Theory of Stochastic Processes
Vol. 12 (28), no. 1–2, 2006, pp. 20–32

UDC 519.21

A. ALEKSEYCHUK AND L. KOVALCHUK

UPPER BOUNDS OF MAXIMUM VALUES OF AVERAGE DIFFERENTIAL AND LINEAR CHARACTERISTIC PROBABILITIES OF FEISTEL CIPHER WITH ADDER MODULO 2^m

The paper discusses the Feistel cipher with a block size of $n = 2m$, where the addition of a round key and a part of an incoming massage in each round is carried out modulo 2^m. In order to evaluate the security of such a cipher against differential and linear cryptanalyses, the new parameters of cipher s-boxes are introduced. The upper bounds of maximum average differential and linear probabilities of one round encryption transformation and the upper bounds of maximum average differential and linear characteristics probabilities of the whole cipher are obtained. The practical security of the cipher GOST (with independent and equiprobable random round keys) against differential and linear cryptanalysis is also evaluated. To the authors' mind, the obtained results allow one to expand the basic statements concerning the practical security of Markov (Feistel and SPN) ciphers against conventionally differential and linear attacks to a cipher of the type under study.

1. Introduction

Differential [1], [2] and linear cryptanalyses [3] are considered as the most powerful statistical techniques of the block cipher cryptographic analysis. The quite developed theory of differential and linear cryptanalysis of Markov block ciphers[1] [2] exists nowadays, techniques of their security estimations against differential and linear attacks are worked out, general techniques of design of SPN-ciphers and Markov Feistel ciphers that are practically secure against such attacks are well known. The literature devoted to this topic includes dozens of published manuscripts. Let's mention here review [4] and papers [5]–[7], where one can find a detailed bibliography.

In spite of the progress of mathematical foundations for differential and linear cryptanalyses, we have to admit that today there is no general theory of analysis and security proofs against the above-mentioned attacks of non-Markov block ciphers. This is caused by the analytical difficulties accompanying the investigations of the non-Markov block cipher security and by the lack of a new adequate mathematical procedure taking into account a specific structure of such ciphers.

The paper studies the analytical upper bounds of the maximum average differential and linear characteristic probabilities of a (non-Markov) Feistel cipher with a key adder modulo 2^m. The well-known example of such a cipher is GOST 28147-89 (hereafter GOST) [8]. The expressions for the obtained upper bounds include new parameters of the cipher s-boxes. These parameters are different from the classical measures (the maximum differential and the maximum linear probabilities of s-boxes) of the Markov

2000 *AMS Mathematics Subject Classification.* Primary 60C05, 94A60.

Key words and phrases. Feistel cipher, addition modulo 2^m, differential cryptanalysis, linear cryptanalysis, GOST.

[1]Hereafter the Markov block cipher is considered as a Markov cipher as to operation $\oplus$ of a bitwise Boolean addition in a set of binary vectors

cipher security against differential and linear cryptanalyses. It is shown that there exist s-boxes (length of 4), for which the maximum average differential probabilities of the round transformation of a cipher with the adder modulo 2^m are less than the maximum average differential probabilities of the round transformation of the corresponding Markov Feistel cipher with arbitrary chosen s-boxes.

The structure of the paper is as follows. Some definitions are introduced in Section 2, the exact task is stated, and the main results (Theorems 1, 2) are described in Section 3, their proofs are presented in Section 4. Section 5 depicts an application of Theorem 2 to the estimation of the average differential and linear probabilities of the GOST cipher modification by independent and equiprobable random round keys. Particular examples of cipher s-boxes are described, for which the maximum values of the average linear and differential characteristic probabilities of a 30-round cipher do not exceed 2^{-40} and $2^{-46.4}$, respectively. Finally, Section 6 discusses the results obtained and the future investigations.

2. Main Notations

Let l be an arbitrary natural number. We denote V_l as a set of Boolean vectors with length l and S^{V_l} as a symmetric group on V_l. For any $\alpha = (\alpha_1 \dots \alpha_l)$, $\beta = (\beta_1 \dots \beta_l) \in V_l$, we define $\alpha\beta = \alpha_1\beta_1 \oplus \dots \oplus \alpha_l\beta_l$, $\alpha \oplus \beta = (\alpha_1 \oplus \beta_1, \dots \alpha_1 \oplus \beta_1)$.

Below, an arbitrary vector $(x_1, \dots, x_l) \in V_l$ is identified with an integer number $x = 2^{l-1}x_1 + \dots + 2^0 x_l$. The symbol $x \overset{l}{+} y$ is used for the sum modulo 2^l of two binary integer numbers corresponding to vectors $x, y \in V_l$. We also use the notation $x + y$ instead of $x \overset{l}{+} y$ if it doesn't cause the confusion, and the value l is defined from the context (from the condition $x, y \in V_l$).

For any $x, y \in V_l$, we denote, by $\nu(x, y)$, the previous carry bit into the most significant (l-th) digit in the sum of two binary numbers x and y in the ring $\mathbb{Z}$.

Let $g \in S^{V_l}$, then

$$g_k(x) = g(x + k),\ x \in V_l, \tag{1}$$

$$C_g(\alpha, \beta) = 2^{-l} \sum_{x \in V_l} (-1)^{\alpha g(x) \oplus \beta x}, \tag{2}$$

$$D_g(\alpha, \beta) = 2^{-l} |\{x \in V_l : g(x \oplus \alpha) \oplus g(x) = \beta\}|, \tag{3}$$

$$d^{(g)}(\alpha, \beta) = 2^{-l} \sum_{k \in V_l} D_{g_k}(\alpha, \beta), \tag{4}$$

$$l^{(g)}(\alpha, \beta) = 2^{-l} \sum_{k \in V_l} \left(C_{g_k}(\beta, \alpha)\right)^2, \tag{5}$$

$$\Lambda^{(g)}(\alpha, \beta) = 2^{-l} \sum_{k \in V_l} \left(2^{-l} \sum_{a \in \{0,1\}} \left| 2^{-l} \sum_{x \in V_l : \nu(x,\, k) = a} (-1)^{\beta g(x+k) \oplus \alpha x} \right| \right)^2, \tag{6}$$

$$\Delta^{(g)}(\alpha, \beta) = 2^{-2l} \times$$

$$\times \max_{(a_1,\, a_2) \in V_2} \left\{ \sum_{(x,\, k) \in V_l \times V_l} \delta\left(g((x \oplus \alpha) + k + a_1) \oplus g(x + k + a_2),\ \beta\right) \right\}, \tag{7}$$

where $\delta(\cdot,\cdot)$ is the Kronecker delta, $\delta(u,v)=1$ if $u=v$, otherwise $\delta(u,v)=0$.

From Eqs. (1)–(7), we obtain directly the following relations:

$$d^{(g)}(\alpha,0)=l^{(g)}(\alpha,0)=\Delta^{(g)}(\alpha,0)=\Lambda^{(g)}(\alpha,0)=\delta(\alpha,0), \tag{8}$$

$$d^{(g)}(0,\beta)=l^{(g)}(0,\beta)=\Delta^{(g)}(0,\beta)=\Lambda^{(g)}(0,\beta)=\delta(0,\beta), \tag{9}$$

$$0\le d^{(g)}(\alpha,\beta)\le\Delta^{(g)}(\alpha,\beta)\le 1, \tag{10}$$

$$0\le l^{(g)}(\alpha,\beta)\le\Lambda^{(g)}(\alpha,\beta)\le 1, \tag{11}$$

for any $g\in S^{V_l}$, $\alpha,\beta\in V_l$.

3. Problem Statement and Main Results

Let's consider an r-round Feistel cipher $\Im$ with the set of plaintexts (ciphertexts) V_n, where $n=2m$, $m\ge 2$, the set of round keys $K=V_n$, and the encryption function $F: V_n\times K^r\to V_n$. A transformation $F^{(\lambda)}$ of the plaintext $x\in V_n$ into the ciphertext $y\in V_n$ with the key $\lambda=(k(1),\dots,k(r))\in K^r$ is a composition of r round encryption transformations $f^{(k(1))},\dots,f^{(k(r))}$ defined by the key λ:

$$y=F^{(\lambda)}(x)=(f^{(k(r))}\circ\dots\circ f^{(k(1))})(x),\ x\in V_n. \tag{12}$$

We assume that the encryption transformation $f^{(k)}$ $(k\in V_m)$ in each round from 1 to r takes the form

$$f^{(k)}(x)=f^{(k)}(u,v)=(v,u\oplus\varphi(v+k)), \tag{13}$$

where $x=(u,v)$ is the input of this round, $u,v\in V_m$, $\varphi\in S^{V_m}$, and the $+$ symbol (according to our agreement) denotes a sum modulo 2^m of m-digit binary integer numbers.

Assume that $m=pt$, p, $t\in\mathbb{N}$, and a substitution φ takes the form

$$\varphi(z)=A\left(s^{(p-1)}(z^{(p-1)}),\dots,s^{(0)}(z^{(0)})\right)^T,\ z=\left(z^{(p-1)},\dots,z^{(0)}\right)\in V_m, \tag{14}$$

where $z^{(j)}\in V_t$, $s^{(j)}\in S^{V_t}$ for any $j=\overline{0,p-1}$, and A is an invertible matrix of order m over the field $\mathbf{GF}(2)$.

The mapping φ is called a round function, and the substitutions $s^{(j)}$ $(j=\overline{0,p-1})$ are called s-boxes of a cipher $\Im$.

Below, a differential (linear) characteristic of the cipher $\Im$ is considered as an arbitrary sequence $\Omega=(\omega_0,\omega_1\dots,\omega_r)$ of non-zero Boolean vectors $\omega_0,\omega_1\dots,\omega_r\in V_n$.

We assume that the key $\lambda=(k(1),\dots,k(r))$ of the cipher $\Im$ is a random element with the equiprobable distribution on the set K^r. Let us consider the formal products

$$EDP(\Omega)\stackrel{def}{=}\prod_{i=1}^{r}\left(2^{-m}\sum_{k\in V_m}D_{f^{(k)}}(\omega_{i-1},\omega_i)\right), \tag{15}$$

$$ELP(\Omega)\stackrel{def}{=}\prod_{i=1}^{r}\left(2^{-m}\sum_{k\in V_m}\left(C_{f^{(k)}}(\omega_i,\omega_{i-1})\right)^2\right). \tag{16}$$

We call them as *the average differential characteristic probability* Ω and *the average linear characteristic probability* Ω *of a block cipher* $\Im$. Then

$$M_D(\Im)=\max_{(\Omega)}\{EDP(\Omega)\}, \tag{17}$$

$$M_L(\Im) = \max_{(\Omega)} \{ELP(\Omega)\}. \tag{18}$$

Notice that these definitions of the average probabilities $EDP(\Omega)$, $ELP(\Omega)$ actually coincide with the definitions of the same notations for Markov block ciphers [9]. In this case, the parameter upper bounds of (17), (18) are the standard values characterizing the practical security of (Markov) block ciphers against conventionally differential cryptanalysis and linear cryptanalysis, respectively [1], [3], [7], [9]–[11].

The paper solves the problem of obtaining the upper bounds of expressions (17), (18) for any Feistel cipher $\Im$ defined by expressions (12)–(14) in terms of certain parameters depending on the cipher s-boxes.

The following theorem plays a central role in obtaining the defined upper bounds.

Theorem 1. *Let $t, m \in \mathbb{N}$, $t \le m-1$, $\psi^{(1)}$ and $\psi^{(2)}$ are substitutions on the sets V_t and V_{m-t}, respectively. We define the substitution $\psi \in S^{V_m}$ assuming that*

$$\psi(x_2, x_1) = \left(\psi^{(2)}(x_2), \psi^{(1)}(x_1)\right),\ x_1 \in V_t,\ x_2 \in V_{m-t}. \tag{19}$$

Then, for any $\alpha = (\alpha_2, \alpha_1)$, $\beta = (\beta_2, \beta_1)$, where $\alpha_1, \beta_1 \in V_t$, $\alpha_2, \beta_2 \in V_{m-t}$, the following inequalities hold:

$$d^{(\psi)}(\alpha, \beta) \le d^{(\psi^{(l)})}(\alpha_1, \beta_1)\, \Delta^{(\psi^{(2)})}(\alpha_2, \beta_2), \tag{20}$$

$$l^{(\psi)}(\alpha, \beta) \le \Lambda^{(\psi^{(l)})}(\alpha_1, \beta_1)\, l^{(\psi^{(2)})}(\alpha_2, \beta_2). \tag{21}$$

The following result arises directly from Theorem 1 and relations (10), (11).

Corollary 1. *Let φ be a substitution (4), $\alpha = (\alpha^{(p-1)}, \dots, \alpha^{(0)})$, $\beta = (\beta^{(p-1)}, \dots, \beta^{(0)})$, where $\alpha^{(j)}, \beta^{(j)} \in V_t$, $j = \overline{0, p-1}$. Then*

$$d^{(\varphi)}(\alpha, A\beta^T) \le \prod_{j=0}^{p-1} \Delta^{(s_j)}(\alpha^{(j)}, \beta^{(j)}), \quad l^{(\varphi)}(\alpha, \beta A^{-1}) \le \prod_{j=0}^{p-1} \Lambda^{(s_j)}(\alpha^{(j)}, \beta^{(j)}). \tag{22}$$

The following theorem states the upper bounds of (17), (18), depending only on the s-boxes of the cipher $\Im$ and the number of rounds r.

Theorem 2. *Let $\Im$ be a Feistel cipher defined by expressions (12)–(14). Then the following relations hold for the maximum average differential and maximum average linear characteristic probabilities of the cipher $\Im$:*

$$M_D(\Im) \le \Delta(\Im)^{\lfloor \frac{2r}{3} \rfloor}, \quad M_L(\Im) \le \Lambda(\Im)^{\lfloor \frac{2r}{3} \rfloor}, \tag{23}$$

where

$$\Delta(\Im) = \max\left\{\Delta^{(s^{(j)})}(\alpha, \beta) : \alpha, \beta \in V_t \setminus \{0\},\ j = \overline{0, p-1}\right\}, \tag{24}$$

$$\Lambda(\Im) = \max\left\{\Lambda^{(s^{(j)})}(\alpha, \beta) : \alpha, \beta \in V_t \setminus \{0\},\ j = \overline{0, p-1}\right\}. \tag{25}$$

Notice that, for the Markov Feistel cipher with bijective round function φ, relations similar to (23) were obtained earlier in [11] (with the parameters $D_{s^{(j)}}(\alpha, \beta)$ and $\left(C_{s^{(j)}}(\alpha, \beta)\right)^2$ instead of $\Delta(\Im)$ and $\Lambda(\Im)$, respectively, $\alpha, \beta \in V_t \setminus \{0\}$, $\supset = \overline{0, p-1}$).

4. Proofs of Theorems

4.1. Proof of Theorem 1. We make some preliminary remarks. For any vector $z \in V_m$, we define z_1 and z_2 as the sub-vectors of z including its t least significant bits and $m-t$ most significant bits, respectively. The vector z will take the form $z = (z_2, z_1)$.

Let $x = (x_2, x_1)$, $k = (k_2, k_1)$, where $x_1, k_1 \in V_t$, $x_2, k_2 \in V_{m-t}$. We consider the integer numbers $x = x_1 + 2^t x_2$ and $k = k_1 + 2^t k_2$ corresponding to the above-mentioned Boolean vectors. Notice that $x_1, k_1 \in \overline{0, 2^t - 1}$, $x_2, k_2 \in \overline{0, 2^{m-t} - 1}$.

The following equality holds:

$$x \overset{m}{+} k = (x_1 \overset{t}{+} k_1) + 2^t (x_2 \overset{m-t}{+} k_2 \overset{m-t}{+} \nu(x_1, k_1)). \tag{26}$$

Here, $\nu(x_1, k_1)$ is a previous carry bit to the most significant (t-th) digit in the sum of the numbers x_1 and k_1 in the ring $\mathbb{Z}$.

Let us prove inequality (20). Applying the formulas (1), (3), (4), (19), and (26), we obtain the following chain of relations:

$$d^{(\psi)}(\alpha, \beta) = 2^{-m} \sum_{k \in V_m} \left(2^{-m} \sum_{x \in V_m} \delta\left(\psi_k(x \oplus \alpha) \oplus \psi_k(x),\, \beta\right) \right) =$$

$$= 2^{-2m} \sum_{x_1, k_1 \in V_t} \delta\left(\psi^{(1)}((x_1 \oplus \alpha_1) + k_1) \oplus \psi^{(1)}(x_1 + k_1),\, \beta_1\right) \times \tag{27}$$

$$\times \sum_{x_2, k_2 \in V_{m-t}} \delta\left(\psi^{(2)}((x_2 \oplus \alpha_2) + k_2 + \nu(x_1 \oplus \alpha_1, k_1)) \oplus \psi^{(2)}(x_2 + k_2 + \nu(x_1, k_1)),\, \beta_2\right).$$

For any $a_1, a_2 \in \{0, 1\}$, $k_1 \in V_t$, $k_2 \in V_{m-t}$, we assume

$$u_{k_1}(a_1, a_2) = 2^{-2t} \sum_{\substack{x_1 \in V_t: \\ \nu(x_1 \oplus \alpha_1, k_1) = a_1, \\ \nu(x_1, k_1) = a_2}} \delta\left(\psi^{(1)}((x_1 \oplus \alpha_1) + k_1) \oplus \psi^{(1)}(x_1 + k_1),\, \beta_1\right),$$

$$\nu_{k_2}(a_1, a_2) = 2^{-2(m-t)} \sum_{x_2 \in V_{m-t}} \delta\left(\psi^{(2)}((x_2 \oplus \alpha_2) + k_2 + a_1) \oplus \psi^{(2)}(x_2 + k_2 + a_2),\, \beta_2\right).$$

Then, using (27), we obtain

$$d^{(\psi)}(\alpha, \beta) = \sum_{\substack{k_1 \in V_t, \\ k_2 \in V_{m-t}}} \sum_{(a_1, a_2) \in V_2} u_{k_1}(a_1, a_2)\, \nu_{k_2}(a_1, a_2) \leq$$

$$\leq \left(\sum_{k_1 \in V_t} \sum_{(a_1, a_2) \in V_2} u_{k_1}(a_1, a_2) \right) \left(\max_{(a_1, a_2) \in V_2} \left\{ \sum_{k_2 \in V_{m-t}} \nu_{k_2}(a_1, a_2) \right\} \right). \tag{28}$$

Notice that, according to formulas (1), (4), and (7),

$$\sum_{k_1 \in V_t} \sum_{(a_1, a_2) \in V_2} u_{k_1}(a_1, a_2) = 2^{-t} \sum_{k_1 \in V_t} \left(2^{-t} \sum_{x_1 \in V_t} \delta\left(\psi^{(1)}((x_1 \oplus \alpha_1) + k_1) \oplus \right.\right.$$

$$\left.\left. \oplus \psi^{(1)}(x_1 + k_1),\, \beta_1\right) \right) = d^{(\psi^{(1)})}(\alpha_1, \beta_1), \tag{29}$$

$$\max_{(a_1,a_2)\in V_2}\left\{\sum_{k_2\in V_{m-t}}\nu_{k_2}(a_1,a_2)\right\}=\Delta^{(\psi^{(2)})}(\alpha_2,\beta_2). \tag{30}$$

So, on the basis of relations (28)–(30), inequality (20) is proved.

Now we prove inequality (21).

Let us denote $\chi(a)=(-1)^a$, where $a\in\{0,1\}$. We obtain the upper bound of the quantity

$$|C_{\psi_k}(\beta,\alpha)|=2^{-m}\left|\sum_{x\in V_m}\chi(\beta\psi(x+k)\oplus\alpha x)\right| \tag{31}$$

for a fixed $k=(k_1,k_2)$, where $k_1\in V_t$, $k_2\in V_{m-t}$. Applying formula (26), we can write down quantity (31) in the following form:

$$|C_{\psi_k}(\beta,\alpha)|=$$

$$=2^{-m}\left|\sum_{\substack{x_1\in V_t,\\ x_2\in V_{m-t}}}\chi\left(\beta_1\psi^{(1)}(x_1+k_1)\oplus\alpha_1x_1\oplus\beta_2\psi^{(2)}(x_2+k_2+\nu(x_1,k_1))\oplus\alpha_2x_2\right)\right|=$$

$$=2^{-m}\left|\sum_{a\in\{0,1\}}\sum_{\substack{x_1\in V_t,\\ \nu(x_1,k_1)=a}}\chi\left(\beta_1\psi^{(1)}(x_1+k_1)\oplus\alpha_1x_1\right)\times\right. \tag{32}$$

$$\left.\times\sum_{x_2\in V_{m-t}}\chi\left(\beta_2\psi^{(2)}(x_2+k_2+a)\oplus\alpha_2x_2\right)\right|.$$

For any $a\in\{0,1\}$, $k_1\in V_t$, $k_2\in V_{m-t}$, we assume

$$u_{k_1}(a)=2^{-t}\sum_{\substack{x_1\in V_t,\\ \nu(x_1,k_1)=a}}\chi\left(\beta_1\psi^{(1)}(x_1+k_1)\oplus\alpha_1x_1\right),\ u_{k_1}=|u_{k_1}(0)|+|u_{k_1}(1)|,$$

$$\nu_{k_2}(a)=2^{-(m-t)}\sum_{x_2\in V_{m-t}}\chi\left(\beta_2\psi^{(2)}(x_2+k_2+a)\oplus\alpha_2x_2\right)$$

Then, on the basis of (32), we have

$$|C_{\psi_k}(\beta,\alpha)|=\left|\sum_{a\in\{0,1\}}u_{k_1}(a)\nu_{k_2}(a)\right|\le\sum_{a\in\{0,1\}}|u_{k_1}(a)||\nu_{k_2}(a)|.$$

So taking the convexity down of the function $x\mapsto x^2$ into account, we obtain the relations

$$|C_{\psi_k}(\beta,\alpha)|^2\le(u_{k_1}(a))^2\left(\frac{|u_{k_1}(0)|}{u_{k_1}}|\nu_{k_2}(0)|+\frac{|u_{k_1}(1)|}{u_{k_1}}|\nu_{k_2}(1)|\right)^2\le$$

$$\le(u_{k_1}(a))^2\left(\frac{|u_{k_1}(0)|}{u_{k_1}}|\nu_{k_2}(0)|^2+\frac{|u_{k_1}(1)|}{u_{k_1}}|\nu_{k_2}(1)|^2\right)^2= \tag{33}$$

$$=u_{k_1}(a)\left(|u_{k_1}(0)||\nu_{k_2}(0)|^2+|u_{k_1}(1)||\nu_{k_2}(1)|^2\right).$$

Hence, on the basis of (5) and (33), we have

$$l^{(\psi)}(\alpha,\beta)=2^{-m}\sum_{k\in V_m}\left(C_{\psi_k}(\beta,\alpha)\right)^2\le2^{-m}\sum_{\substack{k_1\in V_t,\\ k_2\in V_{m-t}}}u_{k_1}\sum_{a\in\{0,1\}}|u_{k_1}(a)||\nu_{k_2}(a)|^2=$$

$$= 2^{-t} \sum_{k_1 \in V_t} u_{k_1} \sum_{a \in \{0,1\}} |u_{k_1}(a)| \left(2^{-(m-l)} \sum_{k_2 \in V_{m-t}} |\nu_{k_2}(a)|^2 \right). \tag{34}$$

Now notice that, for any $a \in \{0,1\}$,

$$2^{-(m-l)} \sum_{k_2 \in V_{m-t}} |\nu_{k_2}(a)|^2 =$$

$$= 2^{-(m-l)} \sum_{k_2 \in V_{m-t}} \left(2^{-(m-l)} \sum_{x_2 \in V_{m-t}} \chi \left(\beta_2 \psi^{(2)}(x_2 + k_2 + a) \oplus \alpha_2 x_2 \right) \right)^2.$$

Substituting the variable $k_2^{'} = k_2 + a$ in the right-hand side of the last equality, we obtain

$$2^{-(m-l)} \sum_{k_2 \in V_{m-t}} |\nu_{k_2}(a)|^2 =$$

$$= 2^{-(m-l)} \sum_{k_2^{'} \in V_{m-t}} \left(2^{-(m-l)} \sum_{x_2 \in V_{m-t}} \chi \left(\beta_2 \psi^{(2)}(x_2 + k_2^{'}) \oplus \alpha_2 x_2 \right) \right)^2 =$$

$$= 2^{-(m-l)} \sum_{k_2 \in V_{m-t}} \left(C_{\psi_{k_2}^{(2)}}(\beta_2, \alpha_2) \right)^2 = l^{(\psi^{(2)})}(\alpha_2, \beta_2).$$

Then we get

$$l^{(\psi)}(\alpha, \beta) \le 2^{-t} \sum_{k_1 \in V_t} u_{k_1} \left(\sum_{a \in \{0,1\}} |u_{k_1}(a)| \right) l^{(\psi^{(2)})}(\alpha_2, \beta_2) =$$

$$= \Delta^{(\psi^{(1)})}(\alpha_1, \beta_1)\, l^{(\psi^{(2)})}(\alpha_2, \beta_2),$$

from the previous equality, by applying (34) and (6), which completes the proof of Theorem 1.

4.2. Proof of Theorem 2. Let $\Omega = (\omega_0, \omega_1, \dots, \omega_r)$ and $\Omega^{'} = (\omega_0^{'}, \omega_1^{'}, \dots, \omega_r^{'})$ be arbitrary differential and linear characteristics of a cipher $\Im$, respectively. Without any restriction, we assume that

$$EDP(\Omega) \ne ELP(\Omega^{'}) \ne 0 \tag{35}$$

and show that, in this case,

$$EDP(\Omega) \le \Delta(\Im)^{\lfloor \frac{2r}{3} \rfloor} \tag{36}$$

$$ELP(\Omega^{'}) \le \Lambda(\Im)^{\lfloor \frac{2r}{3} \rfloor}, \tag{37}$$

where $\Delta(\Im)$, $\Lambda(\Im)$ are defined by formulas (24), (25), respectively.

Now let us prove some auxiliary statements.

Lemma 1. *Under condition (35), there exist sequences* $(\alpha_0, \alpha_1, \dots, \alpha_{r+1})$, $(\beta_0, \beta_1, \dots, \beta_{r+1})$ *of the m-dimensional Boolean vectors such that*

$$EDP(\Omega) = \prod_{i \in N(\Omega)} d^{(\varphi)}(\alpha_i, \alpha_{i-1} \oplus \alpha_{i+1}), \tag{38}$$

$$(\alpha_i, \alpha_{i+1}) \neq (0,0),\ i \in \overline{0,r}, \tag{39}$$

$$ELP(\Omega^{'}) = \prod_{i \in N(\Omega^{'})} l^{(\varphi)}(\beta_{i-1} \oplus \beta_{i+1}, \beta_i), \tag{40}$$

$$(\beta_i, \beta_{i+1}) \neq (0,0),\ i \in \overline{0,r}, \tag{41}$$

where

$$N(\Omega) = \{1, 2, \dots, r\} \setminus \{i \in \overline{0,r} : (\alpha_i, \alpha_{i-1} \oplus \alpha_{i+1}) = (0,0)\}, \tag{42}$$

$$N(\Omega^{'}) = \{1, 2, \dots, r\} \setminus \{i \in \overline{0,r} : (\beta_{i-1} \oplus \beta_{i+1}, \beta_i) = (0,0)\}. \tag{43}$$

In this case, the following inequality holds:

$$|N(\Omega)| \geq \left\lfloor \frac{2r}{3} \right\rfloor,\ |N(\Omega^{'})| \geq \left\lfloor \frac{2r}{3} \right\rfloor. \tag{44}$$

Proof. Let $\Omega = (\omega_0, \omega_1, \dots, \omega_r)$, $\omega_i = (\alpha_i, \gamma_i) \neq (0,0)$, where $\alpha_i,\ \gamma_i \in V_m$, $i \in \overline{0,r}$. Using formulas (3), (13), it's easy to check that, for any $k \in V_m$, $i \in \overline{1,r}$, the following equality holds:

$$D_{f^{(k)}}(\omega_{i-1}, \omega_i) = \delta(\gamma_{i-1},\ \alpha_i)\, D\varphi_k(\gamma_{i-1}; \alpha_{i-1} \oplus \gamma_i). \tag{45}$$

Let $\alpha_{r+1} = \gamma_r$. Substituting (45) in (15) and taking (35) into account, we obtain $\gamma_i = \alpha_{i+1}$, $i \in \overline{0,r}$; in particular, equalities (39) hold. Notice that

$$EDP(\Omega) = \prod_{i=1}^{r} \left(2^{-m} \sum_{k \in V_m} D\varphi_k(\alpha_i, \alpha_{i-1} \oplus \alpha_{i+1}) \right).$$

This relation and formulas (4), (8), and (42) yield equality (38).

The proof of (40), (41) is similar, with the use of formulas (2), (5), (8), (13), (16), and (43).

Now we prove the validity of inequality (44). Let $N_0(\Omega) = \{1, 2, \dots, r\} \setminus N(\Omega)$. For any $i \in \overline{1,r}$,

$$(i \in N_0(\Omega)) \Rightarrow \Bigg(\Big((i+1 \leq r) \Rightarrow (i+1 \in N(\Omega)) \Big) \& \tag{46}$$

$$\& \Big((i+2 \in N(\Omega)) \Rightarrow (i+2 \in N(\Omega)) \Big) \Bigg).$$

Then $|N_0(\Omega)| \leq \left\lceil \frac{r}{3} \right\rceil$, which directly implies the first inequality in (44). The second inequality has a similar proof.

Now we conclude that implication (46) is true. Let $i \in \overline{1,r}$ and $(\alpha_i, \alpha_{i-1} \oplus \alpha_{i+1}) = = (0,0)$. Then, applying (39), we have $\alpha_{i+1} \neq 0$ and, consequently, $\alpha_{i+2} = \alpha_i \oplus \oplus \alpha_{i+2} \neq 0$, because, otherwise, we obtain $EDP(\Omega) = 0$ on the basis of (8) and (38), which contradicts condition (35).

So we have

$$((\alpha_i, \alpha_{i-1} \oplus \alpha_{i+1}) = (0,0)) \Rightarrow ((\alpha_{i+1}, \alpha_i \oplus \alpha_{i+2}) \neq (0,0)), \text{ if } i+1 \leq r,$$

$$((\alpha_i, \alpha_{i-1} \oplus \alpha_{i+1}) = (0,0)) \Rightarrow ((\alpha_{i+2}, \alpha_{i+1} \oplus \alpha_{i+3}) \neq (0,0)), \text{ if } i+2 \leq r,$$

and Lemma 1 is completely proved.

Lemma 2. *Let φ be a substitution of the form (14),*

$$\alpha = (\alpha^{(p-1)}, \dots, \alpha^{(0)}), \qquad \beta = (\beta^{(p-1)}, \dots, \beta^{(0)}) \in V_m \setminus \{0\},$$

where $\alpha^{(j)}, \beta^{(j)} \in V_t$, $j \in \overline{0, p-1}$. Then

$$(d^{(\varphi)}(\alpha, A\beta^T) \neq 0) \Rightarrow (\exists i \in \overline{0, p-1} : (\alpha^{(i)} \neq 0) \& (\beta^{(i)} \neq 0)), \tag{47}$$

$$(l^{(\varphi)}(\alpha, \beta A^{-1}) \neq 0) \Rightarrow (\exists i \in \overline{0, p-1} : (\alpha^{(i)} \neq 0) \& (\beta^{(i)} \neq 0)). \tag{48}$$

L. et us assume that implication (47) is invalid. Suppose

$$i_1 = \min\{j \in \overline{0, p-1} : \alpha^{(i)} \neq 0)\}, \; i_2 = \min\{j \in \overline{0, p-1} : \beta^{(i)} \neq 0)\}.$$

We assume that $i_1 > i_2$ and consider the substitutions

$$\psi(x) = A^{-1}\varphi(x), \; x = (x^{(p-1)}, \dots, x^{(0)}),$$

$$\psi^{(1)}(x_1) = (s^{(i_1-1)}(x^{(i_1-1)}), \dots, s^{(0)}(x^{(0)})), \; x_1 = (x^{(i_1-1)}, \dots, x^{(0)}),$$

$$\psi^{(2)}(x_2) = (s^{(p-1)}(x^{(p-1)}), \dots, s^{(i_1)}(x^{(i_1)})), \; x_2 = (x^{(p-1)}, \dots, x^{(i_1)}),$$

where $x^{(j)} \in V_t, j \in \overline{0, p-1}$.

Notice that, according to inequality (20),

$$d^{(\varphi)}(\alpha, A\beta^T) = d^{(\psi)}(\alpha, \beta) \leq d^{(\psi^{(1)})}(\alpha_1, \beta_1) \, \Delta^{(\psi^{(2)})}(\alpha_2, \beta_2) \tag{49}$$

The following relations hold by the definitions of values i_1, i_2:

$$\alpha = (\alpha^{(i_1-1)}, \dots, \alpha^{(0)}) = 0, \; \beta = (\beta^{(i_1-1)}, \dots, \beta^{(0)}) \neq 0,$$

which implies $d^{(\psi^{(1)})}(\alpha_1, \beta_1) = 0$ [see (8)]. Then, using (49), we obtain $d^{(\varphi)}(\alpha, A\beta^T) = 0$, which contradicts the condition of implication (47).

So the case $i_1 > i_2$ is impossible. In the same way, we can show that $i_1 \geq i_2$. So $i_1 = i_2$, which yields the validity of implication (47). The proof of implication (48) is similar, with the use of inequality (21).

The lemma is completely proved.

To complete the proof of Theorem 2, we use expressions (38) and (40). Let us show that each factor $d^{(\varphi)}(\alpha_i, \alpha_{i-1} \oplus \alpha_{i+1})$, $i \in N(\Omega)$ on the right-hand side of equality (38) does not exceed $\Delta(\Im)$. In view of the first inequality (44), this allows us to directly get estimation (36).

Notice that, on the basis of relations (35), (42) for any $i \in N(\Omega)$, $\alpha \stackrel{def}{=} \alpha_1 \neq 0$, $A\beta^T \stackrel{def}{=} \alpha_{i-1} \oplus \alpha_{i+1} \neq 0$. According to Corollary 1 of Theorem 1,

$$d^{(\varphi)}(\alpha, A\beta^T) \leq \prod_{j=0}^{p-1} \Delta^{(s_j)}(\alpha^{(j)}, \beta^{(j)}). \tag{50}$$

In addition, using Lemma 2, we obtain that there are $j \in \overline{0, p-1}$ such that $\alpha^{(j)} \neq 0$, $\beta^{(j)} \neq 0$. Consequently, $\Delta^{(s_j)}(\alpha^{(j)}, \beta^{(j)}) \leq \Delta(\Im)$ and, on the basis of (50),

$$d^{(\varphi)}(\alpha_i, \alpha_{i-1} \oplus \alpha_{i+1}) \leq \Delta(\Im)$$

for any $i \in N(\Omega)$, what had to be proved. The validity of inequality (37) can be proved in the same way.

So Theorem 2 is completely proved.

5. Estimations of Maximum Average Linear and Differential Characteristic Probabilities of GOST Modification

As an example of the application of the obtained results, we consider a modification of the block cipher GOST, where round keys are chosen independently and equiprobably from V_m.

It's known [8] that GOST is a 32-round Feistel cipher with the block size $n = 64$, whose round encryption transformations and round function are defined by formulas (13) and (14), respectively. In our notations, $m = 32$, $t = 4$, $p = 8$, and the matrix A in expression (14) is substitutional (it corresponds to the left cyclic shift to 11 positions on the set V_{32}). It's also known that the s-boxes of GOST are its key parameters and, generally speaking, can be arbitrary substitutions belonging to the symmetric group S^{V_4}.

According to inequalities (23), the upper bounds of the maxima of the average differential and linear characteristic probabilities of the (modified) GOST depend on the parameters

$$\Delta^{(s)} = max\{\Delta^{(s)}(\alpha,\beta) : \alpha,\beta \in V_4 \setminus \{0\}\},$$
$$\Lambda^{(s)} = max\{\Lambda^{(s)}(\alpha,\beta) : \alpha,\beta \in V_4 \setminus \{0\}\},$$

where $\Delta^{(s)}(\alpha,\beta)$ and $\Lambda^{(s)}(\alpha,\beta)$ are defined by formulas (6) and (7), and a substitution s passes through the set of s-boxes of the given cipher.

Tables 1 and 2 demonstrate the results of statistical estimations for the parameters $\Delta^{(s)}$, $\Lambda^{(s)}$ (as functions of the random and equiprobable substitution $s \in S^{V_4}$), respectively. As we can see in Table 1, the value of $\Delta^{(s)}$ is between 0.151 and 0.200 for 7536 substitutions s out of 100000, generated randomly, independently and equiprobable on set V_4. Similarly, the value of $\Lambda^{(s)}$ is between 0.201 and 0.250 for 1591 substitutions s out of 100000 ones generated under the same conditions (see Table 2). Notice that, during our calculations, we cannot find any substitution $s \in S^{V_4}$ with the $\Lambda^{(s)} \leq 0.250$ property.

In Table 3, we have the examples of substitutions with small values of the parameters Δ^0 and Λ^0. The results of Theorem 2 demonstrate that, in the case where modified GOST cipher s-boxes are chosen from Table 3, the maximum average linear and differential characteristic probabilities of the 30-round GOST cipher do not exceed $(0.2)^{20} \approx 2^{-46.4}$ and $(0.25)^{20} = 2^{-40}$, respectively.

The estimations obtained didn't allow us to make any exact conclusions about the security of the cipher ГОСТ 28147-89 against differential or linear attacks. But, to our mind, the general methods of construction of similar estimations on the basis of Theorems 1 and 2 are the first steps towards the mathematically strict proof of the condition for the practical security of GOST against differential and linear cryptanalyses.

6. Discussion of Results and Future Investigations

Theorem 1 and Corollary 1 allow us to define the way of the construction of a substantial theory of the security evaluation of block ciphers described by relations (12)–(14) against a differential (linear) cryptanalysis in a similar way as to the well-known theory of estimation and proof of the security of Markov Feistel ciphers against differential (linear) attacks (see [7], [9]–[11] and references therein).

Let us put the described cipher $\Im$ in correspondence to the Markov block cipher $\Im_{\oplus}$. Their single difference consists in that the encryption transformation $f_{\oplus}^{(k)}$ $(k \in V_m)$

TABLE 1. Statistical estimation of the $\Delta^{(s)}$ parameter distribution (for 100000 substitutions $s \in S^{V_4}$)

Interval of values Δ^0	Number of substitutions	Interval of valuesΔ^0	Number of substitutions
$0.000 - 0.050$	0	$0.501 - 0.550$	0
$0.051 - 0.100$	0	$0.551 - 0.600$	0
$0.101 - 0.150$	0	$0.601 - 0.650$	0
$0.151 - 0.200$	7536	$0.651 - 0.700$	0
$0.201 - 0.250$	58633	$0.701 - 0.750$	0
$0.251 - 0.300$	26410	$0.751 - 0.800$	0
$0.301 - 0.350$	6424	$0.801 - 0.850$	0
$0.351 - 0.400$	893	$0.851 - 0.900$	0
$0.401 - 0.450$	104	$0.901 - 0.950$	0
$0.451 - 0.500$	0	$0.951 - 1.000$	0

TABLE 2. Statistical estimation of the $\Lambda^{(s)}$ parameter distribution (for 100000 substitutions $s \in S^{V_4}$)

Interval of values Λ^0	Number of substitutions	Interval of valuesΛ^0	Number of substitutions
$0.000 - 0.050$	0	$0.501 - 0.550$	396
$0.051 - 0.100$	0	$0.551 - 0.600$	14561
$0.101 - 0.150$	0	$0.601 - 0.650$	418
$0.151 - 0.200$	0	$0.651 - 0.700$	0
$0.201 - 0.250$	1591	$0.701 - 0.750$	0
$0.251 - 0.300$	40450	$0.751 - 0.800$	0
$0.301 - 0.350$	32049	$0.801 - 0.850$	0
$0.351 - 0.400$	7850	$0.851 - 0.900$	0
$0.401 - 0.450$	1693	$0.901 - 0.950$	0
$0.451 - 0.500$	761	$0.951 - 1.000$	231

TABLE 3. Examples of the substitution with small values of parameters Δ^0 and Λ^0

Substitutions$s \in S^{V_4}$	$\Delta^{(s)}$	$\Lambda^{(s)}$
$11, 2, 1, 14, 0, 7, 15, 4, 8, 9, 6, 12, 5, 13, 3, 10$	0.179688	0.250000
$7, 3, 8, 14, 2, 5, 1, 13, 15, 10, 9, 12, 4, 6, 11, 0$	0.187500	0.250000
$1, 8, 2, 9, 14, 5, 0, 13, 7, 4, 12, 3, 10, 6, 15, 11$	0.187500	0.250000
$3, 15, 12, 6, 8, 4, 1, 5, 13, 9, 14, 2, 11, 7, 0, 10$	0.187500	0.250000
$7, 11, 13, 0, 8, 2, 14, 15, 4, 10, 1, 3, 5, 12, 6, 9$	0.187500	0.250000
$14, 0, 4, 7, 9, 1, 12, 10, 13, 2, 3, 6, 11, 8, 15, 5$	0.195312	0.250000
$14, 4, 11, 3, 1, 6, 7, 8, 10, 12, 2, 9, 13, 0, 5, 15$	0.195312	0.250000
$5, 15, 2, 7, 13, 3, 12, 0, 6, 10, 14, 1, 9, 8, 11, 4$	0.195312	0.250000
$1, 0, 14, 10, 2, 8, 12, 3, 15, 7, 11, 5, 13, 6, 4, 9$	0.195312	0.250000
$11, 8, 6, 10, 13, 14, 1, 0, 4, 12, 5, 7, 3, 15, 9, 2$	0.195312	0.250000

contains $\oplus$ instead of $+$ in (13):

$$f_{\oplus}^{(k)}(u,v) = (v,\ u \oplus \varphi(v \oplus k)),\ u,v \in V_m \tag{51}$$

Applying equalities (2), (3), and (14), it's easy to see that the expressions for the average differential probability

$$(\omega_0, \omega_1) = ((\alpha_0, \alpha), (\alpha, \alpha_0 \oplus A\beta^T))$$

and the linear probability

$$(\omega_0^{'}, \omega_1^{'}) = ((\beta A^{-1}, \beta_0), (\alpha \oplus \beta_0, \beta A^{-1}))$$

of the random transformation $f_{\oplus}^{(k)}$, where $\alpha_0, \beta_0 \in V_m$,

$$\alpha = (\alpha^{(p-1)}, \dots, \alpha^{(0)}),\ \beta = (\beta^{(p-1)}, \dots, \beta^{(0)}),\ \alpha^{(j)}, \beta^{(j)} \in V_t,\ j \in \overline{0, p-1},$$

take the forms

$$2^{-m} \sum_{k \in V_m} D_{f_{\oplus}^{(k)}}(\omega_0, \omega_1) = D_{\varphi}(\alpha, A\beta^T) = \prod_{j=0}^{p-1} D_{s^{(j)}}(\alpha^{(j)}, \beta^{(j)}), \tag{52}$$

$$2^{-m} \sum_{k \in V_m} \left(C_{f_{\oplus}^{(k)}}(\omega_1^{'}, \omega_0^{'})\right)^2 = \left(C_{\varphi}(\beta A^{-1}, \alpha)\right)^2 = \prod_{j=0}^{p-1} \left(C_{s^{(j)}}(\beta^{(j)}, \alpha^{(j)})\right)^2, \tag{53}$$

respectively.

On the other hand, on the basis of formulas (22), (38), and (40), we obtain

$$2^{-m} \sum_{k \in V_m} D_{f^{(k)}}(\omega_0, \omega_1) = d^{(\varphi)}(\alpha, A\beta^T) \le \prod_{j=0}^{p-1} \Delta^{(s_j)}(\alpha^{(j)}, \beta^{(j)}), \tag{54}$$

$$2^{-m} \sum_{k \in V_m} \left(C_{f^{(k)}}(\omega_1^{'}, \omega_0^{'})\right)^2 = l^{(\varphi)}(\alpha, \beta A^{-1}) \le \prod_{j=0}^{p-1} \Lambda^{(s_j)}(\alpha^{(j)}, \beta^{(j)}). \tag{55}$$

As we can see from relations (52) and (54) [also (53) and (55)], the differential (linear) properties of the round encryption transformations of ciphers $\Im_{\oplus}$ and $\Im$ have similar analytical descriptions in terms of some parameters of their s-boxes.

To our mind, the similarity mentioned above allows us to expand the existing techniques for the practical security estimation of Markov Feistel ciphers against differential and linear cryptanalyses [with round transformations (51)] to a non-Markov cipher class [with round transformations (13)]. The above can be also applied to SPN-ciphers and their "2^m modulo" modifications. In particular, using the well-known active s-box counting technique [7], it's possible to make estimations (17), (18) depending on the matrix A from (14) and more accurate.

It is worth comparing the parameter values

$$\Delta_t \stackrel{def}{=} \min_{s \in S^{V_t}} \max \left\{\Delta^{(s)}(\alpha, \beta) : \alpha, \beta \in V_t \setminus \{0\}\right\},$$

$$D_t \stackrel{def}{=} \min_{s \in S^{V_t}} \max \left\{D_s(\alpha, \beta) : \alpha, \beta \in V_t \setminus \{0\}\right\}$$

and, respectively,

$$\Lambda_t \stackrel{def}{=} \min_{s \in S^{V_t}} \max \left\{\Lambda^{(s)}(\alpha, \beta) : \alpha, \beta \in V_t \setminus \{0\}\right\},$$

$$C_t \stackrel{def}{=} \min_{s\in S^{V_t}} \max\left\{C_s(\alpha,\beta)^2 : \alpha,\beta \in V_t \setminus \{0\}\right\}$$

that characterize the differential and linear probabilities of the best $\Im$ and $\Im_{\oplus}$ cipher s-boxes.

It is well known [12] that, at $t = 4$, $C_4 = D_4 = 0.25$. On the other hand, according to the data in Table 3, $\Lambda_4 \le 0.25$, $\Delta_4 \le 0.18$. So, at least at $t = 4$, the sets of s-boxes of the cipher $\Im$ exist, for which the maximum average differential probability of the one-round encryption transformation is less than the maximum average differential probability of the one-round encryption transformation of the cipher $\Im\oplus$ with arbitrary determined s-boxes [see relations (52) and (54)]. The problem of the calculation of exact values of Δ_t and Λ_t isn't solved still.

Finally, we have to remark that the important task for the future investigations is the extension of Theorem 1 to a wider class of group operations applied for the definitions of differential and linear approximations of the block cipher transformations. We can include the addition modulo 2^m into natural operations of the same type.

Acknowledgement

The authors would like to thank Victor Bezditny and Sergey Ignatenko for their help in the statistical estimation with PC of the results described in Section 5 of this paper.

Bibliography

1. Biham E., Shamir A., *Differential cryptanalysis of DES-like cryptosystems*, J. of Cryptology **4** (1991), no. 1, 3–72.
2. Lai X., Massey J.L., Murphy S., *Markov ciphers and differential cryptanalysis*, Advances in Cryptology - EUROCRYPT'91, Proceedings, Springer, 1991, pp. 17–38.
3. Matsui M., *Linear cryptanalysis methods for DES cipher*, Advances in Cryptology - EUROCRYPT'93, Proceedings, Springer, 1994, pp. 386 – 397.
4. Biryukov A., *Block ciphers and stream ciphers: the state of the art*, http://eprint.iacr.org/2004/094.
5. Vaudenay S., *Decorrelation: a theory for block cipher security*, J. of Cryptology **16** (2003), no. 4, 249–286.
6. Daemen J., Rijmen V., *Statistics of correlation and differentials in block ciphers*, http://eprint.iacr.org/ 2005/212.
7. Kanda M., *Practical security evaluation against differential and linear cryptanalyses for Feistel ciphers with SPN round function*, Selected Areas in Cryptography. - SAC 2000, Proceedings (2001), Springer Verlag, 324–338.
8. Gosudarstvennyi Standart 28147-89. Cryptographic Protection for Data Processing Systems, Government Committee of the USSR for Standarts (1989).
9. Vaudenay S., *On the security of CS-cipher*, Fast Software Encryption. - FSE'99, Proceedings, Springer, 1999, pp. 260–274.
10. Knudsen L.R., *Practically secure Feistel cipher*, Fast Software Encryption. - FSE'94, Proceedings, Springer, 1994, pp. 211–221.
11. Kanda M., Takashima Y., Matsumoto T., et al., *A strategy for constructing fast round functions with practical security against differential and linear cryptanalysis*, Selected Areas in Cryptography. - SAC 1998, Proceedings, Springer, 1999, pp. 264–279.
12. Canteaut A., *Cryptographic functions and design criteria for block ciphers*, INDOCRYPT'2001, Proceedings, Springer, 2001, pp. 1–16.

National Technical University of Ukraine (KPI), 37, Peremogy Ave., Kyiv 03056, Ukraine