

# A New Measure for Conditional Mutual Information and its Properties

Renato Renner<sup>1</sup>Juraj Skripsky<sup>1</sup>Stefan Wolf<sup>2</sup>

**Abstract** — We propose a new conditional mutual information measure, called the *reduced intrinsic information*, and show its significance in the context of determining the number of secret-key bits that can be extracted from distributed information by public communication.

## I. THE REDUCED INTRINSIC INFORMATION

The *secret-key rate*  $S(X; Y|Z)$  of a tripartite probability distribution  $P_{XYZ}$  is the rate at which two parties, knowing realizations of  $X$  and  $Y$ , respectively, can generate, by public communication, common bits about which a third party, who has access to  $Z$ , remains almost completely ignorant [1]. It is a fundamental problem to express  $S(X; Y|Z)$  in terms of  $P_{XYZ}$ . In [2], the *intrinsic information*  $I(X; Y \downarrow Z) := \inf_{P_{\bar{Z}|Z}}(I(X; Y|\bar{Z}))$  was shown to be an upper bound on  $S(X; Y|Z)$ . (Here, the infimum is taken over all possible ways the third party Eve can process her information  $Z$ .)

The following facts were shown in [3] and imply that this bound is, however, *not tight*: First, we have for all  $P_{XYZU}$  that  $S(X; Y|ZU) \geq S(X; Y|Z) - H(U)$  holds, whereas, secondly, the intrinsic information does *not* have this property which we will call *smoothness* (and which the usual mutual information  $I(X; Y|Z)$  clearly has). Intuitively speaking,  $I(X; Y \downarrow Z)$  fails to be smooth since *additional* side information  $U$  can also help the adversary to use the *previous* information  $Z$  more effectively, thereby reducing the information shared by the legitimate partners by more than just  $H(U)$ .

These observations lead to a stronger upper bound on  $S(X; Y|Z)$ , namely the largest smooth lower bound on the intrinsic information, which we call *reduced intrinsic information*.

**Definition 1.** The *reduced intrinsic information* between  $X$  and  $Y$ , given  $Z$ , is

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

## II. PROPERTIES

According to the above discussion, the reduced intrinsic information measure is an upper bound on the secret-key rate,

$$S(X; Y|Z) \leq I(X; Y \downarrow\downarrow Z).$$

As sketched already, it can be strictly smaller than the previous bound  $I(X; Y \downarrow Z)$  because possible refinements, using

<sup>1</sup>Computer Science Department, Swiss Federal Institute of Technology (ETH Zürich), CH-8092 Zurich, Switzerland. E-mail: {renner@inf, jskripsky@student}.ethz.ch. The first author was supported by the Swiss National Science Foundation (SNF).

<sup>2</sup>Département d'Informatique et recherche opérationnelle, Université de Montréal, C.P. 6128 succ Centre-Ville, Montréal, Québec, H3C 3J7, Canada. E-mail: wolf@iro.umontreal.ca. Supported by Canada's NSERC.

some side information  $U$ , of Eve's strategy for minimizing the correlation shared by the other parties are taken into account. It is important to note, however, that Eve, knowing  $Z$  but not  $U$ , cannot actually apply these strategies; their mere existence, however, allows for improving the bound.

**Theorem 1.** Let  $P_{XYZ}$  be a distribution, and let  $\mathcal{E}_1, \mathcal{E}_2, \dots, \mathcal{E}_n$  be disjoint events with probabilities  $\text{Prob}[\mathcal{E}_i] = p_i$  such that  $\sum_i p_i = 1$ . Then

$$I(X; Y \downarrow\downarrow Z) \leq \sum_{i=1}^n p_i I(X; Y \downarrow Z | \mathcal{E}_i) + H([p_1, p_2, \dots, p_n]).$$

In order to derive, from Theorem 1, the mentioned fact that  $I(X; Y \downarrow\downarrow Z)$  can be strictly smaller than  $I(X; Y \downarrow Z)$ , we consider the special case where  $P_{XYZ}$  is composed in a certain way by two distributions—for which Eve's strategies of minimizing the information are a priori different. Then,  $I(X; Y \downarrow\downarrow Z)$  takes “adaptive” strategies, i.e., separate minimization, into account, whereas  $I(X; Y \downarrow Z)$  only allows for one global minimization, i.e., one single channel  $P_{\bar{Z}|Z}$ .

**Corollary 2.** Let  $P_{XYZ}$  be a distribution, let  $\mathcal{X}$  and  $\mathcal{Y}$  be the ranges of  $X$  and  $Y$ , respectively, let  $\mathcal{X} = \mathcal{X}_0 \cup \mathcal{X}_1$  (where  $\mathcal{X}_0$  and  $\mathcal{X}_1$  are disjoint) and analogously  $\mathcal{Y} = \mathcal{Y}_0 \cup \mathcal{Y}_1$ , such that  $P_{XYZ}(x, y, z) = 0$  if  $x \in \mathcal{X}_0$  and  $y \in \mathcal{Y}_1$  or vice versa, and let  $p = \text{Prob}[x \in \mathcal{X}_0]$ . We denote by  $P_{XYZ}^0 = P_{X^0 Y^0 Z^0}$  the distribution  $P_{XYZ|_{\mathcal{E}_0}}$ , and analogously for  $\mathcal{E}_1$ . Then we have

$$I(X; Y \downarrow\downarrow Z) \leq p \cdot \inf_{P_{\bar{Z}^0|Z^0}} (I(X^0; Y^0|\bar{Z}^0)) + (1-p) \cdot \inf_{P_{\bar{Z}^1|Z^1}} (I(X^1; Y^1|\bar{Z}^1)) + h(p).$$

Based on the bound of Corollary 2 it is not difficult to find distributions for which  $I(X; Y \downarrow\downarrow Z) < I(X; Y \downarrow Z)$  holds [3]. In combination with another result of [3], stating that the intrinsic information  $I(X; Y \downarrow Z)$  is a lower bound on the rate at which secret-key bits are required to generate a secret correlation  $P_{XYZ}$  by public communication, the gap between  $I(X; Y \downarrow Z)$  and  $I(X; Y \downarrow\downarrow Z)$  implies that some distributions do not allow for the extraction of the same number of secret-key bits as are needed to generate them (in fact, these quantities can differ by an arbitrarily large factor). Interestingly, a similar phenomenon is already well-known for mixed bipartite quantum states.

## REFERENCES

- [1] U. Maurer, Secret key agreement by public discussion from common information, *IEEE Transactions on Information Theory*, Vol. 39, No. 3, pp. 733–742, 1993.
- [2] 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.
- [3] R. Renner and S. Wolf, New bounds in secret-key agreement: the gap between formation and secrecy extraction, *Proceedings of EUROCRYPT 2003*, LNCS, Springer-Verlag, 2003.