New Bounds in Secret-Key Agreement: The Gap Between Formation and Secrecy Extraction

Renato Renner[1] Stefan Wolf[2]

[1] Department of Computer Science, ETH Zurich, Switzerland.
renner@inf.ethz.ch
[2] DIRO, Université de Montréal, Canada.
wolf@iro.umontreal.ca

Abstract. Perfectly secret message transmission can be realized with only partially secret and weakly correlated information shared by the parties as soon as this information allows for the extraction of information-theoretically secret bits. The best known upper bound on the rate S at which such key bits can be generated has been the *intrinsic information* of the distribution modeling the parties', including the adversary's, knowledge. Based on a new property of the secret-key rate S, we introduce a conditional mutual information measure which is a stronger upper bound on S. Having thus seen that the intrinsic information of a distribution P is not always suitable for determining the number of secret bits *extractable from* P, we prove a different significance of it in the same context: It is a lower bound on the number of key bits required to *generate* P by public communication. Taken together, these two results imply that sometimes, (a possibly arbitrarily large fraction of) the correlation contained in distributed information cannot be extracted in the form of secret keys by any protocol.

Keywords. Information-theoretic security, secret-key agreement, reductions among primitives, information measures, quantum entanglement purification.

1 Information-Theoretic Secret-Key Agreement from Distributed Information

1.1 From Partially Secret Weak Correlations to Perfect Secrecy

The unarguably strongest type of security in cryptography is based on *information theory* (rather than *computational complexity theory*) and withstands attacks even by an adversary whose capacities (of both computation and memory) are unlimited. According to a famous theorem by Shannon [11], such a high level of security can be achieved only by parties sharing an unconditionally secret key initially; a result by Maurer [6] states that such a key can, even interactively, not be generated from scratch, i.e., without any prior *correlation between* *the legitimate partners Alice and Bob that is not completely under control of or accessible to the adversary (or environment) Eve*. The meaning of the previous sentence might not be entirely clear; in fact, determining its exact interpretation is one of this paper's main concerns.

In [6] and [9], the pessimistic statement that *information-theoretic security is possible only when given information-theoretic security to start with* was relativized by showing that the required prior correlation and privacy can both be arbitrarily weak, still allowing for the generation of an unconditionally secret key (and hence unbreakably secure message transmission [13]). This was shown both in a very general but purely classical scenario, where Alice and Bob share classical information, as well as in a setting where they start with shared quantum states and try to generate a "quantum key" (the privacy of which is guaranteed by the laws of physics).

1.2 State of the Art: Facts and Conjectures

In the classical scenario, the starting point is a probability distribution P_{XYZ}, where X, Y, and Z represent Alice's, Bob's, and Eve's pieces of information, respectively. The *intrinsic information* between X and Y given Z (the mutual information shared by Alice and Bob as seen from Eve's best choice of all possible points of view), has been shown to be an upper bound to the *secret-key rate* (a quantification of Alice and Bob's ability of generating a secret key by starting from independent repetitions of the random experiment characterized by P_{XYZ}). No better bound on this rate has been found so far, and it has even been conjectured that the two quantities might always be equal [8].

The parallels between the classical and quantum scenarios of information-theoretic secret-key agreement pointed out in [3], [2], however, suggest that a well-known phenomenon on the quantum side, called *bound entanglement* [4], [5], has a classical counterpart. Bound entanglement is a kind of correlation between Alice and Bob inaccessible to Eve but nevertheless of no use for generating a secret (quantum) key. Unfortunately, the existence of such bound information, which would contradict the mentioned conjecture on the classical side of the picture, could not be proven so far. We make a significant step towards such a proof in the present paper by showing that the gap between the intrinsic information and the secret-key rate can in fact be arbitrarily large.

1.3 Contributions and Outline of this Paper

The contributions of this paper are the following. Based on a new property of the secret-key rate (Section 3.1), a new conditional information measure, the *reduced* intrinsic information, is proposed and shown to be a stronger upper bound on the secret-key rate (Sections 3.2 and 3.3). The analysis of a particular class of distributions shows that this new quantity, and hence also the secret-key rate, can be smaller than the intrinsic information by an arbitrarily large factor; this is used to prove the existence of the phenomenon of bound information asymptotically (Section 3.4).

Because of this gap between intrinsic information and the secret-key rate, one might think that intrinsic information was simply not the right measure to be used in this context. This is certainly true in a way, but untrue in another: We show (in Section 4) that the same intrinsic-information measure is a lower bound on what we will call "information of formation," namely the amount of secret-key bits required to generate a certain distribution by public communication (which is the inversion of the process of extracting key bits from the distribution). In Section 4.3, we sketch how to generalize this to a "calculus of secret correlations."

In the light of Section 4, the results of Section 3 imply that there exist distributions requiring asymptotically more secret-key bits to be *generated* than can be *extracted* from them. The somewhat counter-intuitive existence of such a gap has its counterpart on the quantum side: Two important measures for quantum entanglement [10], namely *entanglement of formation* on one side and *distillability* on the other, can differ by an arbitrary factor (where the former is always at least as big as the latter).

2 Measuring the Extractable Secret Correlation of a Distribution

2.1 The Secret-Key Rate

The model of *information-theoretic key-agreement by common (classical) information* has been introduced by Maurer [6] as an interactive generalization of earlier settings by Wyner [14] and Csiszár and Körner [1]. Alice, Bob, and Eve are assumed to have access to many independent outcomes of X, Y, and Z, respectively, where the random experiment is characterized by a discrete probability distribution P_{XYZ}. The amount of extractable secret correlation of such a distribution was quantified by the maximal length of a highly secret key that can be generated by Alice and Bob using public but authenticated two-way communication.

Definition 1. [6], [7] Let P_{XYZ} be the joint distribution of three discrete random variables X, Y, and Z. The *secret-key rate* $S(X;Y||Z)$ is the largest real number R such that for all $\varepsilon > 0$ there exists $N_0 \in \mathbf{N}$ such that for all $N \geq N_0$ there exists a protocol between Alice (knowing N realizations $X^N := (X_1, \ldots, X_N)$ of X) and Bob (knowing Y^N) satisfying the following conditions: Alice and Bob compute, at the end of the protocol, random variables S_A and S_B, respectively, with range $\mathcal{S}$ such that there exists a random variable S with the same range and[3]

$$H(S) = \log|\mathcal{S}| \geq RN \ , \tag{1}$$

$$\text{Prob}\,[S_A = S_B = S] > 1 - \varepsilon \ , \tag{2}$$

$$I(S; CZ^N) < \varepsilon \ . \tag{3}$$

[3] H and I stand for the usual Shannon entropy and mutual information measures, respectively. All logarithms in the paper are binary.

Here, C stands for the entire protocol communication.

Similar models have been defined for the case where Alice and Bob start with a shared quantum state instead of classical information and try to generate, by classical communication, unitary operations on their local quantum systems, and local measurements, quantum keys, i.e., maximally entangled quantum states.

This paper is concerned with the classical model, but some of its results are inspired by the parallels between the two settings pointed out in [3]. Although we will come back to the quantum setting later in the paper in order to illustrate a further correspondence between the models, it can be fully understood without any knowledge in quantum physics or quantum information processing.

2.2 Measuring S: Information Bounds and Bound Information

The secret-key rate as a measure of the amount of extractable secret correlation in a distribution has been studied extensively in the literature. The objective is to express $S(X;Y||Z) = S(P_{XYZ})$, which is defined asymptotically and by a maximization over the set of all possible protocols, in terms of simpler, non-asymptotically defined properties of the distribution P_{XYZ} such as the information-theoretic quantities $I(X;Y)$ or $I(X;Y|Z)$.

The following *lower* bound is a consequence of a random-coding argument by Csiszár and Körner [1] and states that an initial advantage can be used for extracting a secret key.

Theorem 1. [1], [6], [7] *For any distribution P_{XYZ}, we have*

$$S(X;Y||Z) \geq \max\{I(X;Y) - I(X;Z)\,,\, I(Y;X) - I(Y;Z)\}\ . \tag{4}$$

Inequality (4) is not tight: $S(X;Y||Z)$ can be positive even when the right-hand side of (4) is negative [6], [9].

The best *upper* bound on $S(X;Y||Z)$ known so far is the intrinsic information $I(X;Y\downarrow Z)$ between X and Y, given Z, which is, intuitively, the remaining mutual information between Alice and Bob after Eve's choice of her best possible viewpoint.

Definition 2. [8] Let P_{XYZ} be a discrete probability distribution. Then the *intrinsic conditional mutual information between X and Y given Z* is

$$I(X;Y{\downarrow}Z) := \inf_{XY \to Z \to \overline{Z}} I(X;Y|\overline{Z})\ .$$

The infimum in Definition 2 is taken over all $\overline{Z}$ such that $XY \to Z \to \overline{Z}$ is a Markov chain, i.e., over all channels $P_{\overline{Z}|Z}$ that can be chosen by Eve for processing her data. (A recent unpublished result states that if $|\mathcal{Z}|$ is finite, then the infimum is a *minimum*, taken by a channel $P_{\overline{Z}|Z}$ which does not extend the alphabet, i.e., $|\overline{\mathcal{Z}}| \leq |\mathcal{Z}|$.)

Theorem 2. [8] *For any distribution P_{XYZ}, we have*

$$S(X;Y||Z) \leq I(X;Y{\downarrow}Z) \ . \tag{5}$$

The question whether the bound (5) is tight or not has been open. Motivated by the phenomenon of *bound* (non-distillable) quantum entanglement, distributions for which $S = 0$ holds although $I(X;Y{\downarrow}Z)$ is positive are said to have bound information, but have not been shown to exist. In fact, it has not even been known whether there exist distributions for which equality does *not* hold in (5).

Definition 3. [3] Let P_{XYZ} be such that $I(X;Y{\downarrow}Z) > 0$ but $S(X;Y||Z) = 0$ hold. Then P_{XYZ} is said to have *bound information.*

Let $(P_{XYZ})_n = P_{X_{(n)}Y_{(n)}Z_{(n)}}$ be a sequence of distributions such that

$$I(X_{(n)};Y_{(n)}{\downarrow}Z_{(n)}) \geq c > 0$$

for all n, but

$$S(X_{(n)};Y_{(n)}||Z_{(n)}) \to 0 \ \text{ if } \ n \to \infty \ .$$

Then, the sequence $(P_{XYZ})_n$ is said to have *asymptotic bound information.*

3 A New Bound on the Secret-Key Rate

3.1 The Limited Effect of Adversarial Side Information: A Bit Harms Just a Bit

The secret-key rate $S(X;Y||Z)$ is one particular measure for quantifying the amount of conditional correlation in a distribution. Another, simpler, such measure is the conditional mutual information $I(X;Y|Z)$. As a preparation for the rest of this paper, we show that the secret-key rate has an important property in common with the conditional information, namely that *additional side information accessible to the adversary cannot reduce the quantity in question by more than the entropy of this side information.* For the conditional information, this property reads as follows (where X, Y, Z, and U are arbitrary discrete random variables):

$$I(X;Y|ZU) \geq I(X;Y|Z) - H(U) \ .^{4} \tag{6}$$

[4] A stronger version of this inequality is

$$|I(X;Y|ZU) - I(X;Y|Z)| \leq H(U)$$

and implies immediately Shannon's above-mentioned theorem if we interpret X as the message, Y as the ciphertext, and U as the key (Z being trivial):

$$|\underbrace{I(X;Y|U)}_{=H(X)} - \underbrace{I(X;Y)}_{=0}| \leq H(U) \ .$$

It is less surprising that this property holds for the secret-key rate than that it *does not hold* for the intrinsic information, as we will see in Section 3.2.

Theorem 3. *Let X, Y, Z, and U be arbitrary discrete random variables. Then*

$$S(X;Y||ZU) \geq S(X;Y||Z) - H(U) \ .$$

Proof. Let $R < S(X;Y||Z)$. Then there exists, for all $\varepsilon > 0$ and sufficiently large N, a protocol (with communication C) such that Alice and Bob (knowing X^N and Y^N) end up with S_A and S_B, respectively, and such that there exists S satisfying (1), (2), and (3). Let $\mathcal{E}$ denote the event $S_A \neq S \vee S_B \neq S$, let $\overline{\mathcal{E}}$ be its complement and $\chi_{\mathcal{E}}$ its characteristic random variable, satisfying $\chi_{\mathcal{E}} = \mathcal{E}$ if $\mathcal{E}$ occurs and $\chi_{\mathcal{E}} = \overline{\mathcal{E}}$ otherwise. We then have[5]

$$\begin{aligned}
H(S_A) &\geq H(S_A|\chi_{\mathcal{E}}) \\
&\geq P_{\chi_{\mathcal{E}}}(\overline{\mathcal{E}}) \cdot H(S_A|\chi_{\mathcal{E}} = \overline{\mathcal{E}}) \\
&\geq (1-\varepsilon) \cdot H_\infty(S_A|\chi_{\mathcal{E}} = \overline{\mathcal{E}}) \\
&\geq (1-\varepsilon)(-\log(1/|\mathcal{S}|(1-\varepsilon))) \\
&= (1-\varepsilon)(\log|\mathcal{S}| + \log(1-\varepsilon)) \ ,
\end{aligned}$$

$$\begin{aligned}
H(S_A|S_B) &\leq H(S_A|S_B\chi_{\mathcal{E}}) + H(\chi_{\mathcal{E}}) \\
&\leq P_{\chi_{\mathcal{E}}}(\mathcal{E}) \log|\mathcal{S}| + h(\varepsilon) \\
&\leq \varepsilon \log|\mathcal{S}| + h(\varepsilon) \ ,
\end{aligned}$$

$$\begin{aligned}
I(S_A;CZ^NU^N) &= I(S_A;CZ^N) + \underbrace{I(S_A;U^N|CZ^N)}_{\leq H(U^N)} \\
&\leq I(S;CZ^N) + H(S_A|S) + N \cdot H(U) \\
&\leq \varepsilon + \varepsilon \log|\mathcal{S}| + h(\varepsilon) + N \cdot H(U) \ ,
\end{aligned}$$

and, because of (1),

$$\underbrace{I(S_A;S_B)}_{H(S_A)-H(S_A|S_B)} \quad - \quad I(S_A;CZ^NU^N) \geq (R - H(U) - \Theta(\varepsilon))N$$

holds for sufficiently large N. According to the bound (4), secret-key agreement with respect to the new random variables S_A, S_B, and $[CZ^NU^N]$ is possible at a rate $S(S_A;S_B||CZ^NU^N) \geq (R - H(U) - \Theta(\varepsilon))N$. Since N realizations of $(X, Y, [ZU])$ are required to achieve one realization of $(S_A, S_B, [CZ^NU^N])$, we have

$$S(X;Y||ZU) \geq S(S_A\,;\,S_B\,||\,CZ^NU^N)/N \geq R - H(U) - \Theta(\varepsilon) \ .$$

This concludes the proof because $\varepsilon > 0$ and $R < S(X;Y||Z)$ were arbitrary. □

[5] Here, $h(p) := -(p\log p + (1-p)\log(1-p))$ is the binary entropy function, and $H_\infty(X)$ is the *min-entropy* of a distribution P_X, defined as $H_\infty(X) := -\log \max_{x\in\mathcal{X}} P_X(x)$. We make use of the fact that for all X, $H_\infty(X) \leq H(X)$ holds.

3.2 The Intrinsic-Information Bound Is Not Tight

Let us now show the more surprising fact that the intrinsic information does not have the property studied in the previous section. Clearly, an immediate consequence will be that equality *cannot* always hold in (5) since two measures with different properties cannot be identical.

Let P_{XYZU} be the following distribution with the ranges $\mathcal{X} = \mathcal{Y} = \{0, 1, 2, 3\}$ and $\mathcal{Z} = \mathcal{U} = \{0, 1\}$.

$$P_{XYZU}(0,0,0,0) = P_{XYZU}(1,1,0,0) = P_{XYZU}(0,1,1,0) = P_{XYZU}(1,0,1,0) = 1/8 ,$$
$$P_{XYZU}(2,2,0,1) = P_{XYZU}(3,3,1,1) = 1/4 .$$

All the other probabilities are 0. We represent this distribution graphically. (Note that Z and U are uniquely determined by X and Y.)

$Y \backslash X$	0	1	2	3
0	1/8	1/8	0	0
1	1/8	1/8	0	0
2	0	0	1/4	0
3	0	0	0	1/4

$$Z \equiv X + Y \pmod 2 \quad \text{if} \quad X, Y \in \{0, 1\}$$
$$Z \equiv X \pmod 2 \quad \text{if} \quad X \in \{2, 3\}$$
$$U = \lfloor X/2 \rfloor .$$

The intuition behind the "weirdness" of this distribution is as follows. Given that Eve does not know the bit U, she has the additional disadvantage (besides not knowing this bit, which can hence directly be used as a secret-key bit by Alice and Bob) not to know how to process the bit Z (i.e., whether to forget it or not) in order to minimize $I(X;Y|\overline{Z})$. This explains both why the intrinsic information reduces by more than one bit when Eve learns U, as well as why the secret-key rate is only 1: Eve has the potential to destroy all the correlation besides U (if only she knew $U\ldots$).

Lemma 1. *For the given distribution, we have*

$$I(X;Y{\downarrow}Z) = 3/2 , \quad I(X;Y{\downarrow}ZU) = 0 , \quad \text{and} \quad H(U) = 1 .$$

Proof. We show first $I(X;Y{\downarrow}Z) = 3/2$. Let $P_{\overline{Z}|Z}$ be an arbitrary discrete binary-input channel, let $\overline{z} \in \overline{\mathcal{Z}}$, and let $p := P_{\overline{Z}|Z}(\overline{z}, 0)$, $q := P_{\overline{Z}|Z}(\overline{z}, 1)$. Then the distribution $P_{XY|\overline{Z}=\overline{z}}$ is given by the following table.

$Y \backslash X$	0	1	2	3
0	$\frac{p}{4(p+q)}$	$\frac{q}{4(p+q)}$	0	0
1	$\frac{q}{4(p+q)}$	$\frac{p}{4(p+q)}$	0	0
2	0	0	$\frac{p}{2(p+q)}$	0
3	0	0	0	$\frac{q}{2(p+q)}$

We have

$$I(X;Y|\overline{Z}=\overline{z}) = 1 + \frac{1}{2}\left(1 - h\left(\frac{p}{p+q}\right)\right) + \frac{1}{2}\, h\left(\frac{p}{p+q}\right) = 3/2 \ .$$

Thus, $I(X;Y|\overline{Z}) = \sum_{\overline{z}} P_{\overline{Z}}(\overline{z}) \cdot I(X;Y|\overline{Z}=\overline{z}) = 3/2$. Since the channel was arbitrary, it follows that $I(X;Y{\downarrow}Z) = 3/2$.

We now show that $I(X;Y{\downarrow}ZU) = 0$. Consider the following channel $P_{\overline{ZU}|ZU}$:

$$P_{\overline{ZU}|ZU}(\Delta|(0,0)) = P_{\overline{ZU}|ZU}(\Delta|(1,0)) = P_{\overline{ZU}|ZU}(0|(0,1)) = P_{\overline{ZU}|ZU}(1|(1,1)) = 1 \ .$$

It is easy to check that $I(X;Y|\overline{ZU}) = 0$ holds, hence $I(X;Y{\downarrow}ZU) = 0$. □

From Lemma 1, combined with Theorem 3, we can immediately conclude that the given distribution satisfies

$$I(X;Y{\downarrow}Z) = 3/2 \ ,$$

but

$$S(X;Y||Z) \leq S(X;Y||ZU) + H(U) \leq I(X;Y{\downarrow}ZU) + 1 \leq 1 \ . \tag{7}$$

In fact, equality holds in (7), i.e.,

$$S(X;Y||Z) = 1 \ ,$$

since the bit called U is a secret-key bit known only to Alice and Bob. We emphasize that this is the first example of a distribution P_{XYZ} for which it is known that $S(X;Y||Z) \neq I(X;Y{\downarrow}Z)$ holds.

Corollary 1. *For the given distribution we have*

$$1 = S(X;Y||Z) < I(X;Y{\downarrow}Z) = 3/2 \ .$$

3.3 A New Information Measure Which Is a Stronger Bound on S

A generalization of this reasoning immediately leads to a new conditional information measure which bounds the secret-key rate from above.

Definition 4. Let P_{XYZ} be a discrete distribution. Then the *reduced intrinsic information of* X *and* Y *given* Z, denoted by $I(X;Y{\downarrow}{\downarrow}Z)$, is defined by

$$I(X;Y{\downarrow}{\downarrow}Z) := \inf_{P_{U|XYZ}} \left(I(X;Y{\downarrow}ZU) + H(U)\right) \ .$$

The infimum is taken over all conditional probability distributions $P_{U|XYZ}$.

Lemma 2. *The reduced intrinsic information has the following properties. Let* X, Y, Z, *and* U *be arbitrary random variables.*

1. $I(X;Y{\downarrow}{\downarrow}Z) \leq I(X;Y{\downarrow}Z)$,
2. $I(X;Y{\downarrow}{\downarrow}ZU) \geq I(X;Y{\downarrow}{\downarrow}Z) - H(U)$.

Proof.

1. Choose U with $H(U) = 0$ in Definition 4.
2. Let P_{XYZU} be a fixed distribution. Then

$$\begin{aligned} I(X;Y{\downarrow}{\downarrow}Z) &= \inf_{P_{V|XYZ}} (I(X;Y{\downarrow}ZV) + H(V)) \\ &\le \inf_{P_{U'|XY(Z,U)}} (I(X;Y{\downarrow}ZUU') + H(UU')) \\ &\le \inf_{P_{U'|XY(Z,U)}} (I(X;Y{\downarrow}ZUU') + H(U') + H(U|U')) \\ &\le I(X;Y{\downarrow}{\downarrow}ZU) + H(U) \ . \end{aligned} \tag{8}$$

In the second step of (8), the infimum is restricted to random variables $V = [UU']$ containing U.

□

The most important property of $I(X;Y{\downarrow}{\downarrow}Z)$, however, is that it is an upper bound on the secret-key rate (that is strictly stronger than $I(X;Y{\downarrow}Z)$). Corollary 2 follows directly from Theorem 3, Corollary 1, and Lemma 2.

Corollary 2. *For* every *distribution P_{XYZ}, we have*

$$S(X;Y||Z) \le I(X;Y{\downarrow}{\downarrow}Z) \le I(X;Y{\downarrow}Z) \ ;$$

for some *distributions P_{XYZ}, we have*

$$I(X;Y{\downarrow}{\downarrow}Z) < I(X;Y{\downarrow}Z) \ .$$

3.4 The Gap Can Be Arbitrarily Large: Asymptotic Bound Information

We have seen in the previous section that the intrinsic information is not always a tight upper bound on the secret-key rate. In Section 4 we will show, however, that $I(X;Y{\downarrow}Z)$ nevertheless remains an interesting and meaningful measure of correlated secrecy since it indicates the amount of perfectly secret bits required to *synthesize* a certain distribution by public communication.

Before this, we show that the gap between the secret-key rate (or the *reduced* intrinsic information) and the intrinsic information can be arbitrarily large; this will imply the existence of asymptotic bound information.

Let $(P_{XYZ})_n$ be the following distribution (where $\mathcal{X} = \mathcal{Y} = \{0, 1, \ldots, 2n-1\}$ and $\mathcal{Z} = \{0, 1, \ldots, n-1\}$).

$Y \backslash X$	0	$\cdots$	$n-1$	n	$n+1$	$\cdots$	$2n-1$
0	$\frac{1}{2n^2}$	$\cdots$	$\frac{1}{2n^2}$	0	0	$\cdots$	0
$\vdots$	$\vdots$		$\vdots$	$\vdots$	$\vdots$		$\vdots$
$n-1$	$\frac{1}{2n^2}$	$\cdots$	$\frac{1}{2n^2}$	0	0	$\cdots$	0
n	0	$\cdots$	0	$\frac{1}{2n}$	0	$\cdots$	0
$n+1$	0	$\cdots$	0	0	$\frac{1}{2n}$		0
$\vdots$	$\vdots$		$\vdots$	$\vdots$		$\ddots$	$\vdots$
$2n-1$	0	$\cdots$	0	0	0	$\cdots$	$\frac{1}{2n}$

$$Z \equiv X + Y \pmod{n} \;\text{ if }\; X, Y \in \{0, \ldots, n-1\}$$
$$Z \equiv X \pmod{n} \;\text{ if }\; X \in \{n, \ldots, 2n-1\} \; .$$

Lemma 3. *For the distribution* $(P_{XYZ})_n$*, we have*

$$I(X_{(n)} ; Y_{(n)} \downarrow Z_{(n)}) = 1 + \frac{1}{2} \log n$$

and

$$I(X_{(n)} ; Y_{(n)} \downarrow\downarrow Z_{(n)}) = 1 \; .$$

The proof of Lemma 3 is very similar to the proof of Lemma 1.

Proof. The index n is omitted. Let first $P_{\overline{Z}|Z}$ be an arbitrary discrete n-ary-input channel, let $\overline{z} \in \overline{\mathcal{Z}}$, and let $p_i := P_{\overline{Z}|Z}(\overline{z}, i)$ for $i = 0, \ldots, n-1$. Then

$$\begin{aligned} I(X;Y|\overline{Z} = \overline{z}) &= 1 + \frac{1}{2}\left(\log n - H\left(\frac{p_0}{\sum p_i}, \ldots, \frac{p_{n-1}}{\sum p_i}\right)\right) + \frac{1}{2}\left(H\left(\frac{p_0}{\sum p_i}, \ldots, \frac{p_{n-1}}{\sum p_i}\right)\right) \\ &= 1 + \frac{1}{2} \log n \; . \end{aligned}$$

Hence $I(X;Y|\overline{Z}) = 1 + (\log n)/2$, and, since the channel was chosen arbitrarily, $I(X;Y{\downarrow}Z) = 1 + (\log n)/2$.

On the other hand, consider the bit

$$U := \lfloor X/n \rfloor \quad \text{satisfying} \quad H(U) = 1 \; .$$

Then $I(X;Y \downarrow ZU) = 0$ (the corresponding channel $P_{\overline{ZU}|ZU}$ is an immediate generalization of the channel from the proof of Lemma 1), and

$$I(X;Y{\downarrow\downarrow}Z) \leq I(X;Y{\downarrow}ZU) + H(U) = 1 \tag{9}$$

hold. In fact, equality holds in (9) since $S(X_{(n)};Y_{(n)}||Z_{(n)}) \geq H(U) = 1$. □

Let now $(Q_{XYZ})_n$ be the following sequence of distributions derived from $(P_{XYZ})_n$ (where all the alphabets are extended by the "erasure symbol" Δ):

$$(Q_{XYZ})_n(x,y,z) = \begin{cases} \frac{1}{\log n}(P_{XYZ})_n(x,y,z) & \text{if } x \neq \Delta\,,\; y \neq \Delta\,,\; z \neq \Delta\,, \\ 1 - \frac{1}{\log n} & \text{if } x = y = z = \Delta\;. \end{cases}$$

For this new distribution, we have

$$I(X_{(n)};Y_{(n)}\downarrow Z_{(n)}) = \frac{1}{\log n}\cdot\left(1+\frac{1}{2}\log n\right) > \frac{1}{2}$$

but

$$S(X_{(n)};Y_{(n)}||Z_{(n)}) = \frac{1}{\log n} \to 0\ .$$

In other words, the intrinsic information can be larger than some positive constant $c = 1/2$ whereas the secret-key rate is, at the same time, arbitrarily close to 0.

Theorem 4. *There exist sequences of distributions with asymptotic bound information.*

4 Building a Distribution from Secret-Key Bits, and Reductions Among Correlations

4.1 Information of Formation ...

In Section 3 we have shown that the intrinsic information measure is *not* a tight bound on the rate at which secret-key bits can be extracted from repeated realizations of a random experiment P_{XYZ}. Despite this fact, and although we have even derived a better (generally smaller) upper bound, intrinsic information nevertheless remains an important quantity for measuring the secret correlation in P_{XYZ}. We will show that it is a lower bound on the number of secret-key bits required to *generate*, using public communication, random variables distributed according to P_{XYZ}. This means that certain distributions require *asymptotically strictly more* secret bits to be formed than can be extracted from them.

We first define the *information of formation* which can be seen as the classical analog to entanglement of formation. It is, roughly speaking, the rate at which secret bits are required to synthesize a distribution which is, in terms of the provided privacy, at least as good as P_{XYZ} from Alice and Bob's point of view.

Definition 5. Let P_{XYZ} be the joint distribution of three discrete random variables X, Y, and Z. The *information of formation of X and Y, given Z*, denoted by $I_{\text{form}}(X;Y|Z)$, is the infimum of all numbers $R \geq 0$ with the property that for all $\varepsilon > 0$ there exists N_0 such that for all $N \geq N_0$, there exists a protocol between Alice and Bob with communication C and achieving the following: Alice and Bob, both knowing the same random $\lfloor RN \rfloor$-bit string S, can finally compute X' and Y', respectively, such that there exist random variables X^N, Y^N, and Z^N jointly distributed according to $(P_{XYZ})^N$ (this is the distribution corresponding to n-fold independent repetition of the random experiment P_{XYZ}) and a channel $P_{\overline{C}|Z^N}$ such that

$$\text{Prob}\left[(X',Y',C) = (X^N,Y^N,\overline{C})\right] \geq 1-\varepsilon$$

holds.

Intuitively, the conditions of Definition 5 imply that with high probability, Alice's and Bob's random variables X' and Y' are distributed according to P_{XY}^N and the entire communication C can be simulated by an Eve knowing the corresponding Z^N. This latter condition formalizes the fact that the protocol communication C observed by Eve does not give her more information than Z^N.

4.2 ... Is Bounded from Below by Intrinsic Information

Theorem 5. *For every distribution P_{XYZ}, we have*

$$I_{\text{form}}(X;Y|Z) \geq I(X;Y{\downarrow}Z) \ .$$

Remark. Note that $I(X;Y \downarrow Z)$ is a stronger bound on $I_{\text{form}}(X;Y|Z)$ than $I(X;Y{\downarrow\downarrow}Z)$, and that both $I(X;Y)$ and $I(X;Y|Z)$ are *not* lower bounds on $I_{\text{form}}(X;Y|Z)$. This can be seen with the examples where X is a random bit and $X = Y = Z$ holds ($I(X;Y) = 1$ but $I_{\text{form}}(X;Y|Z) = 0$), and where X and Y are independent random bits and $Z = X \oplus Y$ ($I(X;Y|Z) = 1$ but $I_{\text{form}}(X;Y|Z) = 0$).

Proof of Theorem 5. The crucial observation here is that local data processing as well as sending messages cannot increase the intrinsic information of Alice's and Bob's pieces of information given what Eve knows.

We have, for arbitrary random variables A, B, E, and C_i (where C_i stands for the i-th message sent and A, B, and E for Alice's, Bob's, and Eve's complete knowledge before C_i is sent), that

$$I(AC_i\,;\, BC_i{\downarrow} EC_i) \leq I(A;B{\downarrow} E) \ .$$

This can be seen as follows. Let us assume without loss of generality that C_i is sent by Alice, i.e., $I(BE;C_i|A) = 0$ holds. Then

$$\begin{aligned}
I(AC_i\,;\, BC_i{\downarrow} EC_i) &\leq \inf_{P_{\overline{E}|E}} I(AC_i\,;\, BC_i\,|\,\overline{E}C_i) \\
&= \inf_{P_{\overline{E}|E}} I(A;B\,|\,\overline{E}C_i) \\
&= \inf_{P_{\overline{E}|E}} (H(B;\overline{E}C_i) - H(B;A\overline{E}C_i)) \\
&\leq \inf_{P_{\overline{E}|E}} (H(B;\overline{E}) - H(B;A\overline{E})) \\
&= \inf_{P_{\overline{E}|E}} I(A;B\,|\,\overline{E}) \\
&= I(A;B{\downarrow} E) \ .
\end{aligned}$$

In the fourth step, we have made use of the fact that the message C_i is generated by Alice.

Let now $R > I_{\mathrm{form}}(X;Y|Z)$ and $\varepsilon > 0$, and let a protocol as in Definition 5 be given. At the beginning of the protocol, which uses $\lfloor RN \rfloor$ secret-key bits to start with, the intrinsic information equals $\lfloor RN \rfloor$. Hence we get

$$\lfloor RN \rfloor \geq I(X';Y' \downarrow C) \ .$$

Let now $\mathcal{E}$ be the event that $(X',Y',C) \neq (X^N, Y^N, \overline{C})$ holds, $\overline{\mathcal{E}}$ its complementary event, and $\chi_{\mathcal{E}}$ its characteristic random variable. Then we have, by definition, $P_{\chi_{\mathcal{E}}}(\mathcal{E}) = \mathrm{Prob}\,[\mathcal{E}] \leq \varepsilon$, and we can conclude[6]

$$\begin{aligned}
\lfloor RN \rfloor &\geq I(X';Y' \downarrow C) \\
&= \inf_{P_{\tilde{C}|C}} I(X';Y'|\tilde{C}) \\
&\geq \inf_{P_{\tilde{C}|C}} (I(X';Y'|\tilde{C}\chi_{\mathcal{E}}) - h(\varepsilon)) \\
&\geq \inf_{P_{\tilde{C}|C}} (P_{\chi_{\mathcal{E}}}(\overline{\mathcal{E}}) \cdot I(X';Y'|\tilde{C},\overline{\mathcal{E}}) - h(\varepsilon)) \\
&= \inf_{P_{\tilde{C}|\overline{C}}} (P_{\chi_{\mathcal{E}}}(\overline{\mathcal{E}}) \cdot I(X^N;Y^N|\tilde{C},\overline{\mathcal{E}}) - h(\varepsilon)) \\
&= \inf_{P_{\tilde{C}|\overline{C}}} (I(X^N;Y^N|\tilde{C}\chi_{\mathcal{E}}) - P_{\chi_{\mathcal{E}}}(\mathcal{E}) \cdot I(X^N;Y^N|\tilde{C},\mathcal{E}) - h(\varepsilon)) \\
&\geq \inf_{P_{\tilde{C}|\overline{C}}} (I(X^N;Y^N|\tilde{C}\chi_{\mathcal{E}}) - \varepsilon \cdot \min(\log|\mathcal{X}^N|, \log|\mathcal{Y}^N|) - h(\varepsilon)) \\
&\geq \inf_{P_{\tilde{C}|\overline{C}}} I(X^N;Y^N|\tilde{C}) - 2h(\varepsilon) - \varepsilon \cdot N \cdot \min(\log|\mathcal{X}|, \log|\mathcal{Y}|) \\
&= I(X^N;Y^N \downarrow \overline{C}) - 2h(\varepsilon) - \varepsilon \cdot N \cdot \min(\log|\mathcal{X}|, \log|\mathcal{Y}|) \\
&\geq I(X^N;Y^N \downarrow Z^N) - 2h(\varepsilon) - \varepsilon \cdot N \cdot \min(\log|\mathcal{X}|, \log|\mathcal{Y}|) \\
&= N \cdot I(X;Y \downarrow Z) - 2h(\varepsilon) - \varepsilon \cdot N \cdot \min(\log|\mathcal{X}|, \log|\mathcal{Y}|) \ .
\end{aligned}$$

In the second last step we have used the fact that $\overline{C}$ can be generated by sending Z^N over a channel $P_{\overline{C}|Z^N}$ (which is true by definition).

Since $\varepsilon > 0$ and $R > I_{\mathrm{form}}(X;Y|Z)$ were arbitrary, this concludes the proof. □

For every distribution P_{XYZ} we now have

$$S(X;Y||Z) \leq I(X;Y\downarrow\downarrow Z) \leq I(X;Y\downarrow Z) \leq I_{\mathrm{form}}(X;Y|Z) \ , \qquad (10)$$

and for some, equality does not hold in the second inequality of (10), hence

$$S(X;Y||Z) \neq I_{\mathrm{form}}(X;Y|Z) \ .$$

[6] For simplicity, the proof is only given for the case where at least one of the ranges $\mathcal{X}$ or $\mathcal{Y}$ is finite. The proof for the general case is somewhat more involved and uses a separation of the ranges into a finite and an infinite part such that the random variables X and Y, restricted to the infinite part, have only negligible mutual information.

These distributions have the property to require asymptotically more secret bits to be generated than can be maximally extracted from them. The rest of the correlation seems to be used up, or trapped in X, Y, and Z forever.

4.3 Generating a Secret Correlation From Another: In General, There Are Losses

The concepts of key agreement and formation of a distribution studied above can be seen as special cases of a general *secret-correlations calculus*: Given the outcomes of (many independent realizations) of a random experiment P_{XYZ}, is it possible to construct instances of another distribution $P_{X'Y'Z'}$ (or a distribution less favorable for Eve, i.e., where Eve has less information in the sense of Definition 5), and if *yes*, at which rate

$$R_{\rm sec}(P_{X'Y'Z'} \leftarrow P_{XYZ}) \ ?$$

By similar arguments as used in the proof of Theorem 5, one obtains the bound

$$R_{\rm sec}(P_{X'Y'Z'} \leftarrow P_{XYZ}) \leq \frac{I(X;Y{\downarrow}Z)}{I(X';Y'{\downarrow}Z')} \ . \tag{11}$$

(Note, as above, that the same bound does *not* hold if the intrinsic information is replaced by, for instance, the usual conditional mutual information.)

Theorems 2 and 5 are now special cases of inequality (11): If $P_{BB\Delta}$ denotes the distribution of a secret bit ($P_{BB\Delta}(0,0,\delta) = P_{BB\Delta}(1,1,\delta) = 1/2$), then we have

$$R_{\rm sec}(P_{BB\Delta} \leftarrow P_{XYZ}) = S(X;Y||Z)$$

and, since $I(B;B{\downarrow}\,\Delta) = 1$, inequality (11) is nothing else but Theorem 2. On the other hand, we have

$$R_{\rm sec}(P_{XYZ} \leftarrow P_{BB\Delta}) = \frac{1}{I_{\rm form}(X;Y|Z)} \ ,$$

and inequality (11) turns into Theorem 5.

The results of Section 3 imply that equality does generally not hold in (11). Even worse, for every $\varepsilon > 0$ there exist distributions P_{XYZ} and $P_{X'Y'Z'}$ with

$$R_{\rm sec}(P_{X'Y'Z'} \leftarrow P_{XYZ}) \cdot R_{\rm sec}(P_{XYZ} \leftarrow P_{X'Y'Z'}) < \varepsilon \ .$$

Like currency exchange, "exchanging secret correlations" is (even asymptotically) not loss-free.

5 Concluding Remarks and Open Questions

We have shown that some partially-secret correlations P_{XYZ} are wasteful with secret bits in the sense that some of the key bits that would be required to construct the correlation cannot be extracted. More specifically, for some distributions even an arbitrarily large fraction of them are lost.

A similar phenomenon is well-known in the scenario of quantum key agreement. Let ρ be a mixed quantum state between Alice and Bob. The *entanglement of formation* (the classical analog of which is defined in Section 4) is the rate at which EPR pairs (maximally entangled quantum bits) are required asymptotically in order to construct (a state close to) ρ by classical communication and local quantum operations. The *distillability* (its classical analog is the secret-key rate) on the other hand is the number of EPR pairs (or states very close to EPR pairs) that can (asymptotically) be distilled from ρ by local quantum operations and classical communication. (The adversary does not have to be taken into account here since EPR pairs are *pure* states and hence not entangled with the environment.) The entanglement of formation and the distillability are two *measures for entanglement* which can differ by an arbitrarily large factor.

Let us conclude with two questions. First, is $S(X;Y||Z) \neq I(X;Y\downarrow\downarrow Z)$ possible? Secondly, is $I_{\mathrm{form}}(X;Y|Z) > 0$ but $S(X;Y||Z) = 0$ possible? We believe that the answer to the second question is *yes*. Some examples of distributions that might have this property were presented in [3]; they are the classical translations of bound entangled quantum states. Another candidate, which (at first sight) is not related to bound entanglement, arises when the distribution of Section 3.2 is modified as follows.

Y \ X	0	1	2	3
0	1/8	1/8	a	a
1	1/8	1/8	a	a
2	a	a	1/4	0
3	a	a	0	1/4

$$
\begin{aligned}
&Z \equiv X + Y \pmod 2 \;\; \text{if} \;\; X, Y \in \{0, 1\} \;, \\
&Z \equiv X \pmod 2 \;\; \text{if} \;\; X, Y \in \{2, 3\} \;, \\
&Z = (X, Y) \;\; \text{otherwise.}
\end{aligned}
$$

(The distribution must be re-normalized.) We have $I(X;Y\downarrow Z) > 0$ for any $a \geq 0$, but it seems that $S(X;Y||Z)$ vanishes if a is chosen large enough (probably $a \geq 1/4\sqrt{2}$, in which case the correlation useful for key agreement seems destroyed). An indication that this is indeed so is the fact that the "translation" of this distribution to a quantum state turned out to be a bound entangled state (one that has not been known previously) [12].

Acknowledgments

The distribution analyzed in Section 3.2 was proposed by Juraj Skripsky. The authors thank Nicolas Gisin and Ueli Maurer for interesting and helpful discussions on the subject of this paper. The first author was supported by the Swiss National Science Foundation (SNF), and the second author was supported by Canada's NSERC.

References

1. I. Csiszár and J. Körner, Broadcast channels with confidential messages, *IEEE Transactions on Information Theory*, Vol. IT-24, pp. 339–348, 1978.
2. 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.
3. N. Gisin and S. Wolf, Linking classical and quantum key agreement: is there "bound information"?, *Proceedings of CRYPTO 2000*, Lecture Notes in Computer Science, Vol. 1880, pp. 482–500, Springer-Verlag, 2000.
4. 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.
5. P. Horodecki, Separability criterion and inseparable mixed states with positive partial transposition, *Phys. Lett. A*, Vol. 232, p. 333, 1997.
6. U. Maurer, Secret key agreement by public discussion from common information, *IEEE Transactions on Information Theory*, Vol. 39, No. 3, pp. 733–742, 1993.
7. U. Maurer and S. Wolf, Information-theoretic key agreement: from weak to strong secrecy for free, *Proceedings of EUROCRYPT 2000*, Lecture Notes in Computer Science, Vol. 1807, pp. 352–368, Springer-Verlag, 2000.
8. U. Maurer and S. Wolf, Unconditionally secure key agreement and the intrinsic conditional information, *IEEE Transactions on Information Theory*, Vol. 45, No. 2, pp. 499–514, 1999.
9. U. Maurer and S. Wolf, Towards characterizing when information-theoretic secret key agreement is possible, *Proceedings of ASIACRYPT '96*, Lecture Notes in Computer Science, Vol. 1163, pp. 196–209, Springer-Verlag, 1996.
10. S. Popescu and D. Rohrlich, Thermodynamics and the measure of entanglement, quant-ph/9610044, 1996.
11. C. E. Shannon, Communication theory of secrecy systems, *Bell System Technical Journal*, Vol. 28, pp. 656–715, 1949.
12. F. Spedalieri, personal communication, 2003.
13. G. S. Vernam, Cipher printing telegraph systems for secret wire and radio telegraphic communications, *Journal of the American Institute for Electrical Engineers*, Vol. 55, pp. 109–115, 1926.
14. A. D. Wyner, The wire-tap channel, *Bell System Technical Journal*, Vol. 54, No. 8, pp. 1355–1387, 1975.