Теорія Ймовір. та Матем. Статист.
Вип. 78, 2008

Theor. Probability and Math. Statist.
No. 78, 2009, Pages 167–174
S 0094-9000(09)00770-4
Article electronically published on August 4, 2009

AN ESTIMATE FOR THE MEAN ERROR PROBABILITY OF A BAYESIAN CRITERION FOR TESTING HYPOTHESES IN THE PROBLEM OF CRYPTANALYSIS OF A COMBINED GAMMA GENERATOR WITH NONUNIFORM NOISE

UDC 519.21

A. M. OLEKSIĬCHUK AND R. V. PROSKUROVS'KIĬ

Abstract. A probability model for a combined gamma generator with nonuniform noise in a resynchronization mode is studied. We consider the problem of testing hypotheses about the distribution of a random binary vector $X^{(0)}$ (the state of a combined gamma generator) by using a sampled binary sequence whose signs depend on $X^{(0)}$ in a specified way and on certain other random parameters. We obtain a nonasymptotic upper bound for the mean error probability of a Bayesian criterion for testing the hypotheses mentioned above.

1. The setting of the problem and main results

Let n, L, and t be natural numbers, Δ be a nonempty subset of the set

$$\{0,1,\dots,L-1\}^n,$$

$a=(a_1,\dots,a_n)\in\Delta$ be a fixed vector, $f\colon V_n \stackrel{\text{def}}{=} \{0,1\}^n\to\{0,1\}$ be a Boolean function such that

$$|\{x\in V_n\colon f(x)=1\}|=2^{n-1}, \tag{1}$$

and let $g^{(1)},\dots,g^{(t)}$ be an arbitrary sequence of n-dimensional Boolean vectors. Further, let $X^{(0)}=\big(X_j^{(0)}(i)\colon j\in\{1,\dots,n\},i\in\{0,\dots,L-1\big\})$,

$$C^{(l)}=\left(C_j^{(l)}(i)\colon j\in\{1,\dots,n\},i\in\{0,\dots,L-1\}\right),$$

and let $\delta^{(l)}=\big(\delta_1^{(l)},\dots,\delta_n^{(l)}\big)$, $l\in\{1,\dots,t\}$, be jointly independent random vectors such that

(a) the vector $X^{(0)}$ has the uniform probability distribution in the set V_{nL},
(b) the vector $C^{(l)}$ has the uniform probability distribution in the set

$$U_{g^{(l)}},\qquad l\in\{1,\dots,t\},$$

where

$$U_s \stackrel{\text{def}}{=} \{(y_j(i)\colon j\in\{1,\dots,n\},i\in\{0,\dots,L-1\})\in V_{nL}\mid (y_1(a_1),\dots,y_n(a_n))=s\} \tag{2}$$

for all $s\in V_n$,

2000 *Mathematics Subject Classification.* Primary 94A60; Secondary 94B70.
Key words and phrases. Statistical methods of cryptanalysis, test of hypotheses.

(c) the vectors $\delta^{(l)}$, $l \in \{1, \dots, t\}$, assume their values in the set Δ and have the same probability distribution

$$\mathsf{P}\left\{\delta^{(l)} = u\right\} = p(u), \qquad u \in \Delta. \tag{3}$$

Consider a sequence of random variables

$$\gamma^{(l)} = f\left(X_1^{(l)}\big(\delta_1^{(l)}\big), \dots, X_n^{(l)}\big(\delta_n^{(l)}\big)\right), \qquad l \in \{1, \dots, t\}, \tag{4}$$

where $X_j^{(l)}(i) \stackrel{\text{def}}{=} X_j^{(0)}(i) \oplus C_j^{(l)}(i)$, $j \in \{1, \dots, n\}$, $i \in \{0, \dots, L-1\}$, $l \in \{1, \dots, t\}$. Here the symbol $\oplus$ stands for the addition operation in the field of two elements. The problem is to reconstruct the vector

$$X^{(0)}(a) = \left(X_1^{(0)}(a_1), \dots, X_n^{(0)}(a_n)\right) \tag{5}$$

from a known sample of the random sequence (4).

The problems of this kind appear when designing and studying the effectiveness of correlation methods in the cryptanalysis of combined gamma generators with nonuniform noise [1, 2]. Such a generator is a finite automata transforming an input sequence

$$\{(x(i), \varepsilon(i))\colon i = 0, 1, \dots\},$$

where

$$x(i) = (x_1(i), \dots, x_n(i)) \in V_n, \qquad \varepsilon(i) = (\varepsilon_1(i), \dots, \varepsilon_n(i)) \in \mathbf{N}_0^n, \qquad i = 0, 1, \dots,$$

to the output sequence $\{f(x_1(\delta_1(i)), \dots, x_n(\delta_n(i)))\colon i = 0, 1, \dots\}$, where

$$\delta_j(0) = 0, \qquad \delta_j(i) = \sum_{k=0}^{i-1} \varepsilon_j(k), \qquad i = 1, 2, \dots, \ j \in \{1, \dots, n\}.$$

Relations (4) describe the rule of the transformation of t input binary states of a combined gamma generator with nonuniform noise to t output binary signs in the so-called resynchronization mode (more details concerning this topic can be found, for example, in [2, 3]).

The problem of reconstruction of the vector (5) can be stated as follows: it is necessary to construct a statistical method for testing the simple 2^n hypotheses

$$H_s\colon \qquad X^{(0)}(a) = s, \quad s \in V_n, \tag{6}$$

by using a sampled random sequence (4). The a priori probabilities are the same for all hypotheses (6) and equal 2^{-n} by condition (a). The optimal criterion for testing those hypotheses is the Bayesian criterion [4]. In the case under consideration, this criterion is to use the sample $\gamma_1, \dots, \gamma_t$ of the form (4) and to accept the hypothesis H_{s^*} for which the vector $s^* = s^*(\gamma_1, \dots, \gamma_t) \in V_n$ is a point of maximum of the function

$$\mathsf{P}_s(\gamma_1, \dots, \gamma_t) \stackrel{\text{def}}{=} \mathsf{P}\left(\big(\gamma^{(1)}, \dots, \gamma^{(t)}\big) = (\gamma_1, \dots, \gamma_t) \mid X^{(0)}(a) = s\right), \qquad s \in V_n.$$

We prove the theorem containing the explicit form of the probability

$$\mathsf{P}_s\big(\gamma^{(l)} = \gamma\big) = \mathsf{P}\big(\gamma^{(l)} = \gamma \mid X^{(0)}(a) = s\big), \qquad s \in V_n, \ l \in \{1, \dots, t\}.$$

Put

$$\rho_{f,a}(x) = 2^{-n} \sum_{y \in V_n \setminus \{0\}} (-1)^{xy} W_f(y) \pi(a; y), \qquad x \in V_n, \tag{7}$$

where $W_f(y) = \sum_{x \in V_n} (-1)^{f(x) \oplus xy}$ is the Walsh–Hadamard transform of the Boolean function f (see [5]). Here and in what follows the symbol xy stands for the Boolean scalar product $x_1 y_1 \oplus \cdots \oplus x_n y_n$ of two binary vectors $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$,

$$\pi(a; y) = \sum_{u \in \Delta(a; y)} p(u), \qquad y \in V_n \setminus \{0\}, \tag{8}$$

$$\Delta(a; y) = \big\{ u = (u_1, \ldots, u_n) \in \Delta \;\big|\; \text{for all } j \in \{1, \ldots, n\} \colon (y_j = 1) \Rightarrow (u_j = a_j) \big\}.$$

Theorem 1. *The members of the random sequence* (4) *are jointly conditionally independent given an arbitrary hypothesis H_s, $s \in V_n$. Moreover,*

$$\mathsf{P}_s\big(\gamma^{(l)} = \gamma\big) = \frac{1}{2}\left(1 + (-1)^{\gamma} \rho_{f,a}\big(s \oplus g^{(l)}(a)\big)\right), \qquad \gamma \in \{0, 1\}, \tag{9}$$

for all $s \in V_n$ and $l \in \{1, \ldots, t\}$.

Theorem 1 means that the optimal statistical procedure for reconstructing the vector (5) from the sample $\gamma_1, \ldots, \gamma_t$ of the random sequence (4) is to evaluate the sum $\sigma_s(\gamma_1, \ldots, \gamma_t) = \sum_{l=1}^{t} \ln \mathsf{P}_s\big(\gamma^{(l)} = \gamma_l\big)$ for every $s \in V_n$ by using relations (7)–(9) and to construct the estimator $X^{(0)}(a) = s^*$, where $s^* = s^*(\gamma_1, \ldots, \gamma_t)$ is an arbitrary element of the set V_n such that

$$\sigma_{s^*}(\gamma_1, \ldots, \gamma_t) = \max_{s \in V_n} \{\sigma_s(\gamma_1, \ldots, \gamma_t)\}. \tag{10}$$

Let $\lambda_t = 2^{-n} \sum_{s \in V_n} \mathsf{P}_s\big\{s^*(\gamma^{(1)}, \ldots, \gamma^{(t)}) \neq s\big\}$ be the mean probability of the erroneous reconstruction of the vector (5) for the statistical procedure described above. We also put

$$\rho(f, a) = \max_{x \in V_n} |\rho_{f,a}(x)|, \qquad \mu(f, a) = \min_{\substack{x, y \in V_n, \\ x \neq y}} |\rho_{f,a}(x) - \rho_{f,a}(y)|,$$

where the numbers $\rho_{f,a}(x)$, $x \in V_n$, are defined by (7).

Theorem 2. *Let*

$$\rho(f, a) < 1. \tag{11}$$

Then

$$\lambda_t \leq (2^n - 1) \exp\left\{ -\frac{t}{8} \mu(f, a)^2 \left(1 - \rho(f, a)^2\right)^2 \right\}. \tag{12}$$

In particular, if $\mu(f, a) > 0$, then $\lim_{t \to \infty} \lambda_t = 0$ provided condition (11) *holds.*

2. Proof of Theorem 1

Let $X^{(l)} = \big(X_j^{(l)}(i) \colon j \in \{1, \ldots, n\}, i \in \{0, \ldots, L-1\}\big)$, $l \in \{1, \ldots, t\}$. Note that the random vectors $X^{(l)}$, $l \in \{1, \ldots, t\}$, are jointly conditionally independent given the hypothesis H_s by conditions (a) and (b), since the random vectors $X^{(0)}$, $C^{(l)}$, $l \in \{1, \ldots, t\}$, are independent. This implies that the random variables $\gamma^{(l)}$, $l \in \{1, \ldots, t\}$, are independent by equality (4), since the vectors $\delta^{(l)}$, $l \in \{1, \ldots, t\}$, are independent.

Now we prove equality (9). Consider the independent random vectors

$$X = (X_j(i) \colon j \in \{1, \ldots, n\}, i \in \{0, \ldots, L-1\})$$

and $\delta = (\delta_1, \ldots, \delta_n)$ such that X is uniformly distributed in the set V_{nL}, while δ is distributed by the law (3). Put

$$P_{f,a}(s) \stackrel{\text{def}}{=} \mathsf{P}\big(f(X_1(\delta_1), \ldots, X_n(\delta_n)) = 0 \mid X_1(a_1) = s_1, \ldots, X_n(a_n) = s_n\big) \tag{13}$$

for all $s = (s_1, \ldots, s_n) \in V_n$.

It follows from (4) that

$$\begin{aligned}\mathsf{P}_s\big(\gamma^{(l)}=0\big)&=\mathsf{P}\big(\gamma^{(l)}=0\bigm|X^{(0)}(a)=s\big)\\&=\mathsf{P}\Big(f\big(X_1^{(l)}\big(\delta_1^{(l)}\big),\dots,X_n^{(l)}\big(\delta_n^{(l)}\big)\big)=0\bigm|\big(X_1^{(l)}(a_1),\dots,X_n^{(l)}(a_n)\big)=s\oplus g^{(l)}\Big)\\&=P_{f,a}\big(s\oplus g^{(l)}\big),\qquad s\in V_n,\end{aligned}$$

by the definitions of the random vectors X, δ, $X^{(l)}$, and $\delta^{(l)}$, $l\in\{1,\dots,t\}$. Thus (9) follows from

$$P_{f,a}(s)=\frac{1}{2}(1+\rho_{f,a}(s)),\qquad s\in V_n. \tag{14}$$

To prove equality (14) we need some further notation. For arbitrary

$$u=(u_1,\dots,u_n)\in\mathbf{N}_0^n,\qquad v=(v_1,\dots,v_n)\in\mathbf{N}_0^n,\qquad y=(y_1,\dots,y_n)\in V_n,$$

put

$$I(u,v)=\{j\in\{1,\dots,n\}\mid u_j=v_j\},\qquad \operatorname{supp}(y)=\{j\in\{1,\dots,n\}\colon y_j=1\}.$$

Let $A=\{i_1,\dots,i_s\}\subseteq\{1,2,\dots,n\}$, where $1\le i_1<\dots<i_s\le n$. For an arbitrary vector $x=(x_1,\dots,x_n)$, denote the vector $(x_{i_1},\dots,x_{i_s})$ by x_A. The vector x will be written in the form $x=(x_A,x_{\bar A})$, where $\bar A=\{1,2,\dots,n\}\setminus A$. The similar notation $X_A(u_A)$ is used for the random vector $(X_{i_1}(u_{i_1}),\dots,X_{i_s}(u_{i_s}))$, where $u=(u_1,\dots,u_n)\in\Delta$ and $A=\{i_1,\dots,i_s\}\subseteq\{1,2,\dots,n\}$. For the case of $A=\{1,2,\dots,n\}$, we omit the subscript A in the notation $X_A(u_A)$. For arbitrary $g\colon V_n\to\{0,1\}$ and $\alpha=(\alpha_1,\dots,\alpha_s)\in V_s$, denote by g_A^α the function obtained from g by fixing its arguments with indices belonging to the set A at the values of the corresponding coordinates of the vector α. Note that g_A^α is a function of arguments belonging to the family $x_{\bar A}$ if g is a Boolean function of the arguments $x_1,\dots,x_n$.

We transform equality (13) by using (1), the full probability formula, and the definitions of the random vectors X and δ:

$$\begin{aligned}P_{f,a}(s)&=2^n\,\mathsf{P}\big\{X_1(a_1)=s_1,\dots,X_n(a_n)=s_n,f(X_1(\delta_1),\dots,X_n(\delta_n))=0\big\}\\&=2^n\sum_{A\subseteq1,\dots,n}\sum_{\substack{u\in\Delta\colon\\I(a,u)=A}}p(u)\,\mathsf{P}\big\{X(a)=s,f(X_A(a_A),X_{\bar A}(u_{\bar A}))=0\big\}\\&=2^n\sum_{A\subseteq1,\dots,n}\sum_{\substack{u\in\Delta\colon\\I(a,u)=A}}p(u)\,\mathsf{P}\{X(a)=s\}\,\mathsf{P}\big\{f(s_A,X_{\bar A}(u_{\bar A}))=0\big\}\qquad(15)\\&=\sum_{A\subseteq1,\dots,n}\mathsf{P}\big\{f_A^{s_A}(X_{\bar A})=0\big\}\sum_{\substack{u\in\Delta\colon\\I(a,u)=A}}p(u).\end{aligned}$$

Consider the term of expression (15) corresponding to the set $A=\varnothing$, namely

$$\frac{1}{2}\sum_{\substack{u\in\Delta\colon\\I(a,u)=\varnothing}}p(u)=\frac{1}{2}\left(1-\sum_{\substack{A\subseteq1,\dots,n\colon\\A\ne\varnothing}}\sum_{\substack{u\in\Delta\colon\\I(a,u)=A}}p(u)\right).$$

After some simple algebra we obtain

$$P_{f,a}(s)=\frac{1}{2}\left(1+\sum_{\substack{A\subseteq1,\dots,n\colon\\A\ne\varnothing}}\big(2\,\mathsf{P}\{f_A^{s_A}(X_{\bar A})=0\}-1\big)\sum_{\substack{u\in\Delta\colon\\I(a,u)=A}}p(u)\right),\qquad s\in V_n. \tag{16}$$

Note that

$$\sum_{\substack{u\in\Delta:\\ I(a,u)=A}} p(u) = \mathsf{P}\left(\bigcap_{j\in\bar{A}}\{\delta_A = a_A, \delta_j \neq a_j\}\right)$$

according to equality (3), whence we obtain by an application of the inclusion-exclusion formula that

$$\begin{aligned}\sum_{\substack{u\in\Delta:\\ I(a,u)=A}} p(u) &= \sum_{m=0}^{n-|A|}(-1)^m \sum_{\substack{C\subseteq\bar{A}:\\ |C|=m}} \mathsf{P}\{\delta_A = a_A, \delta_C = a_C\}\\ &= \sum_{B\supseteq A}(-1)^{|B|-|A|}\,\mathsf{P}\{\delta_B = a_B\}.\end{aligned} \tag{17}$$

Further, we use the Walsh–Hadamard transform and Lemma 2.40 of [5]:

$$\begin{aligned}2\,\mathsf{P}\{f_A^{s_A}(X_{\bar{A}}) = 0\} - 1 &= 2^{-(n-|A|)}\sum_{x_{\bar{A}}\in V_{|\bar{A}|}}(-1)^{f(s_A, x_{\bar{A}})}\\ &= 2^{-n}\sum_{\substack{y\in V_n:\\ \operatorname{supp}(y)\subseteq A}} W_f(y)(-1)^{sy}\end{aligned} \tag{18}$$

for all $A\subseteq\{1,\dots,n\}$, $A\neq\varnothing$, and all $s\in V_n$. Substituting expressions (17) and (18) to the formula (16) we get

$$\begin{aligned}&P_{f,a}(s)\\ &= \frac{1}{2}\left(1 + 2^{-n}\sum_{B\neq\varnothing}\mathsf{P}\{\delta_B = a_B\}\sum_{\varnothing\neq A\subseteq B}(-1)^{|B|-|A|}\sum_{\substack{y\in V_n,\\ \operatorname{supp}(y)\subseteq A}} W_f(y)(-1)^{sy}\right)\\ &= \frac{1}{2}\left(1 + 2^{-n}\sum_{y\in V_n\setminus\{0\}} W_f(y)(-1)^{sy}\sum_{B\neq\varnothing}\mathsf{P}\{\delta_B = a_B\}\sum_{\operatorname{supp}(y)\subseteq A\subseteq B}(-1)^{|B|-|A|}\right)\end{aligned} \tag{19}$$

in view of the equality $W_f(0) = 0$, which follows from (1).

Since

$$\sum_{\operatorname{supp}(y)\subseteq A\subseteq B}(-1)^{|B|-|A|} = 0$$

with the only exceptional case being where $B = \operatorname{supp}(y)$, equality (14) follows from (7), (8), and (19).

Thus equality (14) holds, and the proof of the theorem is complete.

3. Proof of Theorem 2

We need some auxiliary results.

Lemma 1 ([6]). *Let $\xi_1,\dots,\xi_t$ be independent random variables such that*

$$\alpha_l \le \xi_l \le \beta_l, \qquad \alpha_l, \beta_l \in \mathbf{R},\ l\in\{1,\dots,t\}.$$

Then

$$\mathsf{P}\left(\sum_{l=1}^t \xi_l - \sum_{l=1}^t \mathsf{E}\,\xi_l \ge tx\right) \le \exp\left\{-\frac{2t^2x^2}{\sum_{l=1}^t(\beta_l-\alpha_l)^2}\right\}$$

for all $x > 0$.

The following result is a particular case of an inequality between the information divergence and the distance in variance for probability distributions on a finite set [7, Problem 17, Section 3, Chapter 1].

Lemma 2. *For all $p, q \in (0,1)$,*

$$D(p \parallel q) \stackrel{\text{def}}{=} p \ln \frac{p}{q} + (1-p) \ln \frac{1-p}{1-q} \geq 2(p-q)^2. \tag{20}$$

Lemma 3. *For all $x, y \in (-1,1)$,*

$$\left| \ln\left(\frac{1+x}{1-x}\right) - \ln\left(\frac{1+y}{1-y}\right) \right| \leq \frac{2|x-y|}{1-(\max\{|x|,|y|\})^2}. \tag{21}$$

Proof. If $x = y$, then inequality (21) is obvious.

Let $x \neq y$. Since

$$\ln(1+z) = \sum_{n=1}^{\infty} (-1)^{n-1} z^n / n, \qquad z \in (-1,1),$$

we have

$$\begin{aligned} \ln\left(\frac{1+x}{1-x}\right) - \ln\left(\frac{1+y}{1-y}\right) &= \sum_{k=0}^{\infty} \frac{2}{2k+1} \left(x^{2k+1} - y^{2k+1}\right) \\ &= 2(x-y) \sum_{k=0}^{\infty} \left(\frac{x^{2k+1} - y^{2k+1}}{x-y}\right) \frac{1}{2k+1}. \end{aligned} \tag{22}$$

Note that

$$\begin{aligned} \left|x^{2k+1} - y^{2k+1}\right| &= |x-y| \left|x^{2k} + x^{2k-1}y + \cdots + y^{2k-1}x + y^{2k}\right| \\ &\leq |x-y|(2k+1)(\max\{|x|,|y|\})^{2k}, \qquad k = 0, 1, \ldots . \end{aligned}$$

This together with (22) implies that

$$\left| \ln\left(\frac{1+x}{1-x}\right) - \ln\left(\frac{1+y}{1-y}\right) \right| \leq 2|x-y| \sum_{k=0}^{\infty} (\max\{|x|,|y|\})^{2k} = \frac{2|x-y|}{1-(\max\{|x|,|y|\})^2},$$

and this is what was to be proved. □

Now we turn to the proof of Theorem 2. The following inequality,

$$\begin{aligned} \lambda_t &= 2^{-n} \sum_{s \in V_n} \mathsf{P}_s \left\{ s^*\left(\gamma^{(1)}, \ldots, \gamma^{(t)}\right) \neq s \right\} \\ &\leq (2^n - 1) \max_{\substack{(s,s') \in V_n \times V_n, \\ s \neq s'}} \mathsf{P}_s \left\{ \sigma_s\left(\gamma^{(1)}, \ldots, \gamma^{(t)}\right) < \sigma_{s'}\left(\gamma^{(1)}, \ldots, \gamma^{(t)}\right) \right\}, \end{aligned}$$

follows from equality (10) and the condition

$$\left\{ s^*\left(\gamma^{(1)}, \ldots, \gamma^{(t)}\right) \neq s \right\} \subseteq \bigcup_{s' \in V_n \setminus \{s\}} \left\{ \sigma_s\left(\gamma^{(1)}, \ldots, \gamma^{(t)}\right) < \sigma_{s'}\left(\gamma^{(1)}, \ldots, \gamma^{(t)}\right) \right\}, \qquad s \in V_n.$$

Therefore if condition (11) holds, then the theorem follows from the inequality

$$\mathsf{P} \left\{ \sigma_s\left(\gamma^{(1)}, \ldots, \gamma^{(t)}\right) < \sigma_{s'}\left(\gamma^{(1)}, \ldots, \gamma^{(t)}\right) \right\} \leq \exp\left\{ -\frac{t}{8} \mu(f,a)^2 \left(1 - \rho(f,a)^2\right)^2 \right\}, \tag{23}$$

where $s, s' \in V_n$, $s \neq s'$.

Fix a pair of different vectors $s, s' \in V_n$ and consider the following random variables:

$$\xi_{s,s'}^{(l)} \stackrel{\text{def}}{=} \ln\left(\frac{1+(-1)^{\gamma^{(l)}}\rho_{f,a}\bigl(s'\oplus g^{(l)}(a)\bigr)}{1+(-1)^{\gamma^{(l)}}\rho_{f,a}\bigl(s\oplus g^{(l)}(a)\bigr)}\right), \qquad l\in\{1,\dots,t\}. \tag{24}$$

The random variables in (24) are well defined in view of (11).

According to Theorem 1, the random variables (24) are jointly conditionally independent given a hypothesis H_s. Moreover

$$\mathsf{P}_s\left\{\sigma_s\bigl(\gamma^{(1)},\dots,\gamma^{(t)}\bigr)<\sigma_{s'}\bigl(\gamma^{(1)},\dots,\gamma^{(t)}\bigr)\right\}=\mathsf{P}_s\left\{\sum_{l=1}^{t}\xi_{s,s'}^{(l)}>0\right\}.$$

Using equality (9) we prove that the mathematical expectation of the random variable $\xi_{s,s'}^{(l)}$ given the hypothesis H_s is equal to

$$\begin{aligned}\mathsf{E}_s\,\xi_{s,s'}^{(l)} &= \frac{1}{2}\Bigl(1+\rho_{f,a}\bigl(s\oplus g^{(l)}(a)\bigr)\Bigr)\ln\left(\frac{1+\rho_{f,a}\bigl(s'\oplus g^{(l)}(a)\bigr)}{1+\rho_{f,a}\bigl(s\oplus g^{(l)}(a)\bigr)}\right)\\ &\quad+\frac{1}{2}\Bigl(1-\rho_{f,a}\bigl(s\oplus g^{(l)}(a)\bigr)\Bigr)\ln\left(\frac{1-\rho_{f,a}\bigl(s'\oplus g^{(l)}(a)\bigr)}{1-\rho_{f,a}\bigl(s\oplus g^{(l)}(a)\bigr)}\right)\\ &= -D\bigl(p_s^{(l)}\parallel p_{s'}^{(l)}\bigr)\end{aligned}$$

where $p_s^{(l)} \stackrel{\text{def}}{=} \mathsf{P}_s\bigl(\gamma^{(l)}=0\bigr)$ and $p_{s'}^{(l)} \stackrel{\text{def}}{=} \mathsf{P}_{s'}\bigl(\gamma^{(l)}=0\bigr)$, $l\in\{1,\dots,t\}$. Thus Lemma 1 implies that

$$\mathsf{P}_s\left\{\sigma_s\bigl(\gamma^{(1)},\dots,\gamma^{(t)}\bigr)<\sigma_{s'}\bigl(\gamma^{(1)},\dots,\gamma^{(t)}\bigr)\right\}\le\exp\left\{-\frac{2\left(\sum_{l=1}^{t}D\bigl(p_s^{(l)}\parallel p_{s'}^{(l)}\bigr)\right)^2}{\sum_{l=1}^{t}(\beta_l-\alpha_l)^2}\right\}, \tag{25}$$

where α_l and β_l are the minimal and maximal values of the random variable $\xi_{s,s'}^{(l)}$, $l\in\{1,\dots,t\}$, respectively.

Note that the random variable $\xi_{s,s'}^{(l)}$ assumes two values, namely

$$\ln\left(\frac{1+\rho_{f,a}\bigl(s'\oplus g^{(l)}(a)\bigr)}{1+\rho_{f,a}\bigl(s\oplus g^{(l)}(a)\bigr)}\right)\quad\text{and}\quad\ln\left(\frac{1-\rho_{f,a}\bigl(s'\oplus g^{(l)}(a)\bigr)}{1-\rho_{f,a}\bigl(s\oplus g^{(l)}(a)\bigr)}\right).$$

Thus

$$(\beta_l-\alpha_l)^2=\left(\ln\left(\frac{1+\rho_{f,a}\bigl(s'\oplus g^{(l)}(a)\bigr)}{1-\rho_{f,a}\bigl(s'\oplus g^{(l)}(a)\bigr)}\right)-\ln\left(\frac{1+\rho_{f,a}\bigl(s\oplus g^{(l)}(a)\bigr)}{1-\rho_{f,a}\bigl(s\oplus g^{(l)}(a)\bigr)}\right)\right)^2,$$

whence

$$\begin{aligned}(\beta_l-\alpha_l)^2 &\le\left(\frac{2\bigl|\rho_{f,a}\bigl(s'\oplus g^{(l)}(a)\bigr)-\rho_{f,a}\bigl(s\oplus g^{(l)}(a)\bigr)\bigr|}{1-\bigl(\max\bigl\{\bigl|\rho_{f,a}\bigl(s\oplus g^{(l)}(a)\bigr)\bigr|,\bigl|\rho_{f,a}\bigl(s'\oplus g^{(l)}(a)\bigr)\bigr|\bigr\}\bigr)^2}\right)^2\\ &\le 4\Bigl(\rho_{f,a}\bigl(s'\oplus g^{(l)}(a)\bigr)-\rho_{f,a}\bigl(s\oplus g^{(l)}(a)\bigr)^2\Bigr)\frac{1}{(1-\rho(f,a)^2)^2},\\ &\qquad l\in\{1,\dots,t\},\end{aligned} \tag{26}$$

by inequalities (11) and (21).

It follows from inequality (20) that

$$D\bigl(p_s^{(l)}\parallel p_{s'}^{(l)}\bigr)\ge\frac{1}{2}\Bigl(\rho_{f,a}\bigl(s'\oplus g^{(l)}(a)\bigr)-\rho_{f,a}\bigl(s\oplus g^{(l)}(a)\bigr)\Bigr)^2, \qquad l\in\{1,\dots,t\}.$$

Hence

$$\left(\sum_{l=1}^{t} D\big(p_s^{(l)} \parallel p_{s'}^{(l)}\big)\right)^2 \geq \frac{1}{4}\left(\sum_{l=1}^{t}\Big(\rho_{f,a}\big(s' \oplus g^{(l)}(a)\big) - \rho_{f,a}\big(s \oplus g^{(l)}(a)\big)\Big)^2\right)^2. \tag{27}$$

Relations (25)–(27) imply the inequality

$$\mathsf{P}_s\left\{\sigma_s\big(\gamma^{(1)},\dots,\gamma^{(t)}\big) < \sigma_{s'}\big(\gamma^{(1)},\dots,\gamma^{(t)}\big)\right\} \leq \exp\left\{-\frac{(1-\rho(f,a)^2)^2}{8}\sum_{l=1}^{t}\Big(\rho_{f,a}\big(s' \oplus g^{(l)}(a)\big) - \rho_{f,a}\big(s \oplus g^{(l)}(a)\big)\Big)^2\right\},$$

whence we obtain the bound (23) by the definition of the parameter $\mu(f,a)$.

Therefore inequality (23) holds and Theorem 2 is proved.

Bibliography

1. P. Ekdahl and T. Johansson, *Another attack on A5/1*, IEEE Trans. on Inform. Theory **IT-49** (2003), no. 1. 284–289. MR1966707 (2004b:94059)
2. A. N. Alekseĭchuk and R. V. Proskurovskiĭ, *A lower bound for the probability of distinguishing the inner states of a clock-controlled combiner*, Pravove, Normatyvne ta Metrologychne Zabezpechennya Systemy Zahystu Informacii v Ukraine **2(13)** (2006), 159–169. (Russian)
3. F. Armknecht, J. Lano, and B. Preneel, *Extending the resynchronization attack*, Cryptology ePrint Archive, Report 2004/232 (http://eprint.iacr.org./2004/232/). MR2180666 (2006h:94069)
4. A. A. Borovkov, *Mathematical Statistics*, Nauka, Moscow, 1984; English transl., Gordon and Breach, Amsterdam, 1998. MR782295 (86i:62001); MR1712750 (2000f:62003)
5. O. A. Logachev, A. A. Sal'nikov, and V. V. Yashchenko, *Boolean Functions in Coding Theory and Cryptology*, Moskovskii Tsentr Nepreryvnogo Matematicheskogo Obrazovaniya, Moscow, 2004. (Russian) MR2078186 (2005g:94001)
6. W. Høffding, *Probability inequalities for sums of bounded random variables*, J. Amer. Statist. Assoc. **58** (1963), no. 301, 13–30. MR0144363 (26:1908)
7. I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, Academic Press, New York, 1981. MR666545 (84e:94007)

Institute of Special Communication and Protection of Information, National Technical University of Ukraine KPI, Moskovs'ka Street 45/1, Kyiv 01011, Ukraine

E-mail address: alex-crypto@mail.ru

Institute of Special Communication and Protection of Information, National Technical University of Ukraine KPI, Moskovs'ka Street 45/1, Kyiv 01011, Ukraine

E-mail address: roman-crypto@mail.ru

Received 4/DEC/2006

Translated by S. KVASKO