Presented at 1994 IEEE International Symposium on Information Theory, Trondheim, Norway, June 27 - July 1, 1994.

On the Secret-Key Rate of Binary Random Variables

(Extended Abstract)

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

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

Consider two parties, Alice and Bob, who would like to communicate securely over an insecure channel to which an eavesdropper Eve has perfect access. Alice and Bob are assumed to be able to authenticate each others messages (e.g., by speaker identification), and the motivation of this paper is to demonstrate protocols that allow Alice and Bob to exchange messages in a provably-confidential manner. It is well-known that a conventional cryptosystem together with a shared secret key, or a public-key cryptosystem [3] when no secret key is shared, can be used for achieving this goal. However, no cryptosystem (conventional or public-key) has yet been proven to be computationally-secure.

The unarguably strongest definition of cipher security, perfect secrecy, was defined by Shannon to mean that plaintext and ciphertext are statistically independent, and hence even an eavesdropper with infinite computing power can obtain no information about the plaintext. The well-known one-time pad is an example of a perfect but generally impractical cipher. Shannon proved the pessimistic result that perfect secrecy can only be achieved if the entropy of the secret key is at least equal to the entropy of the plaintext.

This paper is concerned with achieving perfect secrecy between Alice and Bob, even when they share no secret key initially. For this purpose we allow Alice and Bob to make use of correlated random variables known to them, for instance a string of random bits broadcast by a satellite and received on the earth by Alice, Bob and Eve with individual noise patterns; hence our results do not violate Shannon's theorem. More precisely, 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.

Motivated by Wyner's and Csiszár and Körner's pioneering definition of, and work on, the secrecy capacity of a broadcast channel, the secret key rate of P_{XYZ}, denoted $S(X;Y||Z)$, was defined in [4] 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 [4]:

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

and

$$S(X;Y||Z) \ge \max[I(Y;X) - I(Z;X),\ I(X;Y) - I(Z;Y)]. \tag{1}$$

The lower bound (1) 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 [4] 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 (1) vanishes or is negative. The purpose of this paper is to prove lower bounds 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 $\epsilon_B > \epsilon_E$.

We propose the following protocol for exploiting such a situation. Alice and Bob group the received N bits in pairs. Alice sends the $\lfloor N/2 \rfloor$ parities of her pairs over the public channel. Bob announces, again over the public channel, for which of the pairs his parity agrees with that received from Alice, and Alice and Bob both keep the first bits of these selected pairs, thus forming a new, shorter string. In other words, for $i = 1, \ldots, \lfloor N/2 \rfloor$, Alice keeps X_{2i-1} and Bob keeps Y_{2i-1} if and only if $X_{2i-1} \oplus X_{2i} = Y_{2i-1} \oplus Y_{2i}$. The same step (of grouping a string in pairs, sending the parities of pairs and keeping the first bit of each selected pair) is iterated K times, thereby continuously increasing the reliability of the bits at the expense of shrinking the string. Let $L = 2^K$. The initial bit error probability on Bob's string compared to Alice's string is

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

One can show that the bit error probability of the strings held by Alice and Bob at the end of the protocol is

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

and hence Bob's information about each of Alice's bits is

$$I_B = 1 - h(\beta).$$

The compression rate R_c of both strings is given by

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

where ϵ_i is the bit error probability after the ith step, i.e.,

$$\epsilon_i = \epsilon_{i-1}^2 + (1-\epsilon_{i-1})^2$$

for $i = 1, \ldots, K$.

For each bit finally stored by Alice, Eve's information about this bit consists of the 2^K Z-bits corresponding to those X-bits that contributed to the parity checks sent over the public channel, together with these parity checks. Moreover, Eve's information vectors corresponding to different bits stored by Alice are statistically independent. It can be shown that Eve's mutual information I_E between one of Alice's bits and all the corresponding random variables stored by Eve is given by

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

where

$$\begin{aligned} d_w &= [(1-\epsilon_A)(1-\epsilon_B)(1-\epsilon_E) + \epsilon_A\epsilon_B\epsilon_E]^{L-w}[(1-\epsilon_A)(1-\epsilon_B)\epsilon_E + \epsilon_A\epsilon_B(1-\epsilon_E)]^w \\ &\quad +[(1-\epsilon_A)\epsilon_B(1-\epsilon_E) + \epsilon_A(1-\epsilon_B)\epsilon_E]^{L-w}[(1-\epsilon_A)\epsilon_B\epsilon_E + \epsilon_A(1-\epsilon_B)(1-\epsilon_E)]^w. \end{aligned}$$

According to (1), the secrecy capacity of such a scenario is lower bounded by

$$S(X;Y||Z) \;\geq\; R_c(I_B - I_E).$$

In the following analysis we assume that $\epsilon_A = \epsilon_B$. In order to be able to analyze a given satellite scenario independently of the signal power used in the satellite for broadcasting random bits, we consider a fixed ratio D for the channel capacities of Alice's and Eve's channels, e.g.

$$D = (1 - h(\epsilon_E))/(1 - h(\epsilon_A)),$$

where ϵ_A and ϵ_E can be chosen freely subject to this equation. Table 1 summarizes the optimal number K of steps, the optimal choice of ϵ_A and the achievable secret key rate $R_c(I_B - I_E)$ for various channel capacity ratios D. Note that $R_c(I_B - I_E)$ is a lower bound on $S(X;Y||Z)$. It is an open problem to determine the exact value of $S(X;Y||Z)$, but the authors conjecture that the described protocol and hence the

Ratio D	K	$\epsilon_A = \epsilon_B$	ϵ_E	$R_c(I_B - I_E)$
1	2	0.0799	0.0799	8.778E-3
10	6	0.4244	0.265	8.283E-5
100	9	0.4754	0.259	8.787E-7
1000	12	0.4921	0.256	8.891E-9
10000	15	0.4975	0.255	8.082E-11
100000	19	0.4992	0.252	8.674E-13

Table 1: The secret key rate of binary random variables for various capacity ratios D for Eve's and Alice's channel, assuming $\epsilon_A = \epsilon_B$.

values $R_c(I_B - I_E)$ are close to optimal. Note that $R_c(I_B - I_E)$ decreases approximately as $1/D^2$.

The purpose of this paper is to present the general scenario and definition of secret key rate as well as the techniques used to prove the claimed results. It should be pointed out that the described definition of secret key rate is not completely satisfactory because only the rate, but not the total amount of information about the key obtained by Eve, is bounded. If this paper should be selected for long presentation, we would also present the novel techniques such as those described in [1] for proving that the lower bound (1) also holds for a much stronger definition of secret key rate, which requires that the total amount (rather than the rate) of information that Eve obtains about the final string $S_1, \ldots, S_M$ be negligible, i.e.

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

and that $[S_1, \ldots, S_M]$ be arbitrarily close to uniformly distributed, i.e. $\lim_{N\to\infty}[M - H([S_1, \ldots, S_M])] = 0$. These techniques also allow us to derive results for a similarly strengthened definition of secrecy capacity introduced by Wyner [5] and generalized by Csiszár and Körner [2], and are hence of independent interest in information theory.

References

[1] C.H. Bennett, G. Brassard, C. Crépeau and U.M. Maurer, Privacy amplification against probabilistic information, submitted to IEEE Transactions on Information Theory.

[2] I. Csiszár and J. Körner, Broadcast channels with confidential messages, *IEEE Transactions on Information Theory*, Vol. 24, No. 3, pp. 339-348, 1978.

[3] W. Diffie and M.E. Hellman, New directions in cryptography, *IEEE Transactions on Information Theory*, Vol. 22, No. 6, pp. 644-654, 1976.

[4] 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.

[5] A.D. Wyner, The wire-tap channel, *Bell System Technical Journal*, Vol. 54, No. 8, pp. 1355-1387, 1975.