On the Secret-Key Rate of Binary Random Variables

Martin J. Gander
Department of Computer Science
Stanford University
Stanford, CA 94305-2140, USA

Ueli M. Maurer
Institute for Theoretical Computer Science
ETH Zürich
CH-8092 Zürich, Switzerland

Abstract — **Consider a scenario in which two parties Alice and Bob as well as an opponent Eve receive the output of a binary symmetric source (e.g. installed in a satellite) over individual, not necessarily independent binary symmetric channels. Alice and Bob share no secret key initially and can only communicate over a public channel completely accessible to Eve. We derive a lower bound on the rate at which Alice and Bob can generate secret-key bits about which Eve has arbitrarily little information. This lower bound is strictly positive as long as Eve's binary symmetric channel is not perfect, even if Alice's and Bob's channels are by orders of magnitude less reliable than Eve's channel.**

I. Introduction

We assume in this paper that Alice, Bob and Eve know the sequences of binary random variables $X^N = [X_1, X_2, \ldots X_N]$, $Y^N = [Y_1, Y_2, \ldots Y^N]$ and $Z^N = [Z_1, Z_2, \ldots Z_N]$, respectively, where the triples $(X_i Y_i Z_i)$, for $1 \leq i \leq N$, are generated by a discrete memoryless source according to some probability distribution P_{XYZ}, and P_{XYZ} is of the form $P_{XYZ} = P_R \cdot P_{X|R} \cdot P_{Y|R} \cdot P_{Z|R}$ for an unbiased binary random variable R (the bit broadcast by the satellite) and three independent binary symmetric channels $P_{X|R}$, $P_{Y|R}$ and $P_{Z|R}$ with bit error probabilities ϵ_A, ϵ_B and ϵ_E, respectively. The case of dependent channels can easily be transformed into a corresponding scenario of independent channels.

II. Secret-Key Rate

The secret key rate of P_{XYZ}, denoted $S(X;Y||Z)$, was defined in [2] as the maximal rate M/N at which Alice and Bob can generate secret shared random key bits $S_1, \ldots, S_M$ by exchanging messages over an insecure public channel accessible to Eve, such that the rate at which Eve obtains information about the key is arbitrarily small, i.e., such that

$$\lim_{N\to\infty} \frac{1}{N} I(S_1, \ldots, S_M; Z^N C^t) = 0,$$

where C^t is the collection of messages exchanged between Alice and Bob over the public channel. Note that the bits $S_1, \ldots, S_M$ can be used as the key in the one-time pad system for transmitting a message in perfect secrecy over the public channel.

The following upper and lower bounds on $S(X;Y||Z)$ were proved in [2]:

$$S(X;Y||Z) \leq \min[I(X;Y),\ I(X;Y|Z)]$$

and

$$S(X;Y||Z) \geq \max[I(Y;X) - I(Z;X),\ I(X;Y) - I(Z;Y)].$$

This lower bound states the intuitive result that the secret key rate is positive if either Eve (knowing Z) has less information about Y than Alice or, by symmetry, Eve has less information about X than Bob. Furthermore, it was demonstrated in [2] by an example that, quite surprisingly, $S(X;Y||Z)$ can be positive even if neither of these conditions is satisfied, i.e., if the right hand side of (II) vanishes or is negative. The purpose of this paper is to prove a lower bound on the secret key rate of binary random variables for the case where both Alice's and Bob's channels are noisier than Eve's channel, i.e., $\epsilon_A > \epsilon_E$ and $\epsilon_B > \epsilon_E$.

III. Results

Let

$$\epsilon = (1-\epsilon_A)\epsilon_B + \epsilon_A(1-\epsilon_B)$$

and

$$\beta = \frac{\epsilon^L}{\epsilon^L + (1-\epsilon)^L}.$$

We have

$$S(X;Y||Z) \ \geq\ R_c(1 - h(\beta) - I_E),$$

where

$$I_E = \frac{1}{\epsilon^L + (1-\epsilon)^L} \sum_{w=0}^{L} d_w \binom{L}{w} \left(1 - h\left(\frac{d_w}{d_w + d_{N-w}}\right)\right),$$

and

$$R_c = \frac{1}{L} \prod_{i=0}^{K-1} \left(\epsilon_i^{2^i} + (1-\epsilon_i)^{2^i}\right).$$

This quantity is strictly positive when $\epsilon_E > 0$, $\epsilon_A \neq 1/2$ and $\epsilon_B \neq 1/2$.

IV. Generalizations

Using techniques decribed in [3], the same bound can be proved for the much stronger definition of secret key rate which requires that the total amount of (rather than the rate at which Eve receives) information about S be negligible.

References

[1] C.H. Bennett, G. Brassard, C. Crépeau and U.M. Maurer, Generalized privacy amplification, these proceedings, (also submitted to *IEEE Transactions on Information Theory*).

[2] U.M. Maurer, Secret key agreement by public discussion from common information, *IEEE Transactions on Information Theory*, Vol. 39, No. 3, pp. 733-742, May 1993.

[3] U.M. Maurer, The strong secret key rate of discrete random triples, to appear in *Proc. Symp. on Communications, Coding and Cryptography*, R. Blahut et al. (eds.), Ascona, Switzerland, Feb. 10–13, 1994, Kluwer.

0 - 7803-2015-8/94/$4.00