The Intrinsic Conditional Mutual Information and Perfect Secrecy

Ueli Maurer and Stefan Wolf

Department of Computer Science
Swiss Federal Institute of Technology (ETH Zürich)
ETH Zentrum
CH-8092 Zürich
E-mail: {maurer,wolf}@inf.ethz.ch

Abstract — **Conditions are derived for the possibility and impossibility of information-theoretic secret-key agreement by public discussion. A new quantity, the intrinsic information, is introduced and its relationship to secret-key agreement is investigated. A new protocol is described that allows secret-key agreement in situations for which the previous protocols fail.**

I. Introduction

Consider a scenario in which two parties Alice and Bob and an adversary Eve have access to independent realizations of random variables X, Y, and Z, respectively, with joint distribution P_{XYZ}. The secret-key rate $S(X;Y||Z)$ has been defined in [1] as the maximal rate at which Alice and Bob can generate a secret key by communication over an insecure, but authenticated channel such that Eve's information about this key is arbitrarily small. It was shown in [1] that $S(X;Y||Z) \leq \min\{I(X;Y), I(X;Y|Z)\}$.

II. The Intrinsic Information

The following simple example shows that the secret-key rate can be 0 even if $I(X;Y) > 0$ and $I(X;Y|Z) > 0$.

Example. Let $\mathcal{X} = \mathcal{Y} = \mathcal{Z} = \{0,1,2,3\}$, $P_{XYZ}(0,0,0) = P_{XYZ}(0,1,1) = P_{XYZ}(1,0,1) = P_{XYZ}(1,1,0) = 1/8$, $P_{XYZ}(2,2,2) = P_{XYZ}(3,3,3) = 1/4$. Then $I(X;Y) = 3/2$ and $I(X;Y|Z) = 1/2$, but $S(X;Y||Z) = 0$. The reason for the latter is that Eve can send Z over the channel characterized by $P_{\overline{Z}|Z}(0,0) = P_{\overline{Z}|Z}(0,1) = P_{\overline{Z}|Z}(1,0) = P_{\overline{Z}|Z}(1,1) = 1/2$ and $P_{\overline{Z}|Z}(2,2) = P_{\overline{Z}|Z}(3,3) = 1$. The resulting random variable $\overline{Z}$ satisfies $I(X;Y||\overline{Z}) = 0$.

Intuitively, the additional random variable Z "destroys" all the mutual information between X and Y (because $Z = X = Y$ for $X, Y \in \{2,3\}$). On the other hand, given Z, there is (conditional) information between X and Y that has not been there originally (because $Z = X \oplus Y$ for $X, Y \in \{0,1\}$), and that cannot be used to generate a secret key. This additional information does not exist when Z is replaced by $\overline{Z}$.

We define the intrinsic conditional mutual information which measures only the initial information between X and Y, possibly reduced by Z, as the minimum of $I(X;Y|\overline{Z})$, taken over all random variables $\overline{Z}$ that can be obtained by sending Z over a channel which is independent of X and Y.

Definition. For a distribution P_{XYZ}, the *intrinsic conditional mutual information between X and Y when given Z*, denoted by $I(X;Y{\downarrow}Z)$, is given by

$$I(X;Y{\downarrow}Z) := \min \left\{ I(X;Y|\overline{Z}) \ : \ P_{XYZ\overline{Z}} = P_{XYZ} \cdot P_{\overline{Z}|Z} \right\} .$$

The minimum is taken over all possible conditional distributions $P_{\overline{Z}|Z}$.

It is obvious that $I(X;Y \downarrow Z) \leq I(X;Y)$, $I(X;Y \downarrow Z) \leq I(X;Y|Z)$, and that

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

We conjecture that secret-key agreement is possible unless $I(X;Y \downarrow Z) = 0$, i.e., that for all random variables X, Y, and Z we have $S(X;Y||Z) > 0$ if (and of course only if) $I(X;Y{\downarrow}Z) > 0$.

III. Secret-Key Agreement

For certain distributions P_{XYZ}, the statement of this conjecture has been proved. An example is the scenario where X, Y, and Z are generated by sending a binary random variable R, e.g., random bits emitted by a satellite, over three independent channels. For an analysis of this scenario see [2]. The considered protocol for secret-key agreement is a block protocol based on a simple repeat code. More precisely, it was shown first that one can assume that R, X, and Y are binary and symmetric, and that Z is equal to R sent over an erasure channel. Then, a possible protocol for secret-key agreement works as follows. For some fixed N, Alice randomly chooses a bit C and sends the block $[X_1 \oplus C, \ldots, X_N \oplus C]$ to Bob over the public channel. Bob computes $[(X_1 \oplus C) \oplus Y_1, \ldots, (X_N \oplus C) \oplus Y_N]$ and accepts only if this is equal to $[0,\ldots,0]$ or $[1,\ldots,1]$. It can be shown that, given $I(X;Y{\downarrow}Z) > 0$, Eve's error probability is exponentially (in N) greater than Bob's, and that this guarantees that the protocol allows secret-key agreement for sufficiently large N.

In a second scenario for which the statement of the above conjecture is proved, X and Y are binary and symmetric, and Z is generated by sending the pair (X,Y) over an erasure channel.

In the more general case where Z is generated by sending X and Y over two independent erasure channels, the repeat-code protocol is not optimal, and a probabilistic coding using "pseudo-repeat codes" with a certain fraction of incorrect bits can be better (see [3]).

References

[1] U. M. 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. M. Maurer and S. Wolf, "Towards characterizing when information-theoretic secret key agreement is possible", *Advances in Cryptology - ASIACRYPT '96*, Lecture Notes in Computer Science, Vol. 1163, pp. 196-209, Springer-Verlag, 1996.

[3] U. M. Maurer and S. Wolf, "The intrinsic conditional mutual information and perfect secrecy", preprint, 1996.