CHARACTERIZATION OF THE SECRECY OF A COMMON KEY CONSTRUCTED VIA DATA TRANSMISSION OVER THE TWO–WAY "AND" CHANNEL

Vladimir B. Balakirsky

Eindhoven University of Technology, Electrical Engineering Department
(on leave from the Data Security Association "Confident", St.-Petersburg, Russia)
P.O.Box 513, 5600 MB Eindhoven, the Netherlands

v.b.balakirsky@ele.tue.nl, htpp://www.mathematik.uni-bielefeld.de/~vbal/

We address cryptology aspects of data transmission over the two–way AND channel, also called the multiplying channel, and solve the combinatorial problem of computing the conditional entropy of a common key that can be constructed by communicating persons when the sequence at the output of the channel is known to an eavesdropper.

STATEMENT OF THE PROBLEM AND FORMULATION OF THE RESULT

Problem : *Given $n \geq 2$, construct*

(a) *a matrix of the probability distributions*

$$\mathbf{P} = \begin{bmatrix} P_{X_1} & P_{X_2|X_1,Z_1} & \ldots & P_{X_n|X^{n-1},Z^{n-1}} \\ P_{Y_1} & P_{Y_2|Y_1,Z_1} & \ldots & P_{Y_n|Y^{n-1},Z^{n-1}} \end{bmatrix}$$

where $X_1,\ldots,X_n$ and $Y_1,\ldots,Y_n$ are random variables taking values in $\{0,1\}$ and $Z_1,\ldots,Z_n$ are uniquely determined by the pairs $(X_1,Y_1),\ldots,$ (X_n,Y_n) in such a way that $Z_t = X_t \wedge Y_t,\ \ t=1,\ldots,n;$

(b) *two deterministic functions $K,L:\ \{0,1\}^n \times \{0,1\}^n \ \to\ \mathcal{K}$, where $\mathcal{K}$ is some finite set.*

The following requirements must be satisfied,

(R1) $P_{X^n,Y^n}(\mathbf{x},\mathbf{y}) > 0 \implies K(\mathbf{x},\mathbf{x}\wedge\mathbf{y}) = L(\mathbf{y},\mathbf{x}\wedge\mathbf{y}),$ *for all* $\mathbf{x},\mathbf{y} \in \{0,1\}^n$;

(R2) $H(K|Z^n) \longrightarrow \max$, *where*

$$H(K|Z^n) = -\sum_{key\in\mathcal{K}} \sum_{\mathbf{z}\in\{0,1\}^n} P_{K,Z^n}(key,\mathbf{z}) \log \frac{P_{K,Z^n}(key,\mathbf{z})}{P_{Z^n}(\mathbf{z})}$$

Table 1: The values of the function H_n/n for $n = 2^m$, where $m = 1, \ldots, 14$.

n	H_n/n	n	H_n/n
2	0.25	256	0.292274
4	0.261364	512	0.292583
8	0.273843	1024	0.292738
16	0.282995	2048	0.292816
32	0.287937	4096	0.292855
64	0.290415	8192	0.292874
128	0.291654	16384	0.292884
		∞	0.292893

and the probability distributions belong to the ensemble specified by the matrix $\mathbf{P}$.

Theorem : *Let H_n denote the maximal conditional entropy $H(K|Z^n)$ that can be achieved in the Problem. Then the function H_n can be recurrently found by*

$$H_n = (1-\xi_n)^2 H_{n-1} + 2\xi_n(1-\xi_n)(1+H_{n-2}) + \xi_n^2 H_{n-2}, \quad n = 2, 3, \ldots$$

where $H_0 = H_1 = 0$ and

$$\xi_n = \frac{1 - H_{n-1} + H_{n-2}}{2 - H_{n-1} + H_{n-2}}$$

The function H_n is bounded from below as

$$H_n \geq H_n^{(\xi)} = 2(1-\xi)\xi^{n-1} \cdot \left. \frac{\partial F_\xi^{(n)}(D, I_\xi)}{\partial D} \right|_{D=D_\xi} \tag{1}$$

where

$$\begin{aligned} F_\xi^{(n)}(D, I_\xi) &= \frac{1}{\xi} \sum_{\substack{n_1=0 \\ n_1+n \ odd}}^{n-1} \binom{(n-1+n_1)/2}{n_1} (1+D)^{(n-1-n_1)/2} I_\xi^{n_1} \\ &+ \sum_{\substack{n_1=0 \\ n_1+n \ even}}^{n-2} \binom{(n+n_1)/2-1}{n_1} (1+D)^{(n-n_1)/2} I_\xi^{n_1} \end{aligned}$$

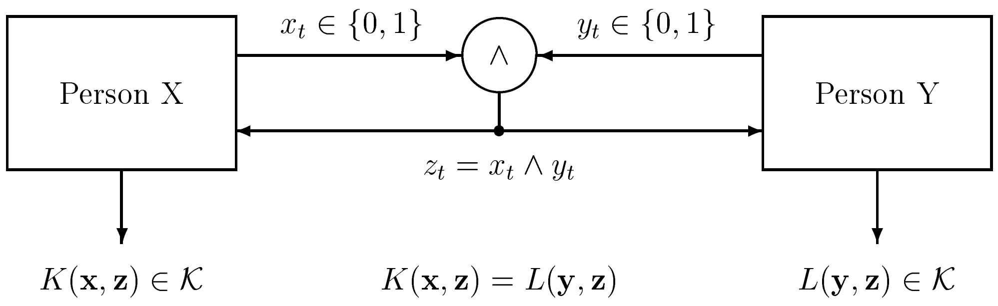

Figure 1: Constructing a common key via data transmission over the AND channel.

and

$$\xi = \sqrt{2} - 1, \quad D_\xi = \frac{2(1-\xi)}{\xi}, \quad I_\xi = \frac{(1-\xi)^2}{\xi} \tag{2}$$

Furthermore,

$$\lim_{n\to\infty} \frac{H_n}{n} = 1 - \frac{\sqrt{2}}{2} = 0.292893\ldots, \quad \lim_{n\to\infty} \xi_n = \sqrt{2} - 1 = 0.414214\ldots$$

Some values of the function H_n/n are given in Table 1.

CONSTRUCTING A COMMON KEY VIA DATA TRANSMISSION OVER THE TWO–WAY "AND" CHANNEL

The problem formulated above relates to data transmission over the two–way AND channel (see Figure 1) where the persons X and Y send bits x_t and y_t to each other and both of them receive $z_t = x_t \wedge y_t$ at time instants $t = 1,\ldots,n$. The bits x_t and y_t transmitted by the persons may depend on $x_1,\ldots,x_{t-1},z_1,\ldots,z_{t-1}$ and $y_1,\ldots,y_{t-1},z_1,\ldots,z_{t-1}$, respectively. Communication over such a channel when the persons want to exchange messages was introduced by Shannon [1] : in this case, x_t and y_t also depend on the messages of the persons X and Y. The problem of finding the region containing all pairs of the maximal possible numbers of messages and the corresponding transmission algorithms was considered in [2],[3],[4],[5], and other papers, but this problem is still unsolved. We address a different problem concerning the two–way channels that belongs to the direction known as constructing the common randomness (see [6],[7],[8], and other papers) when the goal of the persons is the creating a common random process for some further cryptology purposes. In our setup, the person X computes $K(\mathbf{x},\mathbf{z})$ and the person Y computes $L(\mathbf{y},\mathbf{z})$, where the functions K and L are fixed in advance.

If these values coincide for all pairs $(\mathbf{x}, \mathbf{y})$ that can be exchanged over a channel, then they serve as pointers to a table of keys which was also fixed in advance. An eavesdropper has only $\mathbf{z}$ and does not know $\mathbf{x}, \mathbf{y}$. His ambiguity about the pointer is measured by the conditional entropy $H(K|Z^n)$. For the notational convenience, we will associate the values of the functions K and L computed by the persons with the corresponding keys.

The actions of the persons can be represented as some realization of the algorithm consisting of *encoding* (the protocol for data transmission) and *decoding* (computing $K(\mathbf{x}, \mathbf{z})$ and $L(\mathbf{y}, \mathbf{z})$). We investigate the specific communication algorithm that will be referred to as *the H–type algorithm* since it is similar to the Hagelbarger's algorithm for the transmission of messages over the two–way AND channel ([1], p.375).

DESCRIPTION OF THE H–TYPE ALGORITHM

We assume that the persons independently assign one of two values to some auxiliary variable S_t at time instant t in such a way that these values coincide; thus, S_t can be interpreted as the current state of the communication system and we denote the possible states by α and β. The line above in the description of the algorithm denotes the binary inversion, i.e., $\overline{0} = 1$ and $\overline{1} = 0$.

Encoding : the persons X and Y set $S_1 = \alpha$ and follow the procedure below for $t = 1, \ldots, n$, where $\xi_n, \ldots, \xi_1 \in (0,1)$ are given.

(α) If $t < n$ and $S_t = \alpha$, then the persons X and Y choose x_t and y_t as independent random variables taking values 0 and 1 with the probabilities ξ_{n-t+1} and $1 - \xi_{n-t+1}$, respectively; both persons set $S_{t+1} = \alpha$ if $z_t = 1$ and $S_{t+1} = \beta$ if $z_t = 0$. If $t = n$ and $S_t = \alpha$, then the person X sets $x_t = 1$ and the person Y sets $y_t = 1$.

(β) If $S_t = \beta$, then the person X sets $x_t = \overline{x}_{t-1}$ and the person Y sets $y_t = \overline{y}_{t-1}$; both persons set $S_{t+1} = \alpha$.

Decoding : the persons X and Y set $t = 1$ and follow the procedure below while $t \le n$.

(1) If $z_t = 1$, then the person X sets $\hat{y}_t = 1$ and the person Y sets $\hat{x}_t = 1$; both persons increase t by 1.

(00) If $(z_t, z_{t+1}) = (0,0)$, then the person X sets $(\hat{y}_t, \hat{y}_{t+1}) = (\overline{x}_t, 0)$ and the person Y sets $(\hat{x}_t, \hat{x}_{t+1}) = (\overline{y}_t, 0)$; both persons increase t by 2.

(01) If $(z_t, z_{t+1}) = (0,1)$, then the person X sets $(\hat{y}_t, \hat{y}_{t+1}) = (0,1)$ and the person Y sets $(\hat{x}_t, \hat{x}_{t+1}) = (0,1)$; both persons increase t by 2.

The keys are defined as

$$K(\mathbf{x},\mathbf{z}) = [\ (x_1,\hat{y}_1), \ldots, (x_n,\hat{y}_n)\ ], \quad L(\mathbf{y},\mathbf{z}) = [\ (\hat{x}_1, y_1), \ldots, (\hat{x}_n, y_n)\ ].$$

The proof of the theorem includes the statement : *the maximal conditional entropy of a common key H_n is attained using the H–type algorithm.* The algorithm with $\xi_1 = \ldots = \xi_n = \xi$, where ξ is fixed, will be referred to as *the $H^{(\xi)}$–type algorithm* and we present its nonasymptotic analysis leading to (1).

NONASYMPTOTIC ANALYSIS OF THE $H^{(\xi)}$–TYPE ALGORITHM

We will associate data transmission over the two–way AND channel specified by the $H^{(\xi)}$–type algorithm with the parsing of binary sequences when the sequence is represented as a concatenation of codewords of the prefix code $\{00, 01, 1\}$. The code tree is given in Figure 2. A particular binary sequence uniquely determines the path which follows the encoder by returning to the root as soon as he reaches some terminal node. Let us label the nodes of the tree by α and β in such a way that the root and all terminal nodes have the label α. We also introduce two formal variables, D and I, assign the generating function to every edge of the tree as it is shown in Figure 2, and define the generating function of each path of the encoder as the product of the generating functions of all edges of that path. For example, the codewords 00, 01, 1 have the generating functions $D, 1, I$, and the generating function of the sequence 001011011, which is parsed as $(00, 1, 01, 1, 01, 1)$, is equal to DI^3.

For all $j = 0, \ldots, n-1$, let $T_\alpha^{(j)}(D,I)$ and $T_\beta^{(j)}(D,I)$ denote the sums of generating functions of all binary sequences of length j when the encoder reaches the nodes labeled by α and β at the j–th time instant, respectively. Let us also denote

$$\mathbf{T}^{(j)}(D,I) = \left(T_\alpha^{(j)}(D,I), T_\beta^{(j)}(D,I)\right), \quad j = 0, \ldots, n-1.$$

Then, as it is easy to see,

$$\begin{aligned} \mathbf{T}^{(0)}(D,I) &= (1,0) \\ \mathbf{T}^{(j)}(D,I) &= \mathbf{T}^{(j-1)}(D,I) \cdot \begin{bmatrix} I & 1 \\ 1+D & 0 \end{bmatrix}, \quad j = 1, \ldots, n-1. \end{aligned} \tag{3}$$

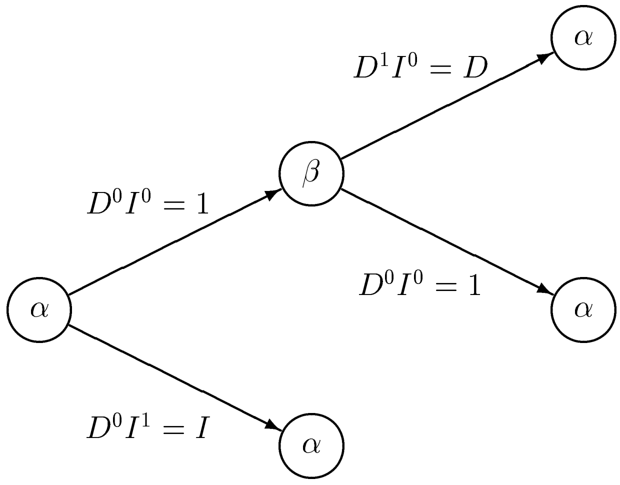

Figure 2: Tree of the prefix code $\{00, 01, 1\}$ with the nodes labeled by α, β and the generating functions assigned to the edges.

Lemma : *Let*

$$T^{(n)}(D,I) = \frac{1}{\xi} \cdot T_\alpha^{(n-1)}(D,I) + (1+D) \cdot T_\beta^{(n-1)}(D,I). \tag{4}$$

Then

$$H_n^{(\xi)} = 2(1-\xi)\xi^{n-1} \cdot \left. \frac{\partial T^{(n)}(D,I)}{\partial D} \right|_{\substack{D=D_\xi \\ I=I_\xi}} \tag{5}$$

where D_ξ and I_ξ are defined in (2).

Proof : Let $\mathcal{Z}_\alpha^n(d,i)$ and $\mathcal{Z}_\beta^n(d,i)$ denote the set of binary sequences of length n which lead the encoder of the prefix code to the nodes labeled by α and β at time instant n and have the property that the parsing procedure, being applied to any of these sequences, generates d codewords 00, i codewords 1, and $n_{01}(\mathbf{z})$ codewords 01, where

$$n_{01}(\mathbf{z}) = \begin{cases} (n-i)/2 - d, & \text{if } \mathbf{z} \in \mathcal{Z}_\alpha^n(d,i) \\ (n-1-i)/2 - d, & \text{if } \mathbf{z} \in \mathcal{Z}_\beta^n(d,i). \end{cases} \tag{6}$$

On the other hand, as it follows from the description of the encoding of the $H^{(\xi)}$–type algorithm, any sequence belonging to the set $\mathcal{Z}_\alpha^n(d,i) \cup \mathcal{Z}_\beta^n(d,i)$ appears at the output of the AND channel if and only if there are $d+i+n_{01}(\mathbf{z})$ time instants when the persons decide that α is the current state of the communication system and they generate d pairs $(x_t, y_t) \in \{(0,1),(1,0)\}$, i pairs $(x_t, y_t) = (1,1)$, and

$n_{01}(\mathbf{z})$ pairs $(x_t, y_t) = (0,0)$ at these time instants. Therefore

$$P_{Z^n}(\mathbf{z}) = (2\xi(1-\xi))^d \cdot \left((1-\xi)^2\right)^i \cdot \left(\xi^2\right)^{n_{01}(\mathbf{z})}, \quad \text{for all } \mathbf{z} \in \mathcal{Z}_\alpha^n(d,i) \bigcup \mathcal{Z}_\beta^n(d,i). \tag{7}$$

Furthermore, since (1) any of these sequences leads to one of 2^d keys constructed by the persons X and Y; (2) the probability distribution on the set of keys is uniform,

$$H(K|\mathbf{z}) = d, \quad \text{for all } \mathbf{z} \in \mathcal{Z}_\alpha^n(d,i) \bigcup \mathcal{Z}_\beta^n(d,i). \tag{8}$$

Equations (6)–(8) and notations (2) imply

$$H_n^{(\xi)} = \xi^n \sum_{d,i} \left(|\mathcal{Z}_\alpha^n(d,i)| + \frac{1}{\xi} \cdot \left|\mathcal{Z}_\beta^n(d,i)\right| \right) D_\xi^d I_\xi^i \cdot d\,. \tag{9}$$

The cardinalities of the sets $\mathcal{Z}_\alpha^n(d,i)$ and $\mathcal{Z}_\beta^n(d,i)$ can be expressed using the coefficients of the generating functions $T_\alpha^{(n-1)}(D,I)$ and $T_\beta^{(n-1)}(D,I)$: if these functions are represented as finite sums

$$T_\alpha^{(n-1)}(D,I) = \sum_{d,i} t_\alpha^{(n-1)}(d,i) D^d I^i, \quad T_\beta^{(n-1)}(D,I) = \sum_{d,i} t_\beta^{(n-1)}(d,i) D^d I^i$$

then

$$|\mathcal{Z}_\alpha^n(d,i)| = t_\beta^{(n-1)}(d,i) + t_\beta^{(n-1)}(d-1,i), \quad |\mathcal{Z}_\beta^n(d,i)| = t_\alpha^{(n-1)}(d,i) \tag{10}$$

where the first equation follows from the fact that the last codeword after the parsing of any sequence $\mathbf{z} \in \mathcal{Z}_\alpha^n(d,i)$ is either 00 or 01, and the second equation follows from the fact that the last bit of any sequence $\mathbf{z} \in \mathcal{Z}_\beta^n(d,i)$ is 0 and that the last codeword constructed by the parsing procedure ends at time instant $n-1$. By (9) and (10),

$$H_n^{(\xi)} = \xi^n \sum_d \sum_i \left(t_\beta^{(n-1)}(d,i) + t_\beta^{(n-1)}(d-1,i) + \frac{1}{\xi} \cdot t_\alpha^{(n-1)}(d,i) \right) D_\xi^d I_\xi^i \cdot d\,. \tag{11}$$

Since (4) defines the generating function

$$T^{(n)}(D,I) = \sum_{d,i} t^{(n)}(d,i) D^d I^i$$

where $t^{(n)}(d,i) = t_\alpha^{(n-1)}(d,i)/\xi + t_\beta^{(n-1)}(d,i) + t_\beta^{(n-1)}(d-1,i)$, equation (11) can be presented as (5). Q.E.D.

Using (3) and induction on $j = 0, \ldots, n-1$ we prove that

$$T_\alpha^{(n-1)}(D,I) = \sum_{\substack{n_1=0 \\ n_1+n\ odd}}^{n-1} \binom{(n-1+n_1)/2}{n_1} (1+D)^{(n-1-n_1)/2} I^{n_1}$$

$$T_\beta^{(n-1)}(D,I) = \sum_{\substack{n_1=0 \\ n_1+n\ even}}^{n-2} \binom{(n+n_1)/2-1}{n_1} (1+D)^{(n-n_1)/2-1} I^{n_1}$$

where the second sum is understood as 0 when $n = 1$, and using (4), (5) obtain (1).

REFERENCES

[1] C.E. Shannon, "Two–Way Communication Channels", in *Claude Elwood Shannon : Collected Papers.* N.J.A. Sloane and A.D. Wyner, Eds. IEEE Press, pp. 351–384, 1993.
The paper was published in the Proc. 4–th Berkley Symp. Math. Stat. and Prob., pp.611–644, 1961.

[2] G. Dueck, "The Capacity Region of the Two–Way Channel Can Exceed the Inner Bound", Inform. Control, 40(3), pp.258–266, 1979.

[3] J.P.M. Schalkwijk, "The Binary Multiplying Channel – A Coding Scheme That Operates Beyond the Shannon Inner Bound", IEEE Trans. Inform. Theory, IT–28(1), pp.107–110, 1982.

[4] J.P.M. Schalkwijk, "On an Extension of an Achievable Rate Region for the Binary Multiplying Channel", IEEE Trans. Inform. Theory, IT–29(3), pp.445–448, 1983.

[5] Z. Zhang, T. Berger, and J.P.M. Schalkwijk, "New Outer Bounds to Capacity Regions of Two–Way Channels", IEEE Trans. Inform. Theory, IT–32(3), pp.383–386, 1986.

[6] R. Ahlswede and B. Verboven, "On Identification via Multiway Channels with Feedback", IEEE Trans. Inform. Theory, IT–37(5), pp.1519–1526, 1991.

[7] U. Maurer, "Secret Key Agreement by Public Discussion from Common Information", IEEE Trans. Inform. Theory, IT–39(3), pp.733–742, 1993.

[8] R. Ahlswede and I. Csiszár, "Common Randomness in Information Theory and Cryptography – Part I : Secret Sharing", IEEE Trans. Inform. Theory, IT–39(5), pp.1121–1131, 1993.