y_1}\otimes P_{BC}^{2\otimes y_2}\otimes P_{AC}^{2\otimes y_3}$$

is allowed by our tripartite monotones. If $u>0$, then the reversible conversion

$$P_{ABC}\rightleftharpoons P_{AB}^{2\otimes y_1}\otimes P_{BC}^{2\otimes y_2}\otimes P_{AC}^{2\otimes y_3}\otimes P_{ABC}^{3\otimes y_5}$$

is allowed by our tripartite monotones. If $u<0$, then the reversible conversion

$$P_{ABC}\rightleftharpoons P_{AB}^{2\otimes y_1}\otimes P_{BC}^{2\otimes y_2}\otimes P_{AC}^{2\otimes y_3}\otimes P_{ABC}^{x\otimes y_4}$$

is allowed by our tripartite monotones.

Thus our monotones, in principle, allow the reversible conversion between any tripartite probability distribution and the distributions P^2_{AB}, P^2_{BC}, P^2_{AC}, P^x_{ABC}, and P^3_{ABC}. Whether or not such a reversible transformation is possible is an open question. To rule this out will probably require discovering additional secrecy monotones.

E. Extremality of the monotones S_3 and T_3

As a final comment about the secrecy monotones in the tripartite case, we note that using the distillation procedures for $P^x_{ABC} \to P^2_{AB}$ and $P^3_{ABC} \to P^2_{AB}$, we can now also prove that $0 \leqslant \lambda \leqslant 1$ is the only range for which the linear combination of S_3 and T_3 is a monotone. This can be seen by calculating $M_3 = \lambda S_3 + (1-\lambda) T_3$ for both distillations. In the first case, we get that $M_3(P^x_{ABC}) = \lambda + 1$ should be greater or equal to $M_3(P^2_{AB}) = 1$, so that $\lambda \geqslant 0$. In the second case, we find that $M_3(P^3_{ABC}) = 2 - \lambda \geqslant M_3(P^2_{AB}) = 1$, so that $\lambda \leqslant 1$. This suggests that if there are other monotones than the M_n's, they will probably not be composed out of entropies.

V. QUANTUM MULTIPARTITE SECRECY MONOTONES

A. Definition of quantum secrecy monotones

The definition of classical secrecy monotone of Sec. II A can be immediately extended to the quantum case. In the case where there is no eavesdropper, the monotone will now be a function defined on multipartite density matrices $\rho_{A_1 \cdots A_n}$ which must be (1) semipositive, (2) vanishing on product density matrices $\rho_{A_1} \otimes \cdots \otimes \rho_{A_n}$, (3) monotonic under local operations [local completely positive (CP) maps], (4) monotonic under public classical communication, (5) additive, (6) continuous.

One can also extend the quantum definition of the secrecy monotone to the case where there is an eavesdropper. In that case, it is defined on a multipartite density matrix $\rho_{A_1 \cdots A_n E}$. The monotonicity properties are then modified to require that the secrecy montone is monotonically decreasing under local operations and public communication by the parties $A_1 \cdots A_n$ and monotonically increasing under local operations and public communication by Eve.

In what follows, we shall for simplicity not include Eve in the discussion, just as we did in the classical case. That is, we shall suppose that initially Eve has no information about the density matrix, but she listens to all public communications and thereby tries to thwart the parties $A_1 \cdots A_n$.

B. Quantum version of the secrecy monotones S_n and T_n

The definitions of the monotones S_n and T_n, Eqs. (14) and (18), have straightforward generalizations to the quantum case:

$$S_n(\hat{\rho}_{A_1 \cdots A_n}) \equiv S(A_1 : \cdots : A_n) = \sum_{i=1}^{n} S(\hat{\rho}_{A_1 \cdots A_{i-1} A_{i+1} \cdots A_n}) - (n-1) S(\hat{\rho}_{A_1 \cdots A_n}) \tag{53}$$

and

$$T_n(\hat{\rho}_{A_1 \cdots A_n}) \equiv T(A_1 : \cdots : A_n) = \sum_{i=1}^{n} S(\hat{\rho}_{A_i}) - S(\hat{\rho}_{A_1 \cdots A_n}), \tag{54}$$

where now $S(\hat{\rho})$ denotes the von Neumann entropy of a density matrix, which is given by $S(\hat{\rho}) = -\mathrm{Tr}(\hat{\rho} \log_2 \hat{\rho})$, and partial traces are written in the form $\hat{\rho}_{A_1 \cdots A_{i-1} A_{i+1} \cdots A_n} = \mathrm{Tr}_{A_i}(\hat{\rho}_{A_1 \cdots A_n})$.

The different rewritings of S_n [Eqs. (13), (15), and (16)] and T_n [Eqs. (20) and (21)] that were obtained in the classical case carry through to the quantum case, in analogy to what was shown for bipartite systems in [13]. This means that the simple properties that followed from these rewritings in the classical case also hold in the quantum case. In particular, the positivity of the S_n and T_n follows from the positivity of the conditional mutual entropy, which holds in both the classical and quantum case (see [18] for a review). The proofs of monotonicity are more involved in the quantum case, so we give them below.

Let us note that, for pure states, S_n and T_n coincide and are equal to the sum of the local entropies:

$$S_n(|\psi_{A_1 \cdots A_n}\rangle) = T_n(|\psi_{A_1 \cdots A_n}\rangle) = \sum_{i=1}^{n} S(\hat{\rho}_{A_i}). \tag{55}$$

Thus, for instance, on a singlet state, S_2 and T_2 are equal to 2, and on a GHZ state, S_3 and T_3 are equal to 3.

We do not at present have a clear interpretation of S_n in the quantum case. The reason is that S_n measures both the classical and the quantum correlations and does not distinguish them. On the other hand, the interpretation of T_n in the quantum case is the same as in the classical case. Indeed, it can be written as the minimum relative entropy between $\hat{\rho}_{A_1 \cdots A_n}$ and a product density matrix $\hat{\eta}_{A_1} \otimes \cdots \otimes \hat{\eta}_{A_n}$ (the minimum being attained when $\hat{\eta}_{A_i} = \hat{\rho}_{A_i}$). Therefore, T_n can be interpreted as the minimum increase of the entropy of local (uncorrelated) environments if the parties erase all correlations between them by letting their quantum systems interact with their local environment.

C. Monotonicity of S_n and T_n

We now give the proofs of monotonicity of S_n and T_n under local operations and public classical communication in the quantum case.

Local operations of one party are described mathematically as local CP maps M_{A_i}, which only act on the subspace of the ith party. We can assume that such a map is implemented as follows [20,21]: A_i adds to its Hilbert space the Hilbert space of an ancilla H_i^{aux}. The ancilla's initial state is $\Pi_{H_i^{aux}} = |0\rangle_{H_i^{aux}} \langle 0|$. It then carries out a unitary transformation $\hat{U}_{A_i H_i^{aux}}$ on its original system and the auxiliary variable. Finally, it traces over a part H_i' of its Hilbert space. Note that

H_i' does not have to coincide with H_i^{aux}. Hence, we can represent a local CP map as

$$\begin{aligned}\tilde{\rho}_{A_1\cdots A_n} &= M_{A_i}\otimes \mathbb{1}_{A_1\cdots A_{i-1}A_{i+1}\cdots A_n}(\hat{\rho}_{A_1\cdots A_i}) \\ &= \mathrm{Tr}_{H_i'}[(\hat{U}_{A_iH_i^{aux}}\otimes \mathbb{1}_{A_1\cdots A_{i-1}A_{i+1}\cdots A_n}) \\ &\quad\times(\hat{\rho}_{A_1\cdots A_n}\otimes \Pi_{H_i^{aux}}) \\ &\quad\times(\hat{U}^{\dagger}_{A_iH_i^{aux}}\otimes \mathbb{1}_{A_1\cdots A_{i-1}A_{i+1}\cdots A_n})]. \end{aligned} \tag{56}$$

We start with S_n and write it in the following form:

$$\begin{aligned} S_n(A_1:\cdots:A_n) &= \sum_{i=1}^{n-1} S_2(A_i:A_1\cdots A_{i-1}A_{i+1}\cdots A_{n-1}A_n) \\ &\quad -\Delta_n \end{aligned} \tag{57}$$

with

$$\Delta_n = \sum_{i=1}^{n-1} S(\hat{\rho}_{A_i}) - S(\hat{\rho}_{A_1\cdots A_{n-1}}). \tag{58}$$

Now we assume that the system A_n undergoes a local CP map M_n, Eq. (56). As Δ_n does not depend on A_n it remains unchanged, thus we only have to check S_2 for monotonicity. For this we rewrite Eq. (56) for two systems A and B,

$$\tilde{\rho}_{AB} = M_A\otimes \mathbb{1}_B(\rho_{AB}) = \mathrm{Tr}_{a'}[(U_{Aa}\otimes \mathbb{1}_B)\rho_{AB}\otimes \Pi_a(U_{Aa}^{\dagger}\otimes \mathbb{1}_B)] \tag{59}$$

and note that neither adding a local auxiliary system a nor performing a unitary transformation changes S_2. Tracing over a local subsystem, however, decreases S_2 since

$$S_2(A'H':B) - S_2(A':B) = S(H':B|A'), \tag{60}$$

which is just the conditional mutual quantum entropy and which, due to strong subadditivity [18], is semipositive, thus implying that

$$S_2(A'H':B) \geqslant S_2(A':B). \tag{61}$$

Due to symmetry, S_n given by Eq. (57) is then monotonic under local CP maps of any party.

For monotonicity under local measurements and public communication of their outcome, we assume that a positive operator valued measurement (POVM) [21] is performed on system A_1. This is realized by adding as above an ancilla $\Pi_{H_1^{aux}}$ to A_1 and then carrying out a von Neumann measurement that transforms $\hat{\rho}_{A_1\cdots A_n}\otimes \Pi_{H_1^{aux}}$ to

$$\tilde{\rho}_{H_1^{aux}A_1\cdots A_n} = \sum_k \hat{\rho}^k_{H_1^{aux}A_1\cdots A_n} = \sum_k p_k \tilde{\rho}^k_{H_1^{aux}A_1\cdots A_n}, \tag{62}$$

with

$$\begin{aligned}\hat{\rho}^k_{H_1^{aux}A_1\cdots A_n} &= (\hat{P}^k_{H_1^{aux}A_1}\otimes \mathbb{1}_{A_2\cdots A_n})(\hat{\rho}_{A_1\cdots A_n}\otimes \Pi_{H_1^{aux}}) \\ &\quad\times(\hat{P}^k_{H_1^{aux}A_1}\otimes \mathbb{1}_{A_2\cdots A_n})\end{aligned}$$

and $\hat{P}^k_{H_1^{aux}A_1}$ being a complete set of orthogonal projectors acting on the extended space of H_1^{aux} and A_1, $\tilde{\rho}^k_{H_1^{aux}A_1\cdots A_n}$ being the joint state after outcome k has been measured and $p_k = \mathrm{Tr}(\hat{\rho}^k_{H_1^{aux}A_1\cdots A_n})$ being the probability that outcome k occurs. We now go back to Eq. (53). The orthogonality of the projectors $\hat{P}^k_{H_1^{aux}A_1}$ implies that the $\tilde{\rho}_{A_1\cdots A_{i-1}A_{i+1}\cdots A_n}$ are block diagonal for $i\neq 1$, so that their entropies can be expressed as

$$\begin{aligned} S(\tilde{\rho}_{A_1\cdots A_{i-1}A_{i+1}\cdots A_n}) \\ = H[p_k] + \sum_k p_k S(\tilde{\rho}^k_{A_1\cdots A_{i-1}A_{i+1}\cdots A_n}) \end{aligned} \tag{63}$$

and

$$S(\tilde{\rho}_{A_1\cdots A_n}) = H[p_k] + \sum_k p_k S(\tilde{\rho}^k_{A_1\cdots A_n}), \tag{64}$$

with $H[p_k]$ denoting the Shannon entropy of the probability distribution p_k. For $i=1$, we find the following inequality for the first term, which makes use of the concavity of entropy

$$S(\tilde{\rho}_{A_2\cdots A_n}) \geqslant \sum_k p_k S(\tilde{\rho}^k_{A_2\cdots A_n}). \tag{65}$$

Replacing all these expressions in Eq. (53), we finally find that

$$S_n\left(\sum_k p_k \tilde{\rho}^k_{A_1\cdots A_n}\right) \geqslant \sum_k p_k S_n(\tilde{\rho}^k_{A_1\cdots A_n}). \tag{66}$$

This shows that the monotone S_n can only decrease on average if A_1 performs a POVM measurement and the outcome is made known to the other parties. By symmetry, this property holds for all A_i, $i=\{1,\ldots,n\}$.

To prove the monotonicity of T_n we proceed as follows. Suppose that A_1 carries out a local CP map. As before, adding a local ancilla and carrying out a local unitary transformation do not change T_n. Tracing over part of A_1's Hilbert space decreases T_n. Indeed,

$$\begin{aligned} T_n(A_1a_1:A_2:\cdots:A_n) - T_n(A_1:\cdots:A_n) \\ = S(a_1:A_2\cdots A_n|A_1) \geqslant 0. \end{aligned} \tag{67}$$

Suppose now that A_1 carries out a measurement (with outcome k) and publicly reveals the result. In Eq. (54), the terms $S(\rho_{A_i})$ with $i\neq 1$ decrease because of the concavity of

entropy [see Eq. (65)] and because the term $S(\rho_{A_1}) - S(\rho_{A_1\cdots A_n})$ stays constant [where we used Eqs. (63) and (64)]. Hence

$$T_n\left(\sum_k p_k \tilde{\rho}^k_{A_1\cdots A_n}\right) \geqslant \sum_k p_k T_n(\tilde{\rho}^k_{A_1\cdots A_n}; A_1 : \cdots : A_n), \tag{68}$$

where we have used the same notation as in Eq. (66).

D. Applications of quantum secrecy monotones

The two quantum monotones described above can be used to provide bounds on the rate of conversion of one multipartite density matrix into another using local operations and classical communication. As an example, we study in this section and the next one how many realizations of a correlated tripartite probability distributions can be obtained from a GHZ state.

Let us recall that the GHZ state, in the z basis, is

$$|\mathrm{GHZ}\rangle = (|000\rangle + |111\rangle)/\sqrt{2}.$$

If the state is measured in the z basis one obtains the probability distribution P^3. In contrast, if the state is measured in the x basis one obtains the probability distribution P^x.

We have shown above that P^3 and P^x cannot be reversibly converted one into the other. This therefore suggests that when using a GHZ state to do multipartite quantum cryptography, there is an irreversible choice that must be made. However, the above discussion leaves open the possibility that the three parties could use a more sophisticated strategy than those just described and thereby obtain more than one of these probability distributions from a single GHZ state.

To address this question, let us compute the monotones S_3 and T_3 on the initial state and on the final probability distributions. We find

$$\begin{aligned} S_3(|\mathrm{GHZ}\rangle) = 3, \quad T_3(|\mathrm{GHZ}\rangle) = 3, \\ S_3(P^3) = 1, \quad T_3(P^3) = 2, \\ S_3(P^x) = 2, \quad T_3(P^x) = 1. \end{aligned} \tag{69}$$

Thus the monotones leave open the possibility of a higher yield than one P^3 or one P^x per GHZ state.

Let us note, however, an interesting feature of Eq. (69), namely, that the sum of the final values of S_3 and T_3 is equal to half the sum of the initial values:

$$\begin{aligned} S_3(P^3) + T_3(P^3) &= S_3(P^x) + T_3(P^x) \\ &= \frac{S_3(|\mathrm{GHZ}\rangle) + T_3(|\mathrm{GHZ}\rangle)}{2}. \end{aligned} \tag{70}$$

We shall now show that this is no accident but is necessarily the case when one passes from a multipartite pure state to a multipartite probability distribution. Thus it is indeed impossible to obtain more than one P^3 or one P^x probability distribution from a single GHZ state, and the simple measurement strategies described above are therefore optimal.

E. Decrease of $S_n + T_n$ when converting a multipartite pure state into a multipartite probability distribution

Let us suppose that initially the parties share a multipartite *pure* state $|\Psi_{A_1\cdots A_n}\rangle$. Initially

$$S_n(|\Psi_{A_1\cdots A_n}\rangle) = T_n(|\Psi_{A_1\cdots A_n}\rangle) = \sum_i S(\rho_{A_i}). \tag{71}$$

Suppose that the aim of the parties is to obtain, by carrying out local measurements and classical communication, a multipartite probability distribution $P_{A_1\cdots A_n}$. In doing so, the monotones S_n and T_n will decrease. More precisely, the amount by which they decrease is such that their sum is decreased by at least a factor 2:

$$S_n(P_{A_1\cdots A_n}) + T_n(P_{A_1\cdots A_n}) \leqslant \sum_i S(\rho_{A_i}). \tag{72}$$

To prove this, let us first consider the bipartite case. Thus the parties initially share a pure state $|\Psi_{AB}\rangle$ and they carry out measurements so as to obtain a probability distribution P_{AB}. Let us first suppose that no communication takes place between the parties. Then, it follows from Holevo's bound [19] that the mutual information between Alice and Bob after the measurement is necessarily less than the local entropies of the original state:

$$S(\rho_A) = S(\rho_B) \geqslant I(A:B). \tag{73}$$

Equality is attained in Eq. (73) only if they measure in the Schmidt basis.

Let us now show that Eq. (73) also holds if the parties communicate classically. We will suppose that the communication takes place in a series of rounds. During each round, one of the parties carries out a partial measurement on the state and communicates information to the other party. After all the communication has taken place the parties measure the states they are left with. Such a general protocol is difficult to analyze, but we can transform it into a simpler protocol. In the simpler protocol, during each round the party transmits all the information obtained by the partial measurement to the other party. This should be contrasted with the most general protocol in which only part of the information obtained by the measurement is transmitted. The simplification follows from the fact that we can divide the measurement into a first partial measurement in which the information transmitted to the other party is obtained, and a second partial measurement in which the information that was kept is obtained. But the second partial measurement could then as well be carried out during the next round. Repeating this reasoning round after round, we can construct a simpler protocol in which the information that is not communicated to the other party is acquired during the last round only.

In the case of the simplified protocol, one can easily show that Eq. (73) holds. Consider the first round. Suppose that Alice carries out a partial measurement. The measurement has outcomes k, with probabilities $p(k)$. The state if the outcome is k is Ψ^k_{AB}. Because of monotonicity of the quantum mutual information, we have

$$S(\rho_A) \geqslant \sum_k p(k) S(\rho_A^k). \tag{74}$$

The local entropies decrease (on average) due to the communication. The same will hold for all the subsequent rounds. Hence, Eq. (73) holds also if the parties carry out public communication. In fact the above reasoning shows that the optimal strategy is for the parties not to communicate, but simply to measure the state in the Schmidt basis.

Finally let us consider the multipartite case. The result for two parties, Eq. (73), implies that for any partition of the parties into one party, say i, and $n-1$ parties, the mutual information between i and the $n-1$ other parties after the measurements is bounded by

$$I(A_i : A_1 \ldots A_{i-1} A_{i+1} \ldots A_n) \leqslant S(\rho_{A_i}). \tag{75}$$

Summing over i and using Eq. (23), we find that

$$S_n(P) + T_n(P) \leqslant \sum_i S(\rho_{A_i}), \tag{76}$$

which is what we wanted to prove.

F. Application to the *W* state

As an additional application let us consider the W state $|W\rangle = (|100\rangle + |010\rangle + |001\rangle)/\sqrt{3}$, which seems to play a particular role in the classification of the tripartite states of two-dimensional systems [22]. It is natural in this case for the parties to measure the state in the computational basis which yields the probability distribution $P^W(100) = P^W(010) = P^W(001) = 1/3$. The secrecy monotones for the probability distribution P^W obey $S_3(P^W) = \log_2 3$ and $T_3(P^W) = 2\log_2 3 - 2$. One finds that $S_3(P^W) + T_3(P^W) = S(\rho_A^W) + S(\rho_B^W) + S(\rho_C^W)$, where $\rho_{A,B,C}$ are the reduced density matrices of the state $|W\rangle$. This shows that this measurement procedure extracts the maximum amount of classical secrecy from $|W\rangle$.

Let us note that the values of these secrecy monotones imply that P^W is not equivalent to either P^3 or P^x. However our monotones do not exclude the possibility of reversibly converting P^W into a product of $P_{AB}^2 \otimes P_{BC}^2 \otimes P_{CA}^2$ and P^x (see Sec. IV D), or because of the symmetry of the state, into a product of P^3 and P^x with appropriate weights. Thus, for instance, the operation $P^W \rightleftharpoons P^{x \otimes y_1} \otimes P^{3 \otimes y_2}$ may be possible for some yields y_1 and y_2. These questions are identical to those raised in Eq. (47) or at the end of Sec. IV D.

VI. CONCLUSION

In this paper, we have introduced the concept of secrecy monotones which are powerful tools to obtain bounds on the distillation rate in Maurer's classical cryptographic scheme as well as bounds on the distillation rate in quantum cryptography.

We introduced two independent multipartite secrecy monotones based on (Shannon or von Neumann) entropies S_n and T_n, which allowed us to investigate the distillation rates for multipartite cryptographic schemes. In the classical case, we studied in detail the tripartite case and showed that there are several inequivalent tripartite probability distributions in the sense that they cannot be converted reversibly one into the other. We also studied the particular case of tripartite quantum cryptography based on the GHZ state. We showed that the parties must choose *a priori* which probability distribution they want to generate when measuring the GHZ state.

The important feature that emerges from our study is thus that in multipartite classical or quantum cryptography, the parties must make an irreversible choice on what final probability distribution they want to obtain. Making the wrong choice entails an irreversible loss. We note that this feature is not unique to cryptography; indeed, a similar situation arises in multipartite entanglement distillation since there are entangled pure states that cannot be reversibly converted one into the other [8,9].

Note added. After this paper was completed, we learned of the work [23] in which monotones (under certain classes of operations) that are positive both on quantum states and probability distributions are considered in the bipartite case.

ACKNOWLEDGMENTS

We would like to thank Daniel Collins, Nicolas Gisin, and Sandu Popescu for helpful conversations. We acknowledge funding by the European Union under the project EQUIP (IST-FET program). S.M. is a research associate of the Belgian National Fund for Scientific Research.

[1] Ch.H. Bennett and G. Brassard, in *International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.
[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[3] U. Maurer, IEEE Trans. Inf. Theory **39**, 733 (1993).
[4] U. Maurer and S. Wolf, IEEE Trans. Inf. Theory **45**, 499 (1999).
[5] N. Gisin and S. Wolf, Phys. Rev. Lett. **83**, 4200 (1999).
[6] N. Gisin and S. Wolf, in *Advances in Cryptology*, edited by M. Bellare, Lect. Notes Comput. Sci. **1880**, 482 (2000).
[7] M. Hillery, V. Buzek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).
[8] C.H. Bennett, S. Popescu, D. Rohrlich, J.A. Smolin, and A.V. Thapliyal, Phys. Rev. A **63**, 012307 (2001).
[9] N. Linden, S. Popescu, B. Schumacher, and M. Westmoreland, e-print quant-ph/9912039.
[10] E.F. Galvao, M.B. Plenio, and S. Virmani, J. Phys. A **33**, 8809 (2000).
[11] M.B. Plenio and V. Vedral, J. Phys. A **34**, 6997 (2001).
[12] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **84**, 2014 (2000).

[13] N.J. Cerf and C. Adami, Phys. Rev. Lett. **79**, 5194 (1997); Physica D **120**, 62 (1998).
[14] C. Adami and N.J. Cerf, Phys. Rev. A **56**, 3470 (1997); N.J. Cerf, *ibid.* **57**, 3330 (1998).
[15] V. Vedral, Proc. R. Soc. London, Ser. A **456**, 969 (2000).
[16] V. Vedral, Rev. Mod. Phys. **74**, 197 (2002).
[17] T.M. Cover and J.A. Thomas, *Elements of Information Theory* (Wiley, New York, 1991).
[18] A. Wehrl, Rev. Mod. Phys. **50**, 221 (1978).
[19] A.S. Holevo, Probl. Peredachi Inf. **9**, 3 (1973).
[20] B. Schumacher, Phys. Rev. A **54**, 2614 (1996).
[21] K. Kraus, *States, Effects, and Operations* (Springer, Berlin, 1983).
[22] W. Dür, G. Vidal, and J.I. Cirac, Phys. Rev. A **62**, 062314 (2000).
[23] B.M. Terhal, M. Horodecki, D.W. Leung, and D.P. DiVincenzo, e-print quant-ph/0202044.