Multipartite Secret Correlations and Bound Information

Lluís Masanes*[†] and Antonio Acín[‡]

September 10, 2017

Abstract

We consider the problem of secret key extraction when n honest parties and an eavesdropper share correlated information. We present a family of probability distributions and give the full characterization of its distillation properties. This formalism allows us to design a rich variety of cryptographic scenarios. In particular, we provide examples of multipartite probability distributions containing non-distillable secret correlations, also known as bound information.

1 Introduction

Many cryptographic applications nowadays are based on *computational security*. In this type of protocols, the security is based on two assumptions: (i) the computational capabilities of an eavesdropper are bounded and (ii) a conjecture on the computational complexity of some mathematical problems. The advent of quantum computing however sheds doubts on the medium-term applicability of these schemes. Indeed, Shor's algorithm [16] will allow an eavesdropper provided with a quantum computer breaking many of the now commonly used schemes, such as RSA.

There is a second type of security which is clearly the strongest one: *information-theoretic security*. This type of protocols are secure against attacks using unlimited resources, since the security is simply guaranteed by known results of Information Theory. The first step in this direction was already given in 1949 by Shannon [15]: such a level of security could only be attained by honest parties initially sharing a secure secret key. An example of a completely secure way of information encryption is given by the one-time pad [18]: in this scheme the honest parties share a private key. The message is summed (XOR) bitwise with the common key and sent through the insecure public channel. The receivers owning the key can read the sent information performing a second bitwise XOR, while no information on the message is accessible to anybody with no access to the key. It turns out however that (i) this protocol works only when the parties willing to interchange the information share a private key of the same length as the message to be encrypted and (ii) the key cannot be reused. Moreover, the following question arises in a natural way: how is the key generated? It was later shown by Maurer that a secure key cannot be generated from nothing [11]. More precisely, the honest parties cannot establish a key by a protocol consisting of local operations and public communication (LOPC). Therefore, a necessary requirement for key-agreement is that the honest parties share prior correlations that are partially secret.

These pessimistic statements were somehow relativized in [11, 12], where it was proven that an arbitrary weak level of correlation and privacy can be in some cases sufficient for generating a key. Furthermore, Quantum Cryptography protocols [2, 8] have been shown to provide an efficient way for establishing these initial partially secret correlations. Indeed, it is a crucial problem in most of Quantum Cryptography protocols how to transform into a perfect secret key the noisy and partially secret data dis-

*School of Mathematics, University of Bristol, Bristol BS8 1TW, United Kingdom

[†]Dept. d'Estructura i Constituents de la Matèria, Univ. de Barcelona, 08028 Barcelona, Spain

[‡]ICFO-Institut de Ciències Fotòniques, Jordi Girona 29, Edifici Nexus II, 08034 Barcelona, Spain

tributed among the honest parties through quantum channels. As said, this key will later be consumed for sending private information by means of one-time pad.

In this work, we study the inter-conversion among different kinds of secret correlations in a multipartite scenario, where n honest parties and an eavesdropper have access to common information. More precisely, each party, including the eavesdropper, has many realizations of a random variable. These $n + 1$ random variables are correlated through a known probability distribution. Since the secrecy content of these correlated data is non-increasing under LOPC, this set of transformations is considered as a free resource. That is, the honest parties are allowed to perform any local operation on their data and to communicate through a public, but authenticated, channel. Given an initial probability distribution P, we focus on two questions: (i) can P be generated by LOPC? and (ii) can perfect secret bits be extracted from P by LOPC?

A family of probability distributions is introduced, allowing the construction of several examples (see below) with a huge variety of distillation properties. In particular, for each probability distribution we can answer the previous two questions (i) and (ii). Note that we do not consider the problem of how these correlations are generated, that is, they will appear as an initially given resource. However, there have been proposed different ways of establishing partially secret correlations, such as the satellite model by Maurer [11], or Quantum Cryptography [2]. The analyzed techniques can be used to prove the existence and activation of *bound information*, a cryptographic analog of bound entanglement, first conjectured in [9] (see also [7]). We finally discuss the connection of these techniques with previous results on entanglement transformations in Quantum Information Theory.

1.1 Examples

In this section we present some examples of multipartite secret correlations showing interesting distillability properties. These probability distributions are explicitly constructed in section 4.6. In the following examples, we consider n separated parties $\{\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_n\}$. Throughout the article, whenever we say that a subset of k parties are together, or form a group, we mean that they can perform k-partite joint secret operations. This can be done by meeting at the same place, or by sharing a sufficiently large k-partite secret key.

Example 1. n honest parties can distill a secret key if at least 70% of them cooperate in the protocol, independent of the fact that they join or not (the choice of 70% is arbitrary).

Example 2. Probability distribution of n honest parties where distillation is possible if, and only if, the cooperating parties join in groups of at least k people, independently of how many parties participate in the distillation protocol.

The previous two examples can be considered as elementary conditions on distillation. In the following two examples we combine them with different logical clauses (AND and OR), in order to obtain more sophisticated distillation scenarios.

Example 3. n honest parties can obtain a secret key if, and only if, at least 70% of them cooperate in the protocol, AND, they join in groups of at least k people.

Example 4. n honest parties can generate a secure key if, and only if, at least 70% of them cooperate in the protocol, OR, the cooperating parties join in groups of at least k people, or both.

In the previous examples all the parties played the same role. In the following some specific parties have a different status, that is, the possibility of distillation may depend on their actions.

Example 5. Distribution of n honest parties where distillation is possible if, and only if, the parties $\mathcal{A}_i\mathcal{A}_j$ participate in the protocol and remain together, independently of how many others cooperate and how they distribute in groups. The same can be done but imposing that parties $\mathcal{A}_i\mathcal{A}_j$ must remain separated.

It is now clear that one can design probability distributions showing unlimited intricate distillation properties.

2 Bipartite secret correlations

In 1993, Maurer introduced the information-theoretic key-agreement model, generalizing previous ideas by Wyner [19] and Csiszár and Körner [3]. In his original formulation, two honest parties (Alice and Bob) are connected by an authenticated but otherwise insecure classical communication channel. Additionally, each party —including Eve— has access to correlated information given by repeated realizations of the random variables A, B and E (possessed by Alice, Bob and Eve respectively), jointly distributed according to $P(A, B, E)$. From now on, we denote by the same symbol, X, a random variable, X, as well as the value it can take, x, e.g. $P(X) = P_X(x)$. The goal for Alice and Bob is to obtain a common string of random bits for which Eve has virtually no information, i.e. a secret key. The maximal amount of secret key bits that can be asymptotically extracted per realization of (A, B) used, is called the secret-key rate, denoted by $S(A : B \parallel E)$ or S. More precisely, this quantity is defined as the largest real number such that for all $\epsilon > 0$, one can find an integer N_0 and a two-way communication protocol for Alice and Bob transforming $N \geq N_0$ realizations of A and B into random variables S_A and S_B satisfying

$$\begin{aligned} P[S_A = S_B = X] &> 1 - \epsilon \\ H(X) = \log(|X|) &\geq (R - \epsilon)N \\ I(X : CE^N) &< \epsilon, \end{aligned} \qquad (1)$$

where X is another random variable and C denotes the communication exchanged during the protocol. Therefore, the secret-key rate quantifies the amount of secret-key bits extractable from a probability distribution.

More recently, another measure for the secrecy content of $P(A, B, E)$, the so-called information of formation $I_{\text{form}}(A : B|E)$, has been introduced in [14]. Intuitively, it can be understood as the minimal number of secret-key bits asymptotically needed to generate each independent realization of (A, B) —distributed according to $P(A, B)$—, such that the information about (A, B) contained in the messages exchanged through the public channel, C, is at most equal to the information in E. More precisely, I_{form} is defined as the infimum over all numbers $R \geq 0$ such that for all $\epsilon > 0$ there exists an integer N, and a protocol with communication C that, with probability $1 - \epsilon$, allows Alice and Bob, knowing the same random $\lceil RN \rceil$-bit string X, to compute A^N and B^N such that

$$P(A^N, B^N, C) = \sum_{E^N} [P(A, B, E)]^N \, P(C|E^N), \qquad (2)$$

where $P(C|E^N)$ defines a channel [14]. According to this definition, we say that a probability distribution P can be established by LOPC if, and only if, $I_{\text{form}} = 0$. Note that this statement does not mean that the result of the corresponding LOPC formation protocol is necessarily P, but it is a distribution P' at least as good as P from Alice and Bob's point of view. More concretely, P' can be obtained from P by processing Eve's information, in the sense of Eq. (2).

Information of formation and secret-key rate are two measures of the secrecy content of a probability distribution with a clear operational meaning: I_{form} quantifies the amount of secret-key bits required for the formation of $P(A, B, E)$, while S specifies the amount of secret bits extractable from $P(A, B, E)$.

A useful upper bound for S is given by the so-called intrinsic information, introduced in [12]. This quantity, denoted by $I(A : B \downarrow E)$ or more briefly $I_\downarrow$, will play a significant role in the proof of our results. The intrinsic information between A and B given E is defined as:

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

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

$$I(A : B|E) = H(A, E) + H(B, E) - H(A, B, E) - H(E) \; , \qquad (4)$$

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

$$S \leq I_\downarrow \leq I_{\text{form}} \; . \qquad (5)$$

3 Multipartite secret correlations

The generalization of Maurer's formulation to the multipartite scenario is straightforward. Consider a set of n honest parties $\mathcal{Q} = \{\mathcal{A}_1, \mathcal{A}_2, \ldots \mathcal{A}_n\}$ connected by a broadcast public communication channel which is totally accessible to the eavesdropper but which is tamper-proof. Each of the parties (including Eve) has access to the correlated information contained in many realizations of its corresponding random variable. We denote by A_i the random variable corresponding to party $\mathcal{A}_i$. Eve's random variable is also denoted by E. In the whole paper curly capital letters refer to parties and sets of parties, while normal capital letters refer to random variables. In this scenario, general secret correlations are represented by probability distributions of the form $P(A_1, \ldots, A_n, E)$. That is, all random variables in each realization are correlated according to P, and each realization is independent of the others.

One possible goal for the honest parties is to obtain an n-partite secret key. Sometimes this is not possible, but still, a subset of m parties (with $1 < m < n$) can get an m-partite key. Therefore, there are many different senses in which a distribution P is (or is not) distillable. In order to get rid of such ambiguity we choose the strongest definition of non-distillability. We say that a distribution P is non-distillable if there does not exist any pair of parties, capable of obtaining a secret key by LOPC, even with the help of the others. For similar reasons, in the multipartite scenario there may be many ways of defining the secret-key rate. But, in this paper we only use the secret-key rate in bipartite situations, where the definition is unique. In general, considering bipartite splittings of the parties will prove to be a very useful tool for obtaining necessary conditions in the multipartite scenario.

3.1 Bipartite splittings

We denote by $\mathcal{P}$ any subset of $\mathcal{Q}$, and by $\overline{\mathcal{P}}$ its complement (the set of all elements in $\mathcal{Q}$ not belonging to $\mathcal{P}$). Each bipartition of $\mathcal{Q}$ can be specified by giving one of the halves, say $\mathcal{P}$.

The following two lemmas concerning any n-party distribution refer to their distillation and formation properties.

Lemma 1: *A necessary condition for obtaining an n-partite secret key is that: for all bipartitions $\mathcal{P}$ of $\mathcal{Q}$, when all parties within each half are together, a bipartite secret key between $\mathcal{P}$ and $\overline{\mathcal{P}}$ can be obtained.*

Proof: Suppose the distribution can be distilled into an n-partite secret key. The same must hold when some of the parties are together. In particular, a bipartite key between the groups $\mathcal{P}$ and $\overline{\mathcal{P}}$ can be obtained, for any $\mathcal{P}$. Therefore, the last is a necessary condition. □

Lemma 2: *A necessary condition for the correlations specified by P being generated by LOPC is that: for all bipartitions $\mathcal{P}$ of $\mathcal{Q}$, when all parties within each half are together, the resulting bipartite distribution can be generated by LOPC.*

Proof: Suppose the distribution can be generated using LOPC by the n honest parties. The same must hold when some of the parties are together, in particular, for the bipartite splitting $\mathcal{P}$ and $\overline{\mathcal{P}}$. Therefore, the last is a necessary condition. □

4 A family of multipartite probability distributions

In this section we present a family of probability distributions, denoted by P_Ω, exhibiting a variety of distillation properties. The examples described in section 1.1 are particular instances of this family.

4.1 Notation and definitions

From now on, we restrict the random variables of the honest parties $A_1, \ldots, A_n$ to take the values $0, 1$. Eve's random variable E can however have a wider range. In the remainder, unless explicitly mentioned, quantities between square brackets $[s]$ are to be understood as $(n-1)$-bit strings. That is, we associate with each integer $s \in \{0, 1, \ldots 2^{n-1} - 1\}$ the $(n-1)$-bit string corresponding to its binary expansion, and denote this by $[s]$. We denote by $[\bar{s}]$ the string where all bits have the opposite value than in $[s]$. As an instance, suppose $n - 1 = 3$, we have that $[2] = 010$ and $[\bar{2}] = 101$. We will use bit strings $[s]$ to label the outcome of the first $(n-1)$ variables $A_1, \ldots, A_{n-1}$; for example $A_1 \ldots A_{n-1} = [s]$.

In what follows, we also use bit strings $[s]$ to specify bipartitions of the set of n parties $\mathcal{Q}$. The subset $\mathcal{P}_{[s]} \subset \mathcal{Q}$ is defined in this way: $A_i \in \mathcal{P}_{[s]}$ if the i^{th} bit of $[s]$ is one. Notice that A_n always belongs to $\overline{\mathcal{P}}_{[s]}$. In this way, we associate with each $(n-1)$-bit string $[s]$ a bipartition of $\mathcal{Q}$. As an example suppose $\mathcal{Q} = \{A_1, A_2, A_3\}$, the string 01 corresponds to the bipartition $(A_2) - (A_1 A_3)$, and, 00 corresponds to the trivial bipartition $() - (A_1 A_2 A_3)$.

Let us denote by $P_\Omega(A_1, \ldots A_n, E)$ the following family of probability distributions.

$A_1 \ldots A_{n-1}$	A_n	E	P_Ω
$[0]$	0	$[0]0$ or $[\bar{0}]1$	$\Omega_{[0]}$
$[\bar{0}]$	1	$[0]0$ or $[\bar{0}]1$	$\Omega_{[0]}$
$[1]$	0	$[1]\,0$	$\Omega_{[1]}$
$[\bar{1}]$	1	$[\bar{1}]\,1$	$\Omega_{[1]}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$[s]$	0	$[s]\,0$	$\Omega_{[s]}$
$[\bar{s}]$	1	$[\bar{s}]\,1$	$\Omega_{[s]}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$[2^{n-1}-1]$	0	$[2^{n-1}-1]\,0$	$\Omega_{[2^{n-1}-1]}$
$\overline{[2^{n-1}-1]}$	1	$\overline{[2^{n-1}-1]}\,1$	$\Omega_{[2^{n-1}-1]}$

In this table, each row corresponds to a different event. For example, in the first row event, the obtained outcomes are $(A_1 \ldots A_n) = (0 \ldots 0)$ and $E =$ "$[0]0$ or $[\bar{0}]1$", and this happens with probability $\Omega_{[0]}$. As can be seen, the 2^n events are grouped in equiprobable pairs. Notice that Eve always knows the value of $A_1 \ldots A_n$, except in the first two events, where she obtains the outcome "$[0]0$ or $[\bar{0}]1$" independently of which is the actual one. The parameters of P_Ω are the positive numbers $\Omega_{[0]}, \ldots, \Omega_{[2^{n-1}-1]}$, only constrained by the normalization condition:

$$\sum_{s=0}^{2^{n-1}-1} \Omega_{[s]} = \frac{1}{2} \,. \qquad (6)$$

A simple example of P_Ω can be found in section 5.1.

4.2 Bipartitions

Let us study the bipartite properties of P_Ω. In the following lemmas, it is assumed that all parties within each half, $\mathcal{P}_{[s]}$ and $\overline{\mathcal{P}}_{[s]}$, are together.

Lemma 3: *A bipartite secret key between the parts $\mathcal{P}_{[s]}$ and $\overline{\mathcal{P}}_{[s]}$ can be obtained if, and only if, $\Omega_{[s]} < \Omega_{[0]}$.*

Proof: To prove the *if* statement we only have to provide an explicit distillation protocol. This protocol has two steps. In the first step, the honest parties discard all realizations of P_Ω in which not all the variables within each half ($\mathcal{P}_{[s]}$ and $\overline{\mathcal{P}}_{[s]}$) have the same value. This operation only filters the following events:

$$(A_1 \ldots A_{n-1}\, A_n) = [0]0,\ [\bar{0}]1,\ [s]0,\ [\bar{s}]1. \qquad (7)$$

The filtered probability distribution is, up to normalization:

$P_{[s]}$	$\overline{P}_{[s]}$	E	$P_{\Omega\vert\text{filtered}}$
0	0	$[0]0$ or $[\bar{0}]1$	$\Omega_{[0]}$
1	1	$[0]0$ or $[\bar{0}]1$	$\Omega_{[0]}$
1	0	$[s]0$	$\Omega_{[s]}$
0	1	$[\bar{s}]1$	$\Omega_{[s]}$

Where $P_{[s]} = A_i$ for all i such that $\mathcal{A}_i \in \mathcal{P}_{[s]}$, and analogously for $\overline{P}_{[s]}$ and $\overline{\mathcal{P}}_{[s]}$. Notice that this is well-defined because all parties in $\mathcal{P}_{[s]}(\overline{\mathcal{P}}_{[s]})$ have obtained the same outcome. The second step is the repeated code protocol, explained in the Appendix. There, it is shown that this protocol generates a secret key if $\Omega_{[0]} > \Omega_{[s]}$, as we wanted to prove.

The *only if* part can be proven by showing that the intrinsic information of this partition is zero, $I(\mathcal{P}_{[s]} : \overline{\mathcal{P}}_{[s]} \downarrow E) = 0$, when $\Omega_{[0]} < \Omega_{[s]}$. For doing so, we perform the following stochastic map $E \to \tilde{E}$: If E is equal to $[s]\,0$ or $[\bar{s}]\,1$, we assign $\tilde{E} :=$ "$[0]0$ or $[\bar{0}]1$" with probability $\Omega_{[0]}/\Omega_{[s]}$, and, with probability $1 - \Omega_{[0]}/\Omega_{[s]}$ we assign $\tilde{E} := E$. In the rest of the cases we also assign $\tilde{E} := E$. It is easy to check that $I(\mathcal{P}_{[s]} : \overline{\mathcal{P}}_{[s]} | \tilde{E}) = 0$, which ensures that $I(\mathcal{P}_{[s]} : \overline{\mathcal{P}}_{[s]} \downarrow E) = 0$. Now, the upper bound (5) implies that the secret-key rate must be also zero. In other words, we have that when $\Omega_{[0]} < \Omega_{[s]}$

$$S(\mathcal{P}_{[s]} : \overline{\mathcal{P}}_{[s]} \| E) = 0, \tag{8}$$

which completes the proof. □

Lemma 3 provides a tool for designing distributions with involved distillation properties. Suppose that, in order to distill a secret key, the n parties join in two groups according to the bipartition $\mathcal{P}_{[s]}$. Now, we can choose in which of these bipartitions distillation will be possible, and in which not. We set $\Omega_{[s]} = 0$, if we allow the parties to obtain a secret key when arranged according to $\mathcal{P}_{[s]}$. Notice that for non-trivial bipartitions $[s] \neq [0]$. We set $\Omega_{[s]} = \Omega_{[0]}$, if we forbid distillation when the parties are arranged according to $\mathcal{P}_{[s]}$. Finally, we set $\Omega_{[0]}$ such that the normalization condition (6) is satisfied. Notice that we have as many free parameters as there are possible bipartitions.

4.3 Multipartitions

Lemma 3 tells us how to construct probability distributions P_Ω, choosing independently which bipartite splits permit secret key extraction, and which do not. Next, we generalize Lemma 3 by considering situations in which the n parties are joined in more than two groups. Of course, this includes the case where the n parties are all separated. Let us introduce some notation first.

An m-partition of $\mathcal{Q}$ is given by m disjoint subsets $\mathcal{Q}_1, \ldots, \mathcal{Q}_m \subset \mathcal{Q}$ such that $\mathcal{Q}_1 \cup \cdots \cup \mathcal{Q}_m = \mathcal{Q}$. As before, we consider that the parties within each subset $\mathcal{Q}_i$ are together. We use Q_i to denote the binary variable associated with "party" $\mathcal{Q}_i$.

Lemma 4: *Consider an m-partition of $\mathcal{Q}$, $\{\mathcal{Q}_1, \ldots, \mathcal{Q}_m\}$. An m-partite secret key among these groups of parties can be obtained if, and only if, for each bit string $[s]$ such that its corresponding bipartition $\mathcal{P}_{[s]}$ does not split any set $\mathcal{Q}_1, \ldots, \mathcal{Q}_m$, the inequality $\Omega_{[s]} < \Omega_{[0]}$ holds.*

Proof: The *only if* assertion is just Lemma 1, but using the equivalence of Lemma 3. Let us prove the *if* part by giving a protocol which is a generalization of the one given in the proof of Lemma 3. First, the honest parties discard all realizations of P_Ω in which there is at least one subset $\mathcal{Q}_i$ containing variables with different values. Or equivalently, they reject all events $A_1 \ldots A_n = [s]0,\ [\bar{s}]1$ such that its associated bipartition $\mathcal{P}_{[s]}$ splits at least one subset $\mathcal{Q}_i$. As usual, $Q_i = A_i$ for all i such that $\mathcal{A}_i \in \mathcal{Q}_i$. After this filtering operation the probability distribution is, up to normalization:

$Q_1 \ldots Q_m$	E	$P_{\Omega\vert\text{filtered}}$
$[0]0$	$[0]0$ or $[\bar{0}]1$	$\Omega_{[0]}$
$[\bar{0}]1$	$[0]0$ or $[\bar{0}]1$	$\Omega_{[0]}$
$\vdots$	$\vdots$	$\vdots$
$[s]0$	$[s]\,0$	$\Omega_{[s]}$
$[\bar{s}]1$	$[\bar{s}]\,1$	$\Omega_{[\bar{s}]}$
$\vdots$	$\vdots$	$\vdots$

Notice that in the first column, we specify the value of the m-bit string $Q_1 \ldots Q_m$ with an n-bit string, say $[s]0$. This is well defined if we recall that, in all filtered events, the bits in $[s]0$ associated with the parties belonging to $\mathcal{Q}_i$, have the same value, and this value is the one assigned to the variable $\mathcal{Q}_i$. Now, the m parties perform the repeated code protocol to $P_{\Omega|\text{filtered}}$. In the Appendix it is shown that this protocol works if the condition of Lemma 4 holds. □

4.4 Non-cooperating parties

It is clear that a single party, say $\mathcal{A}_i$, can always prevent the others from obtaining a secret key. To do so, she only has to make public the value of A_i in each realization of P_Ω. After this procedure, Eve will know the value of each variable in the two events where all variables are equal: $(A_1 \ldots A_n) = (0 \ldots 0), (1 \ldots 1)$. In the rest of events, Eve already knew the value of each variable. Therefore, by a non-cooperating party we do not mean a party who is against the others, but one that does not want to be involved in the distillation protocol. In this section, we generalize Lemma 4 by considering the presence of non-cooperating parties. Let us first, introduce some notation.

In what follows, when referring to the m disjoint subsets $\mathcal{Q}_1, \ldots, \mathcal{Q}_m \subset \mathcal{Q}$, we do not demand that they satisfy $\mathcal{Q}_1 \cup \cdots \cup \mathcal{Q}_m = \mathcal{Q}$. In other words, they don't have to be an m-partition of $\mathcal{Q}$. It is understood, that the parties not belonging to $\mathcal{Q}_1 \cup \cdots \cup \mathcal{Q}_m$ do not participate in the protocol. Within all this section, primed quantities between square brackets $[z']$ have to be understood as $(m-1)$-bit strings. That is, we associate with each integer $z \in \{0, 1, \ldots, 2^{m-1}-1\}$ the $(m-1)$-bit string corresponding to its binary expansion, denoted by $[z']$. As in the rest of the paper, unprimed integers between square brackets mean $(n-1)$-bit strings. We also denote by $[\bar{z}']$ the $(m-1)$-bit string where each bit has the opposite value than in $[z']$. Following the analogy, $\mathcal{P}_{[z']}$ is a subset of $\{\mathcal{Q}_1, \ldots, \mathcal{Q}_m\}$ defined with the same convention as $\mathcal{P}_{[s]}$. That is, $\mathcal{Q}_i$ belongs to $\mathcal{P}_{[z']}$ if the i^{th} bit of $[z']$ has the value one. We define $\bar{\mathcal{P}}_{[z']}$ analogously, which always contains $\mathcal{Q}_m$. We also use $\mathcal{P}_{[z']}$ to denote bipartitions of $\{Q_1, \ldots, \mathcal{Q}_m\}$. Additionally, we associate with each bipartition of $\{Q_1, \ldots, \mathcal{Q}_m\}$ some bipartitions of $\mathcal{Q}$, in the following way. We say that $\mathcal{P}_{[s]}$ is associated with $\mathcal{P}_{[z']}$ if $\mathcal{P}_{[s]}$ contains all parties belonging to the subsets $\mathcal{Q}_i$ such that $\mathcal{Q}_i \in \mathcal{P}_{[z']}$, and, does not contain any party belonging to the subsets $\mathcal{Q}_i$ such that $\mathcal{Q}_i \in \bar{\mathcal{P}}_{[z']}$. Notice that the non-cooperating parties, the ones not belonging to $\mathcal{Q}_1 \cup \cdots \cup \mathcal{Q}_m$, may or may not belong to $\mathcal{P}_{[s]}$. Therefore, there can be many $\mathcal{P}_{[s]}$ associated with one $\mathcal{P}_{[z']}$. We also extend this relation to bit strings in a natural way: we say $[s] \sim [z']$ if $\mathcal{P}_{[s]}$ is associated with $\mathcal{P}_{[z']}$.

Theorem 5: *An m-partite secret key among the groups of parties $\mathcal{Q}_1, \ldots, \mathcal{Q}_m$ can be obtained if, and only if, for each bipartition of these m groups $\mathcal{P}_{[z']}$, the inequality*

$$\sum_{\forall [s] \sim [z']} \Omega_{[s]} < \Omega_{[0]} \tag{9}$$

holds.

Proof: As in the previous cases, we prove the *if* assertion by giving a protocol that works under the stated conditions. The usual protocol is readily generalized to fit this case: The cooperating honest parties discard all realizations of P_Ω for which there is at least one group $\mathcal{Q}_i$, in which not all the variables are equal. Or equivalently, they reject all events $A_1 \ldots A_n = [s]0$, $[\bar{s}]1$ such that, its corresponding bipartition $\mathcal{P}_{[s]}$ splits at least one subset $\mathcal{Q}_i$. Notice that in the filtered events, the non-cooperating parties' variables can have any value. After this filtering, the probability distribution is, up to normalization:

$Q_1 \ldots Q_{m-1}$	Q_m	E	$P_{\Omega\vert\text{filtered}}$
$[0']$	0	$[0']0$ or $[\bar{0}']1$	$\Omega_{[0]}$
$[\bar{0}']$	1	$[0']0$ or $[\bar{0}']1$	$\Omega_{[0]}$
$[1']$	0	$[1']\,0$	$\sum_{\forall [s] \sim [1']} \Omega_{[s]}$
$[\bar{1}']$	1	$[\bar{1}']\,1$	$\sum_{\forall [s] \sim [1']} \Omega_{[s]}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$[z']$	0	$[z']\,0$	$\sum_{\forall [s] \sim [z']} \Omega_{[s]}$
$[\bar{z}']$	1	$[\bar{z}']\,1$	$\sum_{\forall [s] \sim [z']} \Omega_{[s]}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$

As usual, $Q_i = A_i$ for all i such that $\mathcal{A}_i \in \mathcal{Q}_i$. As shown in the Appendix, the repeated code protocol works with $P_{\Omega|\text{filtered}}$ if, for all $[z']$, condition (9) holds. To prove the *only if* part, let us suppose that there exists at least one string $[z'_0]$ such that (9) is not satisfied. According to Lemma 1, when the groups $\mathcal{Q}_1, \ldots, \mathcal{Q}_m$ can distill an m-partite secret key, a bipartite key is also obtainable when the m groups are joined in just two groups. This must hold for any bipartition of $\{\mathcal{Q}_1, \dots \mathcal{Q}_m\}$, say $[z_0']$. Let us see that this is impossible when

$$\sum_{\forall [s] \sim [z_0']} \Omega_{[s]} \geq \Omega_{[0]} \qquad (10)$$

holds. As in the proof of Lemma 3, we show that the secret-key rate between $\mathcal{P}_{[z_0']}$ and $\bar{\mathcal{P}}_{[z_0']}$ is zero, by computing the intrinsic information between these two parts. To do so, we perform a similar stochastic map $E \to \tilde{E}$: If $E = [z']0$ or $E = [\bar{z}']1$ we assign $\tilde{E} =$"[0]0 or $[\bar{0}]$1" with probability $\Omega_{[0]} / \sum_{\forall [s] \sim [z']} \Omega_{[s]}$. In the rest of the cases $\tilde{E} = E$. It is easy to check that

$$I(P_{[z']} : \overline{P}_{[z']} | \tilde{E}) = 0 \ , \qquad (11)$$

which implies the above mentioned impossibility. □

4.5 Correlations without secrecy

In this section, we will characterize those P_Ω that can be established by LOPC. This is the content of the following theorem.

Theorem 6: *A probability distribution P_Ω can be generated by LOPC if, and only if, for all bipartite splittings $\mathcal{P}_{[s]}$,*

$$\Omega_{[s]} \geq \Omega_{[0]} \qquad (12)$$

holds.

Proof: Let us start by the *only if* part. In the proof of Lemma 3 we have seen that whenever $\Omega_{[s]} \geq \Omega_{[0]}$, the intrinsic information for the corresponding bipartite splitting is zero, $I(\mathcal{P}_{[s]} : \overline{\mathcal{P}}_{[s]} \downarrow E) = 0$. It has been proven in [14] that $I_\downarrow = 0$ if, and only if, $I_{\text{form}} = 0$. This result and Lemma 2 imply that (12) is a necessary condition for P_Ω being generated by LOPC.

For the *if* part of the proof, we proceed as follows. First, we introduce a probability distribution P'_Ω and prove it cannot be less secret than P_Ω. This is done by showing that P'_Ω can be obtained from P_Ω by degradating Eve's information; namely, there exists a map for Eve's random variable $E \to \tilde{E}$ such that $P_\Omega \to P'_\Omega$. Next, we give an explicit LOPC protocol producing the probability distribution P'_Ω without any additional resource. Thus, I_{form} is zero for P'_Ω. Then, it follows from the definition of information of formation that P_Ω has also $I_{\text{form}} = 0$.

With each P_Ω such that (12) holds for all $[s]$, we associate the following distribution P'_Ω

$A_1 \dots A_{n-1}$	A_n	$\tilde{E}$	P'_Ω
$[0]$	0	x	$\Omega_{[0]}$
$[\bar{0}]$	1	x	$\Omega_{[0]}$
$[1]$	0	x	$\Omega_{[0]}$
$[\bar{1}]$	1	x	$\Omega_{[0]}$
$[1]$	0	$[1]\,0$	$\Omega_{[1]} - \Omega_{[0]}$
$[\bar{1}]$	1	$[\bar{1}]\,1$	$\Omega_{[1]} - \Omega_{[0]}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$[s]$	0	x	$\Omega_{[0]}$
$[\bar{s}]$	1	x	$\Omega_{[0]}$
$[s]$	0	$[s]\,0$	$\Omega_{[s]} - \Omega_{[0]}$
$[\bar{s}]$	1	$[\bar{s}]\,1$	$\Omega_{[s]} - \Omega_{[0]}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$[2^{n-1}-1]$	0	x	$\Omega_{[0]}$
$\overline{[2^{n-1}-1]}$	1	x	$\Omega_{[0]}$
$[2^{n-1}-1]$	0	$[2^{n-1}-1]\,0$	$\Omega_{[2^{n-1}-1]} - \Omega_{[0]}$
$\overline{[2^{n-1}-1]}$	1	$\overline{[2^{n-1}-1]}\,1$	$\Omega_{[2^{n-1}-1]} - \Omega_{[0]}$

Actually, P'_Ω can be obtained from P_Ω after the following stochastic map on Eve's random variable, $E \to \tilde{E}$. If E is equal to "[0]0 or $[\bar{0}]$1" we assign $\tilde{E} :=$"x". If E is equal to $[s]\,0$ ($[\bar{s}]\,1$), we assign $\tilde{E} :=$ "x" with probability $\Omega_{[0]}/\Omega_{[s]}$, and, with probability $1 - \Omega_{[0]}/\Omega_{[s]}$ we assign $\tilde{E} := E$. Now, we prove that all probability distributions P'_Ω of that kind can be created with the following LOPC protocol. With probability $2^n\,\Omega_{[0]}$ party $\mathcal{A}_1$ broadcasts the public message "x" . After receiving "x", each party $\mathcal{A}_1 \dots \mathcal{A}_n$ locally generates a random bit $A_1 \dots A_n$. With probability $\Omega_{[s]} - \Omega_{[0]}$, party $\mathcal{A}_1$ broadcasts the public message $[s]0$ ($[\bar{s}]1$). After receiving this message each party outputs its corresponding bit from the sequence $[s]0$ ($[\bar{s}]1$). This implies $I_{\text{form}} = 0$ for P'_Ω, and the same result applies to P_Ω. □

4.6 Construction of the examples

In this section we explicitly construct the examples that have been introduced at the beginning of the paper. This is done by repeatedly using Theorem 5.

Example 1. Let us design a probability distribution of n honest parties which is distillable if, and only if, more than m parties cooperate in the protocol. In other words, if $n-m$ parties (or more) do not cooperate, distillation is impossible. Consider the situation where there are m cooperating parties. For each bipartition of them, $\mathcal{P}_{[z']}$, there are 2^{n-m} different ways of distributing the $n-m$ non-cooperating parties between the two groups. That is, there are 2^{n-m} different bipartitions $\mathcal{P}_{[s]}$ associated with $\mathcal{P}_{[z']}$. If we set $\Omega_{[s]} = \Omega_{[0]}/2^{n-m}$ for all $[s] \neq [0]$, equation (9) will be satisfied if, and only if, the sum $\sum_{\forall [s]\sim[z']} \Omega_{[s]}$ has less than 2^{n-m} terms, and this only happens if the number of cooperating parties is larger than m. Notice that $\Omega_{[0]}$ is fixed by the normalization condition (6). Because all $\Omega_{[s]}$ with $[s] \neq [0]$ have the same value, distillation is possible even when the cooperating parties are all separated.

Example 2. Let us construct an n-party distribution, which is distillable if, and only if, the cooperating parties join in groups of at least k people, independently of how many parties do not cooperate. We denote by $W_{[s]}$ the number of ones that the bit string $[s]$ has. We impose $\Omega_{[s]} = 0$ for all strings with $k \leq W_{[s]} \leq n-k$, and $\Omega_{[s]} = \Omega_{[0]}$ for the rest. As before, $\Omega_{[0]}$ is fixed by the normalization condition (6). It is easy to see that, if there is a group of less than k parties, the bipartition having these k parties in one side and the rest in the other side, satisfies $\Omega_{[s]} = \Omega_{[0]}$, and this prevents condition (9) from being satisfied. When all cooperating groups contain at least k people, all bipartitions that do not split any of the groups satisfy $\Omega_{[s]} = 0$, in this case, condition (9) holds independently of how many parties do not cooperate.

Example 3. This n-party distribution is distillable if, and only if,, more than m parties participate in the protocol, AND, they join in groups of at least k people. This is achieved with the following assignments. We set $\Omega_{[s]} = \Omega_{[0]}/2^{n-m}$ if $k \leq W_{[s]} \leq n-k$, and $\Omega_{[s]} = \Omega_{[0]}$ otherwise. As in the example 2, if there is one group of less than k cooperating parties condition (9) does not hold. Reasoning in the same fashion as in example 1, if there are m or less cooperating parties distillation is impossible.

Example 4. This n-party distribution is distillable if, and only if,, there are more than m cooperating parties, OR, they joint in groups of at least k people, or both. We set $\Omega_{[s]} = 0$ if $k \leq W_{[s]} \leq n-k$, and $\Omega_{[s]} = \Omega_{[0]}/2^{n-m}$ for the rest.

Example 5. This n-party distribution is distillable if, and only if, parties A_iA_j cooperate and remain always together. We suppose without loss of generality that $i, j \neq n$. If the i^{th} and j^{th} bits of the string $[s]$ have the same value we set $\Omega_{[s]} = 0$, and $\Omega_{[s]} = \Omega_{[0]}$ otherwise. It is clear that this fulfils our demand. A variation of this example is when distillation is possible if, and only if, parties A_iA_j remain separated. The construction of this case is closely analogous to the previous one. Now, we set $\Omega_{[s]} = 0$ if $[s]$ has different values for the i^{th} and j^{th} bits, and $\Omega_{[s]} = \Omega_{[0]}$ otherwise.

5 Bound information

Bound information represents the cryptographic analog of bound entanglement, an intriguing feature of some quantum states found by the Horodeckis in 1998 [10]. In the bipartite case, bound information can easily be defined using the previously introduced quantities [9]: a probability distribution $P(A,B,E)$ contains bound information when the following two conditions hold:

$$\begin{aligned} S &= 0 \\ I_{\text{form}} &> 0\ . \end{aligned} \qquad (13)$$

Therefore, $P(A,B,E)$ has bound information when (i) no secret-key bits can be extracted from it by LOPC, but (ii) its formation by LOPC is impossible. In other words, the non-zero secrecy content of the probability is bound because secret correlations are necessary for its preparation but cannot be distilled into a pure form. There exist several results supporting the existence of this analog of bound entanglement in the bipartite case: in Refs. [7, 9] several probability distributions were constructed for which one can prove that $I_{\downarrow}$ is strictly positive but none of the known secret-key distillation protocols allow to extract secret bits. Moreover, it was shown in [14] that there exist probability distribution where $S < I_{\text{form}}$. This already proves the irreversibility, in terms of secret bits, in the processes of formation and key distillation for some probability distributions. Actually, the authors of [14] constructed a family of probability distributions where $I_{\text{form}} > 1/2$ while S can be arbitrarily small. Unfortunately, no example of $P(A, B, E)$ such that $0 = S < I_{\text{form}}$ is known until now.

Bound information was initially defined in the case of two honest parties. However, its generalization to the multipartite scenario is again straightforward: a probability distribution $P(A_1, \ldots, A_n, E)$ has bound information when (i) its formation by LOPC is impossible and (ii) no secret-key bits can be extracted between any pair of parties by LOPC. In what follows, we use the techniques described above in order to show the existence of multipartite bound information. We will do that for the case of three honest parties. Moreover, we will see that similarly to what happens in the quantum case, bound information can be activated: the combination of different probability distributions with bound information may give a distillable probability distribution.

5.1 Proof of the existence of bound information

In this section we prove the existence of bound information in the tripartite scenario. In order to do that we give a probability distribution $P(A_1, A_2, A_3, E)$ and show that its formation by LOPC is impossible but no secret-key bits can be extracted from it by the honest parties using LOPC. Although these results already appear in [1], here we review them using the formalism described in the previous section.

Using the introduced notation, an example of tripartite probability distribution having bound information reads as follows:

A_1A_2	A_3	E	P_1
$[0]$	0	$[0]0$ or $[\bar{0}]1$	1/6
$[\bar{0}]$	1	$[0]0$ or $[\bar{0}]1$	1/6
$[1]$	0	$[1]0$	1/6
$[\bar{1}]$	1	$[\bar{1}]1$	1/6
$[2]$	0	$[2]0$	0
$[\bar{2}]$	1	$[\bar{2}]1$	0
$[3]$	0	$[3]0$	1/6
$[\bar{3}]$	1	$[\bar{3}]1$	1/6

Note that the role played by A_2 and A_3 in P_1 is the same, up to a relabelling of Eve's variables.

Using Lemmas 1 and 3, it is relatively simple to see that no pair of parties can distill secret bits from this probability distribution. Consider, for instance, the partition $A_2 - (A_1A_3)$, corresponding to $[s] = [1] = 01$. Because of Lemma 3, no distillation is possible since $\Omega_{[1]} = \Omega_{[0]} = 1/6$. Then, Lemma 1 implies that A_2 can distill secret bits neither with A_1 nor with A_3. Because of the symmetry of the distribution, the same result holds for $(A_1A_2) - A_3$. Therefore no pair of parties can distill a secret key. Finally, consider the third partition $A_1 - (A_2A_3)$. In this case, where $[s] = [2] = 10$, we have $\Omega_{[2]} = 0 < \Omega_{[0]} = 1/6$. That is, the probability distribution corresponding to this partition is distillable, which means that it could not have been created by LOPC. Using Lemma 2, this implies that the initial probability distribution P_1 cannot be created by LOPC either. This proves that the non-zero secrecy content of P_1 is bound, i.e. it constitutes an example of bound information.

The proof presented here is almost the same as in [1], having been adapted to the notation introduced above. Actually, the non-distillability of P_1 could alternatively have been proven using Lemma 4. Note also that many of the probability distributions given above, such as Example 2, already constituted examples of bound information.

5.2 Bound information can be activated

The activation of bound entanglement is perhaps one of the most surprising results found in entanglement theory [5, 17]. Bound entanglement is said to be activated whenever one can distill pure-state entanglement from the combination of several bound entangled states. Remarkably, in some cases this activation can be achieved by mixing different bound entangled states [6]! As it will be shown shortly, a similar feature is observed for classical probability distributions.

Consider the situation where three honest parties and an eavesdropper have access to correlated random variables described by P_1. In addition, they also have access to other random variables described by P_2 and P_3, where these two probability distributions correspond to cyclic permutations, $A_1 \to A_2 \to A_3 \to A_1$, of P_1. Of course, P_1, P_2 and P_3 have bound information. Now, the three honest parties forget what the actual distribution is. Alternatively, one can think that a source is sending to the parties random variables correlated through P_1, P_2 and P_3 with equal probability, and the information about the prepared probability distribution is only accessible to Eve. The resulting distribution, P_{res}, can be described as

A_1A_2	A_3	E	P_{res}
$[0]$	0	$[0]0$ or $[\bar{0}]1$	1/6
$[\bar{0}]$	1	$[0]0$ or $[\bar{0}]1$	1/6
$[1]$	0	$[1]0$	1/9
$[\bar{1}]$	1	$[\bar{1}]1$	1/9
$[2]$	0	$[2]0$	1/9
$[\bar{2}]$	1	$[\bar{2}]1$	1/9
$[3]$	0	$[3]0$	1/9
$[\bar{3}]$	1	$[\bar{3}]1$	1/9

It is now straightforward to see that this probability distribution is distillable, even in the fully multipartite scenario where the three parties remain separated. This follows from Lemma 4, since for all the partitions one has $1/9 < 1/6$. Therefore, the combination of non-distillable probability distributions produces a distillable distribution.

6 Conclusions

In this work, we have presented a family of probability distributions in the multipartite scenario of n honest parties and an eavesdropper. Using this family, we were able to construct different examples of probability distribution with a huge variety of secrecy properties. This rich variety of examples shows how intricate the structure of multipartite secret correlations is. Moreover, the introduced techniques allowed us to prove the existence and activation of bound information, namely non-distillable secret correlations.

We would like to mention here some analogies between our results and the problem of entanglement manipulations in Quantum Information Theory (see Refs. [9, 4]). The intuition for the construction of the previous family of probability distributions came from the quantum states discussed in Refs. [5, 6]. Indeed, these distributions represent the cryptographic classical analog of these states. Moreover, the existence of bound information, that was our initial motivation for this study, was conjectured in 2000 [9] as a classical counterpart of bound entanglement. In this sense, all these results constitute one of the first examples where well-established ideas in Quantum Information Theory have successfully been translated to the classical side. Up to now, the flow of results has mainly been in the opposite direction.

Unfortunately, the existence of bipartite bound information, that is, probability distributions with non-distillable secret correlations, remains as an open question. Indeed, the existence of multipartite bound information exploited the possibility of considering splittings of the parties into different groups, something impossible in the bipartite scenario. In this sense, it is an interesting issue to study how those quantum concepts that allowed to prove the existence of bound entanglement for quantum states, such as partial transposition [13], can be adapted to the key-agreement scenario.

Appendix: Repeated code protocol

In this appendix, the repeated code protocol is described. Consider m separated parties $\mathcal{A}_1, \ldots, \mathcal{A}_m$ willing to generate an m-partite secret key. Each of these parties, say $\mathcal{A}_i$, has access to many realizations of its corresponding random variable A_i. Additionally, there is an eavesdropping party, Eve, who has access to a random variable E correlated to A_i through the probability distribution $P(A_1, \dots, A_m, E)$. Note that it is assumed that each realization of $A_1, A_2, \dots, A_m, E$, is independent of the other. Moreover, this probability distribution is known by all the parties.

The first part of this key distillation protocol is implemented by the following three steps:

1. Each party takes N realizations of her own random variable:
$$\begin{aligned} A_1^N &= \left(A_1^{(1)}, A_1^{(2)}, \dots, A_1^{(N)}\right) \\ &\vdots \\ A_m^N &= \left(A_m^{(1)}, A_m^{(2)}, \dots, A_m^{(N)}\right) \end{aligned}$$
2. One of the honest parties —say $\mathcal{A}_1$— generates locally a random bit k_1, computes the N numbers $X_r := (k_1 + A_1^{(r)} \bmod 2)$ for $r = 1, \dots, N$, and broadcasts through the public channel the N-bit string:
$$(X_1, X_2, \dots, X_N) \ . \tag{14}$$
3. All the remaining parties —in this case $\mathcal{A}_2, \dots, \mathcal{A}_n$— perform the following operation. Party A_i adds bitwise the broadcasted string (14) to his symbols $(A_i^{(1)}, A_i^{(2)}, \dots, A_i^{(N)})$. If he obtains the same result for all of them, that is $(X_r + A_i^{(r)} \bmod 2) = k_i$ for $r = 1, \dots, N$, he accepts k_i and communicates the acceptance to the other parties. If not, all parties reject the N realizations of P_Ω.

The final step to attain a secret key uses as input many realizations of $(k_1, \dots, k_m)$. It consists of the one-way distillation protocol given by Csiszár and Körner in [3]. The fact that this protocol is designed for two parties is not a problem. In our case, one of the honest parties, say $\mathcal{A}_1$, broadcasts all public messages to the rest, who perform error correction and privacy amplification to their data.

Let us analyze under which conditions a probability distribution belonging to the family P_Ω can be distilled into a secret key using this protocol. In the usual notation, a probability distribution P_Ω reads

$A_1 \dots, A_{m-1}$	A_m	E	P_Ω
$[0]$	0	$[0]0$ or $[\bar{0}]1$	$\Omega_{[0]}$
$[\bar{0}]$	1	$[0]0$ or $[\bar{0}]1$	$\Omega_{[0]}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$[s]$	0	$[s]\,0$	$\Omega_{[s]}$
$[\bar{s}]$	1	$[\bar{s}]\,1$	$\Omega_{[s]}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$

Notice that when party $\mathcal{A}_i$, with $i \geq 2$, accepts k_i in step 3, the variables $A_i^{(1)}, \dots, A_i^{(N)}$ are all equal, or, all different to $A_1^{(1)}, \dots, A_1^{(N)}$. This is equivalent to saying that, the N realizations of P_Ω used in this first part of the protocol, have to be all in the same pair of events, characterized by a given s_0, that is, $A_1^{(r)}, \dots, A_m^{(r)} = [s_0]0$ or $A_1^{(r)}, \dots, A_m^{(r)} = [\bar{s}_0]1$ for $r = 1, \dots, N$. This happens with probability
$$p\left(s_0\right) = \frac{\Omega_{[s_0]}^N}{\sum_{[s]} \Omega_{[s]}^N} \ . \tag{15}$$
Notice that in the case $[s_0] = [0]$, the bits $k_1, \dots, k_m$ are all equal, and Eve has no knowledge about them. If $\Omega_{[0]} > \Omega_{[s]}$ for all $[s] \neq [0]$, the probability $p(0)$ tends to one when making N large. Thus, choosing a large enough N, the honest parties can obtain a probability distribution that can be distilled to secret key with non-zero rate by means of the one-way reconciliation techniques of [3].

Result: *An m-partite distribution of the family $\mathcal{P}_\Omega$ can be distilled if $\Omega_{[0]} > \Omega_{[s]}$ for all $[s] \neq [0]$.*

Acknowledgment

The authors would like to thank Ignacio Cirac, Nicolas Gisin, Nick Jones, Renato Renner and Stefan Wolf for discussion. This work has been supported by the the U.K. Engineering and Physical Sciences Research Council (IRC QIP), the Spanish Ministerio de Ciencia y Tecnología, under the "Ramón y Cajal" grant, and the Generalitat de Catalunya.

References

[1] A. Acín, J. I. Cirac and L. Masanes, "Multipartite Bound Information Exists and Can Be Activated", *Phys. Rev. Lett.*, vol. 92, pp. 107903, 2004.

[2] C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing", *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175-179.

[3] I. Csiszár and J. Körner, "Broadcast channels with confidential messages", *IEEE Trans. Inf. Theory*, vol. IT-24, pp. 339-348, 1978.

[4] D. Collins and S. Popescu, "Classical analog of entanglement", *Phys. Rev. A*, vol. 65, pp. 032321, 2002.

[5] W. Dür and J. I. Cirac, "Activating bound entanglement in multiparticle systems", *Phys. Rev. A*, vol. 62, pp. 022302, 2000.

[6] W. Dür and J. I. Cirac, "Multiparticle entanglement and its experimental detection", *J. Phys. A: Math. and Gen.*, vol. 34, No. 35, pp. 6837-6850, 2001.

[7] N. Gisin, R. Renner and S. Wolf, "Linking classical and quantum key agreement: is there a classical analog to bound entanglement?", *Algorithmica*, vol. 34, pp. 389-412, 2002.

[8] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, "Quantum Cryptography", *Rev. Mod. Phys.*, vol. 74, pp. 145-195, 2002.

[9] N. Gisin and S. Wolf, "Linking classical and quantum key agreement: is there bound information?", in *Proceedings of CRYPTO 2000*, Lecture Notes in Computer Science, vol. 1880, pp. 482-500, 2000.

[10] M. Horodecki, P. Horodecki and R. Horodecki, " Mixed-State Entanglement and Distillation: Is there a "Bound" Entanglement in Nature?", *Phys. Rev. Lett.*, vol. 80, pp. 5239-5242, 1998.

[11] U. M. Maurer, "Secret key agreement by public discussion from common information", *IEEE Trans. Inf. Theory* vol. 39, pp. 732-743, 1993.

[12] U. M. Maurer and S. Wolf, "Unconditional Secure Key Agreement and the Intrinsic Information", *IEEE Trans. Inf. Theory*, vol. 45, pp. 499-514, 1999.

[13] A. Peres, "Separability Criterion for Density Matrices", *Phys. Rev. Lett.*, vol. 77, pp. 1413-1415, 1996.

[14] R. Renner and S. Wolf, "New Bounds in Secret-Key Agreement: The Gap Between Formation and Secrecy Extraction", *Adv. Crypt. - EUROCRYPT 2003, Lect. Not. Comp. Sci., Springer-Verlag*, vol. 2656, pp. 562-577, 2003.

[15] C. E. Shannon, "Communication theory of secrecy systems", *Bell Syst. Tech. J.*, vol. 28, pp. 656-715, 1949.

[16] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring", in *Proc. of the 35th Symposium on Foundations of Computer Science*, (Shafi Goldwasser, ed.), IEEE Computer Society Press, Los Alamitos, California, 1994, pp. 124-134.

[17] P. W. Shor, J. A. Smolin and A. V. Thapliyal, "Superactivation of Bound Entanglement", *Phys. Rev. Lett.*, vol. 90, pp. 107901, 2003.

[18] G. S. Vernam, "Cipher printing telegraph systems for secret wire and radio telegraph communications", *J. Am. Inst. Elect Eng.*, vol. 55, pp. 109-115, 1926.

[19] A. D. Wyner, "The wire-tap channel", *Bell Syst. Tech. J.*, vol. 54, No. 8, pp. 1355-1387, 1975.