Towards a Theory of Security Evaluation for GOST-like Ciphers against Differential and Linear Cryptanalysis

A. N. Alekseychuk*, L. V. Kovalchuk**
Institute of Special Communication and Information Security,
National Technical University of Ukraine (KPI)
*alex-crypto@mail.ru
**lv_kov_crypto@mail.ru

Abstract

In this paper, we present new general techniques for practical security evaluation against differential and linear cryptanalysis for an extensive class of block ciphers similar to the cipher GOST. We obtain upper bounds of the average differential and linear characteristic probabilities for an arbitrary GOST-like cipher. The obtained bounds have similar form to the upper bounds of the average differential and linear characteristic probabilities known for some Markov Feistel ciphers. But, the expressions of our bounds contain new parameters (different from the classical differential and linear probabilities) of the cipher's s-boxes. These parameters are very natural for GOST-like ciphers, since they inherit the type of operation (key addition modulo 2^m) used in these ciphers. The methods our proofs are based on are of independent interest and can be used for investigation both of a wider class of block ciphers and of a wider class of attacks.

Application of our results to GOST shows that maximum values of the average differential and linear characteristic probabilities of this cipher (with 32 rounds and some s-boxes) are bounded by $2^{-59.57}$ and 2^{-42}, respectively. The last two estimates of practical security of GOST against the differential and linear cryptanalysis are not quite impressive. But, as far as we know, they are the best of such estimates obtained by an accurate mathematical proof.

1 Introduction

Differential and linear cryptanalysis are considered the most powerful cryptographic attacks known to date. In their basic form, they were applied to DES in early 90-s of the last century [1], [2] and were improved and extended in several ways during recent 20 years.

An important step in the development of differential and linear cryptanalysis was the concept of Markov block cipher [3]. Informally, a block cipher is called Markov [1] one if average difference propagation probability over each round is independent of the round's text input. There are numerous examples of Markov ciphers including DES, Rijndael, Camellia, and many others. For such ciphers, a quite developed theory of security evaluation and security proofs against differential and linear cryptanalysis is

[1] Hereafter the word-combination "Markov block cipher" will denote a Markov cipher with respect to the bitwise XOR operation.

created, and general techniques for design of Markov (Feistel and SPN) block ciphers secure against such attacks are well known. The literature devoted to this topic includes dozens of published works. Let us mention here the papers [4] – [7], where one can find more detailed bibliography.

In spite of the progress in mathematical foundations of differential and linear cryptanalysis, there is no general theory of analysis and security proofs against the above-mentioned attacks for non-Markov ciphers such that the block cipher GOST [8]. A reason of that are some analytical difficulties accompanying security evaluation for such ciphers and the lack of adequate mathematical methods accounting their specific structure. In this paper, we present new general techniques for practical security evaluation against differential and linear cryptanalysis for GOST-like ciphers, and apply our results to the cipher GOST with independent and equiprobable random round keys.

1.1 Previous work on differential and linear cryptanalysis of GOST

As is known, the most significant difference between GOST and others (ordinary Markov) block ciphers consists in using of round key addition modulo 2^{32}. It leads to analytical difficulties in security evaluation for this cipher against differential and linear cryptanalysis because the known traditional methods cannot be used for GOST, see [9] – [12]. In all works known to us that are devoted to differential and linear cryptanalysis of GOST its practical security against mentioned attacks is investigated. The round keys are usually assumed to be fully random and independent. The main purpose of the majority of this works (which are written generally in Russian or in Ukrainian) is to find high-probability differential and linear characteristics of GOST, using some assumptions about the key addition operation. For example, in [12] it is assumed in the calculation of differential characteristics probabilities that, with addition of input messages and keys in all rounds, the carry bits in $4^{\text{th}}, 8^{\text{th}}, \ldots, 28^{\text{th}}$ digits of the sum vanish (in other words, the carry bits between different s-boxes are ignored). It is clear that such mathematical assumptions simplifying a block cipher cannot be taken a priori in security proofs against differential and linear cryptanalysis.

Especially we want to point out the work [13], which results are discussed in recent papers [14], [15]. In [13], the authors write that GOST is secure against differential cryptanalysis after 7 rounds and against linear cryptanalysis after 5 rounds. But, their "proof" relies on numerous implicit assumptions similar to those mentioned above. Moreover, the work [13] contains some mathematical mistakes, so its results cannot be admitted as reliable. For example, it is claimed that "the effectiveness of the linear approximation of the addition mod 2^{32} operation is equal to 2^{-i-1} and the best approximation of the i-th bit of result is the sum mod 2 of the i-th bit of the values" (see [13], P. 6). But, it is well-known that the effectiveness of such linear approximation does not depend on i and is equal to $3/4$ (see [16]). It is a pity that all this facts were left unnoticed in [14], [15].

For the first time, upper bounds of the average differential and linear characteristic probabilities obtained for an extensive class of block ciphers similar to GOST are

adduced in our paper [17]. In [18], [19] these results were extended. The present work contains systematic description of results from [17] – [19] in revised and improved form.

1.2 Contribution of this paper

Our main results are formulated in two theorems, which state upper bounds of the average differential and linear characteristic probabilities for an arbitrary GOST-like cipher. The obtained bounds have similar form to upper bounds of average differential and linear characteristic probabilities known for Markov Feistel ciphers with SPN round functions [7], [20]. But, the expressions of our bounds contain new parameters (different from the classical differential and linear probabilities) of the cipher's s-boxes. Note that these parameters are very natural for GOST-like ciphers, since they inherit the type of operation (key addition modulo 2^m) used in these ciphers. Also note that the methods our proofs are based upon are of independent interest and can be used for investigation both of a wider class of block ciphers (for example, containing "mixed" key operations) and of a wider class of attacks (for example, bilinear cryptanalysis), see [21], [22].

Application of our results to GOST shows that maximum values of the average differential and linear characteristic probabilities of this cipher (with 32 rounds and some s-boxes) are bounded by $2^{-59.57}$ and 2^{-42}, respectively. Note that these two estimates of practical security of GOST against differential and linear cryptanalysis are not quite impressive. But, as far as we know, they are the best of such estimates obtained by an accurate mathematical proof.

The structure of the paper is as follows. Basic notation and definitions are introduced in Section 2. Our main results are presented in Section 3 and their proofs are given in Section 4. Finally, in Section 5 some applications, numerical examples, discussion of the obtained results, and also of the further research are described.

2 Preliminaries

2.1 Basic notation

Let l be an arbitrary natural number. We denote by V_l the set of all l-dimensional Boolean vectors and by S^{V_l} the symmetric group on the set V_l. For any $\alpha = (\alpha_1, \ldots, \alpha_l)$, $\beta = (\beta_1, \ldots, \beta_l) \in V_l$ let us define $\alpha\beta = \alpha_1\beta_1 \oplus \cdots \oplus \alpha_l\beta_l$, $\alpha \oplus \beta = (\alpha_1 \oplus \beta_1, \ldots, \alpha_l \oplus \beta_l)$, where $\oplus$ is the XOR operation. For any $a, b \in \mathbb{Z}$, $a \leq b$, denote by $\overline{a,b}$ the set $\{a, a+1, \ldots, b\}$.

In the sequel, we identify an arbitrary vector $(x_1, \ldots, x_l) \in V_l$ with the number $x = 2^{l-1}x_1 + \cdots + 2^0 x_l$ and denote by $x \overset{l}{+} y$ the sum modulo 2^l of the numbers corresponding to the vectors $x, y \in V_l$. We also use the notation $x + y$ instead of $x \overset{l}{+} y$ if it does not cause the confusion and the value l is defined from the context (i.e., from the condition $x, y \in V_l$).

For any $x, y \in V_l$ let's denote by $\nu(x, y)$ the carry bit into the most significant (i.e., the l-th) digit in the sum of the numbers x and y in the ring $\mathbb{Z}$.

For any $g \in S^{V_l}$,$\alpha, \beta \in V_l$ let us define

$$g_k(x) = g(x \overset{l}{+} k),\ x, k \in V_l,$$

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

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

$$\Lambda^{(g)}(\alpha, \beta) = 2^{-l} \sum_{k \in V_l} \left(2^{-l} \sum_{a \in \{0,1\}} \left| \sum_{x \in V_l : \nu(x,k) = a} (-1)^{\beta g(x \overset{l}{+} k) \oplus \alpha x} \right| \right)^2, \tag{3}$$

$$D_x^{(g)}(\alpha, \beta) = 2^{-l} \sum_{k \in V_l} \delta\left(g_k(x \oplus \alpha) \oplus g_k(x), \beta\right),\ x \in V_l, \tag{4}$$

$$d^{(g)}(\alpha, \beta) = 2^{-l} \sum_{k \in V_l} \delta\left(g(k \overset{l}{+} \alpha) \oplus g(k), \beta\right), \tag{5}$$

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

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

It follows directly from (1)–(6) that

$$l^{(g)}(\alpha, 0) = d^{(g)}(\alpha, 0) = l^{(g)}(0, \alpha) = d^{(g)}(0, \alpha) = \delta(\alpha, 0), \tag{7}$$

$$\Lambda^{(g)}(0, 0) = 1, \tag{8}$$

$$0 \le l^{(g)}(\alpha, \beta) \le \Lambda^{(g)}(\alpha, \beta) \le 1, \tag{9}$$

$$0 \le d_0^{(g)}(\alpha, \beta) + d_1^{(g)}(\alpha, \beta) = d^{(g)}(\alpha, \beta) = D_0^{(g)}(\alpha, \beta) \le 1, \tag{10}$$

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

In what follows we will omit the symbol of transposition in formulas like Az^T, supposing (as usual) that a vector z is a column if it is written on the left of a matrix A.

2.2 GOST-like ciphers

Let us consider an r-round Feistel cipher $\mathfrak{T}$ with the encryption function $F : V_n \times K^r \to V_n$, where V_n is the set of plaintexts (ciphertexts) and $K = V_m$ is the set of round keys of the cipher $\mathfrak{T}$, $n = 2m$, $m \ge 2$. By definition, the transformation of a plaintext $x \in V_n$ into the ciphertext $y \in V_n$ with a key $\lambda = (k(1), \ldots, k(r)) \in K^r$ is defined as follows:

$$y = F(x, \lambda) = \left(f^{(k(r))} \circ \cdots \circ f^{(k(1))}\right)(x),\ x \in V_n, \tag{11}$$

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

$$f^{(k)}(x) = f^{(k)}(x_1, x_2) = (x_2, x_1 \oplus \phi(x_2 \overset{m}{+} k)), \tag{12}$$

$x = (x_1, x_2)$ is the input of this round, $x_1, x_2 \in V_m$, and $\phi \in S^{V_m}$. Next, assume that $m = pt$, $p, t \in \mathbb{N}$, and

$$\phi(z) = A\, s(z) = A(s^{(p-1)}(z^{(p-1)}), \ldots, s^{(0)}(z^{(0)})),\ z = (z^{(p-1)}, \ldots, z^{(0)}) \in V_m, \tag{13}$$

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

We say that $\mathfrak{T}$ is *a GOST-like cipher with the round function ϕ, the s-function s, and s-boxes $s^{(j)}$, $j \in \overline{0, p-1}$*, if the conditions (11) – (13) hold.

A well-known example in the GOST-like ciphers's family is the block cipher GOST (with independent and equiprobable random round keys). Recall [8] that GOST is a 32-round Feistel cipher with the block size $n = 64$, whose round transformations and the round function are defined by formulas (12) and (13), respectively. In our notation, $m = 32$, $t = 4$, $p = 8$, and the matrix A in (13) corresponds to the left cyclic shift to 11 positions on the set V_{32}. It is known that the s-boxes of GOST are its key parameters and, in principle, may be arbitrary substitutions from the symmetric group S^{V_4}.

2.3 Practical security of block ciphers against differential and linear cryptanalysis

Two general approaches to security evaluation of any block cipher against differential and linear cryptanalysis are known. The difference between these approaches lies in using of different security measures. In the first case, to get the *provable security* of a block cipher against differential and linear cryptanalysis, the values of the maximum average differential probability and the maximum average linear hull probability of the cipher are used. In the second case, to get the *practical* (or *heuristical*) *security* of a block cipher, the values of the maximum differential and linear characteristic probabilities are used. We not discuss here the relation between these approaches (see [5], [7], [23] – [26] for complete details).

Let $\mathfrak{T}$ be a block cipher with the encryption function (11). A (*differential* or *linear*) *characteristic* of the cipher $\mathfrak{T}$ is an arbitrary sequence $\Omega = (\omega_0, \omega_1, \ldots, \omega_r)$ of non-zero Boolean vectors $\omega_0, \omega_1, \ldots, \omega_r \in V_n$. For any fixed key $\lambda = (k(1), \ldots, k(r))$ the *differential probability of the characteristic* Ω is defined as follows:

$$DP^{(\lambda)}(\Omega) = \mathbf{P}\left(\bigcap_{i=1}^{r}\{X_i \oplus X_i' = \omega_i\} | X \oplus X' = \omega_0\right), \tag{14}$$

where X and X' are independent and equiprobable random Boolean vectors, $X_i = (f^{(k(i))} \circ \cdots \circ f^{(k(1))})(X)$, $X_i' = (f^{(k(i))} \circ \cdots \circ f^{(k(1))})(X')$, $i \in \overline{1, r}$. The expected value

$$EDP(\Omega) = |K|^{-r} \sum_{\lambda \in K^r} DP^{(\lambda)}(\Omega) \tag{15}$$

is called the *average differential characteristic probability* (*of the characteristic* Ω). The *average linear characteristic probability of* Ω is a formal product

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

where $C_{f^{(k)}}(\omega_i, \omega_{i-1})$, $i \in \overline{1, r}$ are defined by (1).

Let

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

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

According to generally accepted setting (see, for example, [7], [23]), a block cipher $\mathfrak{T}$ is practically secure against differential and linear cryptanalysis if the upper bounds of the values (17) and (18) are less than the security threshold. Thus, to evaluate the practical security of GOST-like ciphers against differential and linear cryptanalysis it is necessary to develop a general and acceptable method for determining the upper bounds of the values (17), (18), by analogy with well-known methods for Markov ciphers.

3 Main results

Let $\mathfrak{T}$ be a GOST-like cipher with the round function (13). We use the following definitions:

$$\Delta(\mathfrak{T}) = \max \left\{ d^{(s^{(j)})}(\alpha, \beta) : \alpha, \beta \in V_t \setminus \{0\},\ j \in \overline{0, p-1} \right\}, \tag{19}$$

$$\Delta'(\mathfrak{T}) = \max \left\{ d_a^{(s^{(j)})}(\alpha, \beta) : \alpha, \beta \in V_t \setminus \{0\},\ j \in \overline{0, p-1},\ a \in \{0, 1\} \right\}, \tag{20}$$

$$\Lambda(\mathfrak{T}) = \max \left\{ l^{(s^{(j)})}(\alpha, \beta) : \alpha, \beta \in V_t \setminus \{0\},\ j \in \overline{0, p-1} \right\}, \tag{21}$$

$$\Lambda_{\mathfrak{T}} = \max \left\{ \Lambda^{(s^{(j)})}(\alpha, \beta) : (\alpha, \beta) \in V_t \times V_t \setminus \{(0, 0)\},\ j \in \overline{0, p-1} \right\}, \tag{22}$$

where the numbers $l^{(s^{(j)})}(\alpha, \beta)$, $\Lambda^{(s^{(j)})}(\alpha, \beta)$, $d^{(s^{(j)})}(\alpha, \beta)$, and $d_a^{(s^{(j)})}(\alpha, \beta)$ are defined by (2), (3), (5), and (6), respectively.

Let $z^{(j)} \in V_t$, $j \in \overline{0, p-1}$, then the *weight* of a vector $z = (z^{(p-1)}, \ldots, z^{(0)}) \in V_m$ is the number $wt(z) = |\{j \in \overline{0, p-1} : z^{(j)} \neq 0\}|$. We denote by W the following subgroup of the Abelian group $(V_m, \oplus)$:

$$W = \{(z^{(p-1)}, \ldots, z^{(0)}) \in V_m : z^{(p-2)} = \cdots = z^{(0)} = 0\}. \tag{23}$$

The *branch number* of an $m \times m$-matrix A over the field $\mathbf{GF}(2)$ is defined as follows [27]:

$$B_A = \min\{wt(x) + wt(xA) : x \in V_m \setminus \{0\}\}. \tag{24}$$

The following theorems state our upper bounds of the values (17), (18) for an arbitrary GOST-like cipher.

Theorem 1. *Let $\mathfrak{T}$ be a GOST-like cipher with the round function (13). Then*

$$M_D(\mathfrak{T}) \leq \Delta(\mathfrak{T})^{\left[\frac{2r}{3}\right]}. \tag{25}$$

Moreover, if

$$\{Az : z \in W\} \cap W = \{0\} \tag{26}$$

then

$$M_D(\mathfrak{T}) \leq \max\left\{\Delta(\mathfrak{T})^{r-1},\ \Delta(\mathfrak{T})^{r+1-2\left\lceil\frac{r}{3}\right\rceil}\,\Delta'(\mathfrak{T})^{\left\lceil\frac{r}{3}\right\rceil}\right\}. \tag{27}$$

Theorem 2. *Let $\mathfrak{T}$ be a GOST-like cipher with the round function (13). Then*

$$M_L(\mathfrak{T}) \leq \Lambda(\mathfrak{T})^{\left[\frac{2r}{3}\right]}. \tag{28}$$

Moreover,

$$M_L(\mathfrak{T}) \leq (\Lambda_{\mathfrak{T}})^r \ \textit{if}\ B_A = 3 \tag{29}$$

and

$$M_L(\mathfrak{T}) \leq (\Lambda_{\mathfrak{T}})^{\left[\frac{r}{4}\right]B_A} \ \textit{if}\ B_A \geq 4. \tag{30}$$

Let us remark that the inequalities (25), (27), and (28) – (30) allows to evaluate the practical security of a GOST-like cipher against differential and linear cryptanalysis directly on the information about the cipher's s-function and the number of rounds r. Note also that the inequalities (25), (28) – (30) are similar to the bounds of the average differential and linear characteristic probabilities known for Markov Feistel ciphers with SPN round functions [7], [20], and can be considered as an extension of these bounds to the class of GOST-like ciphers.

4 Proofs

4.1 Upper bounds for the s-function of a GOST-like cipher

In this subsection upper bounds of the parameters like (2) and (5) for the s-function of an arbitrary GOST-like cipher are presented. These results play the key role in the follow-up statements and are of independent interest. The proofs of these results demonstrate the essence of our methods for obtaining the upper bounds of the values (17) and (18).

The following lemma was first proved in [17].

Lemma 1. *Let $t, m \in \mathbb{N}$, $t < m$, $\psi^{(1)} \in S^{V_t}$, $\psi^{(2)} \in S^{V_{m-t}}$, and*

$$\psi(x_2, x_1) = (\psi^{(2)}(x_2), \psi^{(1)}(x_1)),\ x_1 \in V_t,\ x_2 \in V_{m-t}. \tag{31}$$

Then, for any $\alpha = (\alpha_2, \alpha_1)$, $\beta = (\beta_2, \beta_1)$ such that $\alpha_1, \beta_1 \in V_t$, $\alpha_2, \beta_2 \in V_{m-t}$ the following inequality holds:

$$l^{(\psi)}(\alpha, \beta) \leq \Lambda^{(\psi^{(1)})}(\alpha_1, \beta_1)\, l^{(\psi^{(2)})}(\alpha_2, \beta_2). \tag{32}$$

Proof. Let us make some preliminary remarks. For any vector $z \in V_m$ denote by z_1 and z_2 the sub-vectors of z including its least t significant bits and its most $m-t$ 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 $x_1, k_1 \in V_t$, $x_2, k_2 \in V_{m-t}$. Let's consider the numbers $x = x_1 + 2^t\, x_2$ and $k = k_1 + 2^t\, k_2$ corresponding to above-mentioned Boolean vectors. Observe that $x_1, k_1 \in \overline{0, 2^t - 1}$, $x_2, k_2 \in \overline{0, 2^{m-t} - 1}$, and

$$x \overset{m}{+} k = \left(x_1 \overset{t}{+} k_1 \right) + 2^t \left(x_2 \overset{m-t}{+} k_2 \overset{m-t}{+} \nu(x_1, k_1) \right), \tag{33}$$

where $\nu(x_1, k_1)$ is the carry bit to the t-th digit in the sum of the numbers x_1 and k_1 in the ring $\mathbb{Z}$ (see Subsection 2.1).

Let us define $\chi(a) = (-1)^a$ for $a \in \{0, 1\}$, fix any $k = (k_2, k_1)$, where $k_1 \in V_t$, $k_2 \in V_{m-t}$, and obtain an upper bound of the quantity

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

We have from (33)

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

$$= 2^{-m} \left| \sum_{\substack{x_1 \in V_t, \\ x_2 \in V_{m-t}}} \chi\left(\beta_1 \psi^{(1)}(x_1 + k_1) \oplus \alpha_1 x_1 \oplus \beta_2 \psi^{(2)}(x_2 + k_2 + \nu(x_1, k_1)) \oplus \alpha_2 x_2\right) \right| =$$

$$= 2^{-m} \left| \sum_{a \in \{0,1\}} \sum_{\substack{x_1 \in V_t: \\ \nu(x_1, k_1) = a}} \chi\left(\beta_1 \psi^{(1)}(x_1 + k_1) \oplus \alpha_1 x_1\right) \times \right.$$

$$\left. \times \sum_{x_2 \in V_{m-t}} \chi\left(\beta_2 \psi^{(2)}(x_2 + k_2 + a) \oplus \alpha_2 x_2\right) \right|. \tag{34}$$

For any $a \in \{0, 1\}$, $k_1 \in V_t$, $k_2 \in V_{m-t}$ let's define

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

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

$$u_{k_1} = |u_{k_1}(0)| + |u_{k_1}(1)|.$$

Then from (34) we get

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

Next, taking into account the convexity of the function $x \mapsto x^2$, $x \geq 0$, we obtain the following inequalities:

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

$$\leq (u_{k_1})^2 \left(\frac{|u_{k_1}(0)|}{u_{k_1}} |v_{k_2}(0)|^2 + \frac{|u_{k_1}(1)|}{u_{k_1}} |v_{k_2}(1)|^2 \right) =$$

$$= u_{k_1} \left(|u_{k_1}(0)|\, |v_{k_2}(0)|^2 + |u_{k_1}(1)|\, |v_{k_2}(1)|^2 \right). \tag{35}$$

Hence, from (2) and (35) we have

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

$$= 2^{-t} \sum_{k_1 \in V_t} u_{k_1} \sum_{a \in \{0,1\}} |u_{k_1}(a)| \left(2^{-(m-t)} \sum_{k_2 \in V_{m-t}} |v_{k_2}(a)|^2 \right). \tag{36}$$

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

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

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

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

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

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

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

So, from the previous equality, (36), and (3) we have

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

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

This completes the proof of Lemma 1. □

The following lemma gives two upper bounds of parameter (2) for the s-function of a GOST-like cipher.

Lemma 2. *Let* $\alpha = (\alpha^{(p-1)}, \ldots, \alpha^{(0)})$, $\beta = (\beta^{(p-1)}, \ldots, \beta^{(0)})$, *and*

$$s(z) = (s^{(p-1)}(z^{(p-1)}), \ldots, s^{(0)}(z^{(0)})),\ z = (z^{(p-1)}, \ldots, z^{(0)}) \in V_m, \tag{37}$$

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

$$l^{(s)}(\alpha, \beta) \le \prod_{j=0}^{p-1} \Lambda^{(s_j)}(\alpha^{(j)}, \beta^{(j)}). \tag{38}$$

Furthermore, if $\alpha \ne 0$ *or* $\beta \ne 0$ *then*

$$l^{(s)}(\alpha, \beta) \le \Lambda(\mathfrak{T}), \tag{39}$$

where $\Lambda(\mathfrak{T})$ *is defined by (21).*

Proof. The inequality (38) follows directly from Lemma 1 and (9).

To prove (39) assume, without loss of generality that

$$l^{(s)}(\alpha, \beta) \ne 0 \tag{40}$$

and hence, $\alpha \ne 0$ and $\beta \ne 0$ (see equalities (7)). Let's define

$$i_1 = \max\left\{j \in \overline{0, p-1} : \alpha^{(j)} \ne 0\right\},\ i_2 = \max\left\{j \in \overline{0, p-1} : \beta^{(j)} \ne 0\right\}.$$

We claim that $i_1 = i_2$. Indeed, suppose that $i_1 < i_2$. Then, applying Lemma 1 to the substitutions

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

and

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

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

$$l^{(s)}(\alpha, \beta) = l^{(\psi)}(\alpha, \beta) \le \Lambda^{(\psi^{(1)})}(\alpha_1, \beta_1)\, l^{(\psi^{(2)})}(\alpha_2, \beta_2). \tag{41}$$

Since $i_1 < i_2$, it follows that

$$\alpha_2 = (\alpha^{(p-1)}, \ldots, \alpha^{(i_1+1)}) = 0,\ \beta_2 = (\beta^{(p-1)}, \ldots, \beta^{(i_1+1)}) \ne 0.$$

Thus $l^{(\psi^{(2)})}(\alpha_2, \beta_2) = 0$ and by (41) $l^{(s)}(\alpha, \beta) = 0$, which contradicts to (40). So $i_1 \ge i_2$ and by symmetry $i_1 = i_2$, which we had to prove.

To conclude the proof denote now by ψ, $\psi^{(1)}$, and $\psi^{(2)}$ the following substitutions:

$$\psi(\tilde{x}) = (s^{(i_1)}(x^{(i_1)}), \ldots, s^{(0)}(x^{(0)})),\ \tilde{x} = (x^{(i_1)}, \ldots, x^{(0)}) \in V_{(i_1+1)t},$$

$$\psi^{(1)}(x^{(i_1-1)},\dots,x^{(0)}) = (s^{(i_1-1)}(x^{(i_1-1)}),\dots,s^{(0)}(x^{(0)})),\ (x^{(i_1-1)},\dots,x^{(0)}) \in V_{i_1 t},$$
$$\psi^{(2)}(x^{(i_1)}) = s^{(i_1)}(x^{(i_1)}),\ x^{(i_1)} \in V_t.$$

Let $\tilde{\alpha} = (\alpha^{(i_1)},\dots,\alpha^{(0)})$, $\tilde{\beta} = (\beta^{(i_1)},\dots,\beta^{(0)})$. It follows directly from the condition $i_1 = i_2$, (2), and (33) that $l^{(s)}(\alpha,\beta) = l^{(\psi)}(\tilde{\alpha},\tilde{\beta})$. In addition, by Lemma 1 we have

$$l^{(\psi)}(\tilde{\alpha},\tilde{\beta}) \le \Lambda^{(\psi^{(1)})}\left((\alpha^{(i_1-1)},\dots,\alpha^{(0)}),(\beta^{(i_1-1)},\dots,\beta^{(0)})\right) l^{(\psi^{(2)})}(\alpha^{(i_1)},\beta^{(i_1)}) \le$$

$$\le l^{(\psi^{(2)})}(\alpha^{(i_1)},\beta^{(i_1)}).$$

Thus, $l^{(s)}(\alpha,\beta) \le l^{(\psi^{(2)})}(\alpha^{(i_1)},\beta^{(i_1)}) \le \Lambda(\mathfrak{T})$ (where the last inequality follows from the definition of i_1 and $\Lambda(\mathfrak{T})$). This completes the proof of Lemma 2. □

Note that in [21] a generalization of two above lemmas on the case of bilinear approximations of the function (13) is obtained.

At the end of this subsection, we give an upper bound of parameter (5) for the s-function of a GOST-like cipher.

Lemma 3. *Under the conditions of Lemma 2, the following inequalities hold:*

$$d^{(s)}(\alpha,\beta) \le \Delta(\mathfrak{T}) \tag{42}$$

if $\beta \in W$ (see formula (23)), and

$$d^{(s)}(\alpha,\beta) \le \Delta'(\mathfrak{T}) \tag{43}$$

otherwise.

Proof. Assume, without loss of generality, that $d^{(s)}(\alpha,\beta) \ne 0$ and hence, $\alpha \ne 0$, $\beta \ne 0$ (see equalities (7)). Let's define $i = \min\{j \in \overline{0,p-1} : \beta^{(j)} \ne 0\}$. For any vector $z \in V_m$ denote by z_1 and z_2 the sub-vectors of z including its least $m_1 = ti$ significant bits and its most $m_2 = m - ti$ significant bits, respectively. Denote by s_1 and s_2 the substitutions on the sets V_{m_1} and V_{m_2}, respectively such that $s(z) = (s_2(z_2), s_1(z_1))$, $z = (z_2, z_1) \in V_m$.

It follows directly from equalities $\beta_1 = 0$,

$$x \overset{m}{+} k = \left(x_1 \overset{m_1}{+} k_1\right) + 2^{m_1}\left(x_2 \overset{m_2}{+} k_2 \overset{m_2}{+} \nu(x_1,k_1)\right),\ x,k \in V_m,$$

and formula (5) that

$$d^{(s)}(\alpha,\beta) = d^{(s_2)}(\alpha_2,\beta_2) \tag{44}$$

Assume that $\beta \in W$, i.e., $i = p-1$. Since $\beta^{(p-1)} \ne 0$, we obtain from (44) and (21) that

$$d^{(s)}(\alpha,\beta) = d^{(s^{(p-1)})}(\alpha^{(p-1)},\beta^{(p-1)}) \le \Delta(\mathfrak{T}).$$

So, inequality (42) is proved.

Assume now that $\beta \notin W$. Taking into account (44), we can suppose, without loss of generality, that $i = 0 < p-1$. For any vector $z \in V_m$ let's define $z' = (z^{(p-1)}, \ldots, z^{(1)})$ and $s'(z') = (s^{(p-1)}(z^{(p-1)}), \ldots, s^{(1)}(z^{(1)}))$. We have

$$d^{(s)}(\alpha,\beta) = 2^{-t} \sum_{k^{(0)} \in V_t} \delta\left(s^{(0)}(\alpha^{(0)} + k^{(0)}) \oplus s^{(0)}(k^{(0)}), \beta^{(0)}\right) \times$$

$$\times 2^{-(m-t)} \sum_{k' \in V_{m-t}} \delta\left(s'(\alpha' + k' + \nu(\alpha^{(0)} + k^{(0)})) \oplus s'(k'), \beta'\right) =$$

$$= 2^{-t} \sum_{\substack{k^{(0)} \in V_t: \\ \nu(\alpha^{(0)} + k^{(0)}) = 0}} \delta\left(s^{(0)}(\alpha^{(0)} + k^{(0)}) \oplus s^{(0)}(k^{(0)}), \beta^{(0)}\right) d^{(s')}(\alpha', \beta') +$$

$$+ 2^{-t} \sum_{\substack{k^{(0)} \in V_t: \\ \nu(\alpha^{(0)} + k^{(0)}) = 1}} \delta\left(s^{(0)}(\alpha^{(0)} + k^{(0)}) \oplus s^{(0)}(k^{(0)}), \beta^{(0)}\right) d^{(s')}(\alpha' + 1, \beta') =$$

$$= d_0^{(s^{(0)})}(\alpha^{(0)}, \beta^{(0)})\, d^{(s')}(\alpha', \beta') + d_1^{(s^{(0)})}(\alpha^{(0)}, \beta^{(0)})\, d^{(s')}(\alpha' + 1, \beta') \le$$

$$\le \max\left\{d_0^{(s^{(0)})}(\alpha^{(0)}, \beta^{(0)}), d_1^{(s^{(0)})}(\alpha^{(0)}, \beta^{(0)})\right\} \left(d^{(s')}(\alpha', \beta') + d^{(s')}(\alpha' + 1, \beta')\right),$$

where the numbers $d_0^{(s^{(0)})}(\cdot,\cdot)$ and $d_1^{(s^{(0)})}(\cdot,\cdot)$ are defined by (6).

Thus, from the condition $\beta^{(0)} \neq 0$ and the oblivious inequality

$$d^{(s')}(\alpha', \beta') + d^{(s')}(\alpha' + 1, \beta') \le 1$$

we have $d^{(s)}(\alpha,\beta) \le \Delta'(\mathfrak{T})$. This completes the proof of inequality (43) and also of Lemma 3. □

4.2 Proof of Theorem 1

Let $\Omega = (\omega_0, \omega_1, \ldots, \omega_r)$ be an arbitrary differential characteristic of the cipher $\mathfrak{T}$. Let us define

$$MDP(\Omega) = \prod_{i=1}^{r} \left(2^{-m} \max_{x \in V_n} \left\{\sum_{k \in V_m} \delta\left(f^{(k)}(x \oplus \omega_{i-1}) \oplus f^{(k)}(x),\, \omega_i\right)\right\}\right), \qquad (45)$$

where $f^{(k)}$ $(k \in V_m)$ are defined by (12).

Let us prove some auxiliary statements.

Statement 1. *We have*

$$EDP(\Omega) \le MDP(\Omega). \qquad (46)$$

Proof. For any $x \in V_n$, $(k(1), \ldots, k(r)) \in K^r$, and $i \in \overline{1,r}$ let's define $F^{(i)} = f^{(k(i))} \circ \cdots \circ f^{(k(1))}$, $x_i \in F^{(i)}(x)$. From (14), (15) we get

$$EDP(\Omega) = |K|^{-r} \sum_{(k(1),\ldots,k(r)) \in K^r} 2^{-n} \sum_{x \in V_n} \prod_{i=1}^{r} \delta\left(F^{(i)}(x \oplus \omega_0) \oplus F^{(i)}(x),\, \omega_i\right) =$$

$$= 2^{-n} \sum_{x \in V_n} |K|^{-(r-1)} \sum_{(k(1),\ldots,k(r-1)) \in K^{r-1}} \prod_{i=1}^{r} \delta\left(F^{(i)}(x \oplus \omega_0) \oplus F^{(i)}(x),\, \omega_i\right) \times$$

$$\times 2^{-m} \sum_{k(r) \in K} \delta\left(f^{(k(r))}(x_{r-1} \oplus \omega_{r-1}) \oplus f^{(k(r))}(x_{r-1}),\, \omega_r\right). \tag{47}$$

Since

$$2^{-m} \sum_{k(r) \in K} \delta\left(f^{(k(r))}(x_{r-1} \oplus \omega_{r-1}) \oplus f^{(k(r))}(x_{r-1}),\, \omega_r\right) \leq$$

$$\leq \max_{y \in V_n} \left\{ 2^{-m} \sum_{k(r) \in K} \delta\left(f^{(k(r))}(y \oplus \omega_{r-1}) \oplus f^{(k(r))}(y),\, \omega_r\right) \right\},$$

it follows from (47) that

$$EDP(\Omega) \leq \max_{y \in V_n} \left\{ 2^{-m} \sum_{k(r) \in K} \delta\left(f^{(k(r))}(y \oplus \omega_{r-1}) \oplus f^{(k(r))}(y),\, \omega_r\right) \right\} \times$$

$$\times 2^{-n} \sum_{x \in V_n} |K|^{-(r-1)} \sum_{(k(1),\ldots,k(r-1)) \in K^{r-1}} \prod_{i=1}^{r} \delta\left(F^{(i)}(x \oplus \omega_0) \oplus F^{(i)}(x),\, \omega_i\right) =$$

$$= \max_{y \in V_n} \left\{ 2^{-m} \sum_{k \in K} \delta\left(f^{(k)}(y \oplus \omega_{r-1}) \oplus f^{(k)}(y),\, \omega_r\right) \right\} EDP(\Omega'),$$

where $\Omega' = (\omega_0, \omega_1, \ldots, \omega_{r-1})$. Thus, the inequality (46) follows from the above expressions by induction. □

Let us remark that the inequality (46) holds for any block cipher $\mathfrak{T}$ with the encryption function (11). Moreover, this inequality turns into equality if (11) is a Markov cipher.

The following statement is similar to the one known for Markov Feistel ciphers [7].

Statement 2. *Suppose that*

$$MDP(\Omega) \neq 0. \tag{48}$$

Then there exists a sequence $\alpha_0, \alpha_1, \ldots, \alpha_{r+1} \in V_m$ *such that* $\omega_i = (\alpha_i, \alpha_{i+1})$, $i \in \overline{0, r}$, *and*

$$MDP(\Omega) = \prod_{i \in N(\Omega)} \max_{x \in V_m} \left\{ D_x^{(s)}(\alpha_i, A^{-1}(\alpha_{i-1} \oplus \alpha_{i+1})) \right\}, \tag{49}$$

where s *is the s-function of the cipher* $\mathfrak{T}$, $D_x^{(s)}(\cdot, \cdot)$ *is defined by (4), and*

$$N(\Omega) = \{i \in \overline{1, r} : \alpha_i \neq 0\}. \tag{50}$$

In addition, the following inequality holds:

$$|N(\Omega)| \geq \left\lceil \frac{2r}{3} \right\rceil. \tag{51}$$

Proof. Let $\omega_i = (\alpha_i, \beta_i)$, where $\alpha_i, \beta_i \in V_m$, $i \in \overline{0,r}$. Let's define $\alpha_{r+1} = \beta_r$. Using (4), (12), and (13) it is easy to check that $\beta_i = \alpha_{i+1}$ for all $i \in \overline{0,r}$, and

$$\sum_{k \in V_m} \delta\left(f^{(k)}(x \oplus \omega_{i-1}) \oplus f^{(k)}(x),\, \omega_i\right) = D^{(s)}_{x_2}\left(\alpha_i,\, A^{-1}(\alpha_{i-1} \oplus \alpha_{i+1})\right) \tag{52}$$

for any $x = (x_1, x_2)$, where $x_1, x_2 \in V_m$. The equality (49) follows directly from (45), (48), (50), and (52).

To prove the inequality (51) let us define $N_0(\Omega) = \overline{1,r} \setminus N(\Omega)$ and prove that for all $i \in \overline{1,r}$

$$\begin{aligned}(i \in N_0(\Omega)) \Rightarrow (((i+1 \le r) \Rightarrow (i+1 \in N(\Omega))) \,\&\\ \&\,((i+2 \le r) \Rightarrow (i+2 \in N(\Omega)))).\end{aligned} \tag{53}$$

Then $|N_0(\Omega)| \le \left\lceil \frac{r}{3} \right\rceil$ and hence, (51) is true.

Let us prove the implication (53). Let $i \in \overline{1,r}$ and $\alpha_i = 0$. It follows from (48), (49) that $\alpha_{i-1} \oplus \alpha_{i+1} = 0$. Next, since $\omega_i = (\alpha_i, \alpha_{i+1}) \ne (0,0)$, we have $\alpha_{i+1} \ne 0$ and hence,$\alpha_{i+2} = \alpha_i \oplus \alpha_{i+2} \ne 0$ (in the opposite case we have

$$\max_{x \in V_m}\left\{D^{(s)}_x\left(\alpha_{i+1},\, A^{-1}(\alpha_i \oplus \alpha_{i+2})\right)\right\} = 0,$$

and hence, $MDP(\Omega) = 0$). Thus, (53) and so also Statement 2, are proved. □

Now, let us prove the last auxiliary statement in this subsection. Recall that the group W is defined by (23).

Statement 3. *Under the conditions of Statement 2, for any $i \in N(\Omega)$ the following statements hold:*

1) $A^{-1}(\alpha_{i-1} \oplus \alpha_{i+1}) \in W$ if and only if $\alpha_i \in W$;

2) if $A^{-1}(\alpha_{i-1} \oplus \alpha_{i+1}) \in W$ then

$$\max_{x \in V_m}\left\{D^{(s)}_x\left(\alpha_i,\, A^{-1}(\alpha_{i-1} \oplus \alpha_{i+1})\right)\right\} \le \Delta(\mathfrak{T}); \tag{54}$$

3) if $A^{-1}(\alpha_{i-1} \oplus \alpha_{i+1}) \notin W$ then

$$\max_{x \in V_m}\left\{D^{(s)}_x\left(\alpha_i,\, A^{-1}(\alpha_{i-1} \oplus \alpha_{i+1})\right)\right\} \le \Delta'(\mathfrak{T}). \tag{55}$$

Proof. Let $\alpha = \alpha_i$, $\beta = A^{-1}(\alpha_{i-1} \oplus \alpha_{i+1})$. Observe that, since $i \in N(\Omega)$, we have $\alpha \ne 0$ and hence, by (4), (48), and (49), $\beta \ne 0$.

Let us prove the statement 1). It follows from (4), (48), and (49) that there exist $x, k \in V_m$ such that

$$s((x \oplus \alpha) + k) \oplus s(x + k) = \beta \tag{56}$$

Let's consider the mapping

$$\tau(z) = \tau((z^{(p-1)}, z^{(p-2)}, \ldots, z^{(0)})) = (0, z^{(p-2)}, \ldots, z^{(0)}),\ z^{(i)} \in V_t,\ j = \overline{0, p-1}.$$

Observe that for any $x, y \in V_m$

$$\tau(x) = \tau(y) \Leftrightarrow x - y \in W,\ \tau(s(x)) = \tau(s(y)) \Leftrightarrow \tau(x) = \tau(y).$$

Thus, it follows from (56) that

$$\beta \in W \Leftrightarrow \tau(\beta) = 0 \Leftrightarrow \tau(s(x \oplus \alpha) + k) = \tau(s(x + k)) \Leftrightarrow$$

$$\Leftrightarrow \tau((x \oplus \alpha) + k - x - k) = 0 \Leftrightarrow \tau(x) \oplus \tau(\alpha) = \tau(x) \Leftrightarrow \tau(\alpha) = 0 \Leftrightarrow \alpha \in W,$$

which we had to prove.

Let's prove the statements 2) and 3). By (4), we have

$$\max_{x \in V_m} \left\{ D_x^{(s)}(\alpha, \beta) \right\} = 2^{-m} \max_{x \in V_m} \left\{ \sum_{k \in V_m} \delta \left(s((x \oplus \alpha) + k) \oplus s(x + k), \beta \right) \right\} =$$

$$= 2^{-m} \max_{x \in V_m} \left\{ \sum_{k \in V_m} \delta \left(s(((x \oplus \alpha) - x) + k) \oplus s(k), \beta \right) \right\} \leq$$

$$\leq 2^{-m} \max_{x \in V_m} \left\{ \sum_{k \in V_m} \delta \left(s(x + k) \oplus s(k), \beta \right) \right\}.$$

Hence, by (5),

$$\max_{x \in V_m} \left\{ D_x^{(s)}(\alpha, \beta) \right\} \leq \max_{x \in V_m} \left\{ d^{(s)}(x, \beta) \right\}.$$

Now, to conclude the proof of 2) and 3) we have to use Lemma 3. □

We continue the proof of Theorem 1. Observe that from (5), (6), (19), and (20) we get

$$\Delta'(\mathfrak{T}) \leq \Delta(\mathfrak{T}). \tag{57}$$

Thus, the inequality (25) follows directly from (46), (51), and (54).

To conclude the proof it is sufficient to show that, under the condition (26), for any differential characteristic Ω such that $MDP(\Omega) \neq 0$ the following inequality holds:

$$MDP(\Omega) \leq \max \left\{ \Delta(\mathfrak{T})^{r-1},\ \Delta(\mathfrak{T})^{r+1-2\left\lceil \frac{r}{3} \right\rceil} \Delta'(\mathfrak{T})^{\left\lceil \frac{r}{3} \right\rceil} \right\}. \tag{58}$$

Let us define

$$n_1 = \left| \{ i \in N(\Omega) : \alpha_i \in W \} \right|,\ n_2 = \left| \{ i \in N(\Omega) : \alpha_i \notin W \} \right|,\ n_0 = r - n_1 - n_2, \tag{59}$$

where $N(\Omega)$ is defined by (50). It follows from (49) and Statement 3 that

$$MDP(\Omega) \leq \left(\Delta'(\mathfrak{T}) \right)^{n_2} \left(\Delta(\mathfrak{T}) \right)^{n_1}. \tag{60}$$

In addition, by (51) and (59), we have

$$n_1 \geq 0, n_2 \geq 0, n_1 + n_2 \leq r, n_1 + n_2 \geq r - \left\lceil \frac{r}{3} \right\rceil. \tag{61}$$

Let us prove the following inequality:

$$n_1 + 2n_2 \geq r - 1. \tag{62}$$

Observe that for any $i \in \overline{1, r-1}$

$$(\alpha_i = 0) \Rightarrow ((\alpha_{i+1} \notin W) \vee (\alpha_{i+2} \notin W)). \tag{63}$$

Indeed, if $\alpha_i = 0$ then, by (48) and (49), we have $\alpha_{i+1} \neq 0$, $\alpha_{i+2} \neq 0$. Therefore, by the statement 1) of Statement 3 the assumption $\alpha_{i+1}, \alpha_{i+2} \in W$ implies that $\alpha_{i+2} \in W \setminus \{0\}$ and $A^{-1}\alpha_{i+2} = A^{-1}(\alpha_i \oplus \alpha_{i+2}) \in W$ that contradicts to (26). Thus, the implication (63) is true. Hence, we have $n_2 \geq n_0 - 1$ that is equivalent to (62).

Let's denote by (v_1, v_2) the maximum point of the linear function $n_1 \ln \Delta(\mathfrak{T}) + n_2 \ln \Delta'(\mathfrak{T})$ of variables n_1 and n_2 that satisfy the system of inequalities (61), (62). Since the logarithmic function is monotone, (v_1, v_2) is also a maximum point of the expression in the right-hand side of (60). Observe that all solutions (n_1, n_2) of the inequalities (61) and (62) form a five-angle with the vertices

$$(r, 0), (0, r), (r-1, 0), \left(0, r - \left\lceil \frac{r}{3} \right\rceil\right), \left(r - 2\left\lceil \frac{r}{3} \right\rceil + 1, \left\lceil \frac{r}{3} \right\rceil\right) \tag{64}$$

So, (v_1, v_2) coincides with one of the points (64). From this using (57) and (60) it is easy to obtain (27). This completes the proof of inequality (27) and also of Theorem 1.

4.3 Proof of Theorem 2

Let $\Omega = (\omega_0, \omega_1, \ldots, \omega_r)$ be an arbitrary linear characteristic of the cipher $\mathfrak{T}$. Let us assume, without loss of generality, that

$$ELP(\Omega) \neq 0 \tag{65}$$

and prove that

$$ELP(\Omega) \leq \Lambda(\mathfrak{T})^{\left[\frac{2r}{3}\right]}, \tag{66}$$

where $\Lambda(\mathfrak{T})$ is defined by (21).

We use the following statement, which can be proved in the same way as Statement 2.

Statement 4. *Under the condition (65), there exists a sequence of m-dimensional Boolean vectors $\beta_0, \beta_1, \ldots, \beta_{r+1}$ such that $\omega_i = (\beta_{i+1}, \beta_i)$, $i \in \overline{0, r}$, and*

$$ELP(\Omega) = \prod_{i \in N(\Omega)} l^{(s)}(\beta_{i-1} \oplus \beta_{i+1},\ \beta_i A), \tag{67}$$

where s is the s-function of the cipher $\mathfrak{T}$ and

$$N(\Omega) = \{i \in \overline{1, r} : \beta_i \neq 0\}.$$

In addition, the following inequality holds:

$$|N(\Omega)| \geq \left\lceil \frac{2r}{3} \right\rceil. \tag{68}$$

Now, applying (39) to each factor of (67) we obtain (66) from (68). This proves the inequality (28).

Let us prove (29) and (30). Let's write the vectors $\beta_0, \beta_1, \ldots, \beta_{r+1}$ in the form $\beta_i = (\beta_{i,p-1}, \ldots, \beta_{i,0})$, where $\beta_{i,j} \in V_t$, $i \in \overline{0, r+1}$, $j \in \overline{0, p-1}$. Similarly, let's write the matrix A in the form $A = (A_{p-1}, \ldots, A_0)$, where A_j is $m \times t$-sub-matrix of the matrix A that contains the columns of A with the numbers tj, $tj+1, \ldots$, $tj+t-1$, $j \in \overline{0, p-1}$ (it is assumed that the columns of the matrix A are numbered from left to right, beginning from the null). Let us define

$$V = \left\{(i,j) \in \overline{1,r} \times \overline{0,p-1} : (\beta_{i-1,j} \oplus \beta_{i+1,j},\ \beta_i A_j) \neq (0,0)\right\}. \tag{69}$$

It follows from (67) and (38) that

$$ELP(\Omega) \leq \prod_{i=1}^{r} \prod_{j=0}^{p-1} \Lambda^{(s^{(j)})}(\beta_{i-1,j} \oplus \beta_{i+1,j},\ \beta_i A_j).$$

Hence, by (22) and (69), we have

$$ELP(\Omega) \leq (\Lambda_{\mathfrak{T}})^{|V|}. \tag{70}$$

Moreover, by the definition of the set V,

$$|V| \geq \sum_{i=1}^{r} \max\left\{|\{j \in \overline{0,p-1} : \beta_{i-1,j} \oplus \beta_{i+1,j} \neq 0\}|, |\{j \in \overline{0,p-1} : \beta_i A_j \neq 0\}|\right\} =$$

$$= \sum_{i=1}^{r} \max\left\{wt(\beta_{i-1} \oplus \beta_{i+1}), wt(\beta_i A)\right\}. \tag{71}$$

Now let us obtain a lower bound of the sum (71). Let us group it's terms in the groups of four successive terms and show that the sum of the numbers in each group is not less than the branch number of A. Without loss of generality, let us consider the first group:

$$S = \sum_{i=1}^{4} \max\left\{wt(\beta_{i-1} \oplus \beta_{i+1}), wt(\beta_i A)\right\}.$$

It follows from the condition $\omega_i \neq 0$, $i \in \overline{0,r}$ that $\beta_1 \oplus \beta_3 \neq 0$ or $\beta_2 \oplus \beta_4 \neq 0$. In the first case we get

$$S \geq wt(\beta_1 A) \oplus wt(\beta_1 \oplus \beta_3) \oplus wt(\beta_3 A) \geq wt((\beta_1 \oplus \beta_3)A) \oplus wt(\beta_1 \oplus \beta_3) \geq B_A,$$

and in the second case

$$S \geq wt(\beta_2 A) \oplus wt(\beta_2 \oplus \beta_4) \oplus wt(\beta_4 A) \geq wt((\beta_2 \oplus \beta_4)A) \oplus wt(\beta_2 \oplus \beta_4) \geq B_A.$$

Thus, by (71), we have $|V| \geq \left[\frac{r}{4}\right] B_A$. The inequality (30) follows directly from this bound, (70) and (13).

To prove the inequality (29) let's obtain another bound for $|V|$. Let's define $N_0 = \{i \in \overline{1,r} : \beta_i = 0\}$. By (65), for any $i \in N_0$ such that $i \le r-1$ we have $\beta_{i+1} \ne 0$ and $\beta_{i+2} \ne 0$. Thus, if $i \in N_0$, $i \le r-1$ then

$$\sum_{j=i}^{i+2} \max\{wt(\beta_{j-1} \oplus \beta_{j+1}), wt(\beta_j A)\} \ge wt(\beta_{j+2}) \oplus wt(\beta_{j+2}A) \ge B_A. \tag{72}$$

In addition, it follows from (68) that

$$|N_0| \le \left\lceil \frac{r}{3} \right\rceil. \tag{73}$$

Let's define

$$V_0 = \bigcup_{i \in N_0} \{i, i+1, i+2\},\ V_1 = \{1, 2, \ldots, r\} \setminus V_0.$$

By the definition of the set N_0, (72), and (73), we have

$$|V| \ge \sum_{i=1}^{r} \max\{wt(\beta_{i-1} \oplus \beta_{i+1}), wt(\beta_i A)\} = \sum_{i \in V_0} \max\{wt(\beta_{i-1} \oplus \beta_{i+1}), wt(\beta_i A)\} +$$

$$+ \sum_{i \in V_1} \max\{wt(\beta_{i-1} \oplus \beta_{i+1}), wt(\beta_i A)\} \ge |N_0| B_A + (r - 3|N_0|) = r + |N_0|(B_A - 3).$$

Thus, if $B_A = 3$ we obtain that $|V| \ge r$. The inequality (29) follows directly from the last bound, (70) and (13).

This completes the proof of Theorem 2.

5 Application, discussion, and further research

Let us apple the obtained results to practical security evaluation against differential and linear cryptanalysis for the cipher GOST (with independent and equiprobable random round keys). For any $s \in S^{V_t}$ let's define

$$d^{(s)} = \max\left\{ 2^{-t} \sum_{k \in V_t} \delta\left(s(k+\alpha) \oplus s(k),\, \beta\right) : \alpha, \beta \in V_t \setminus \{0\} \right\}, \tag{74}$$

$$d'^{(s)} = \max\left\{ 2^{-t} \sum_{\substack{k \in V_t: \\ \nu(\alpha,k)=a}} \delta\left(s(k+\alpha) \oplus s(k),\, \beta\right) : \alpha, \beta \in V_t \setminus \{0\},\, a \in \{0,1\} \right\}, \tag{75}$$

$$l^{(s)} = \max\left\{ 2^{-t} \sum_{k \in V_t} \left(2^{-t} \sum_{x \in V_t} (-1)^{\beta s(x+k) \oplus \alpha x} \right)^2 : \alpha, \beta \in V_t \setminus \{0\} \right\}. \tag{76}$$

Recall that in (74) – (76) $\delta(\cdot,\cdot)$ is the Kronecker delta, $+$ denote the addition modulo 2^t, and $\nu(\alpha,k)$ is the carry bit into the t-th digit in the sum of α and k in the ring $\mathbb{Z}$ (see Subsection 2.1).

It is easy to check that the matrix A used in the round function of GOST (i.e., the matrix corresponded to the left cyclic shift to 11 positions on the set V_{32}) satisfies the condition (26), and $B_A = 2$. Hence, we obtain from (27), (28) that (for $r = 32$)

$$M_D(\mathfrak{T}) \le \max\left\{(\Delta\cdot\Delta')^{11},\, \Delta^{31}\right\},\ M_L(\mathfrak{T}) \le \Lambda^{21}, \tag{77}$$

where

$$\Delta = \max\left\{d^{(s^{(j)})} : j \in \overline{0,7}\right\}, \Delta' = \max\left\{d'^{(s^{(j)})} : j \in \overline{0,7}\right\},$$

$$\Lambda = \max\left\{l^{(s^{(j)})} : j \in \overline{0,7}\right\},$$

The inequalities (77) allow to estimate the maximum average differential and linear characteristic probabilities of the cipher GOST directly from the values (74) – (76) computed for s-boxes $s^{(j)}$ ($j \in \overline{0,7}$) of this cipher. The computation of these values for 10000 random s-boxes shows that more than 6500, 5700, and 4500 of them take their values (74), (75), and (76), respectively, in the interval [0.250, 0.299), see Table 1.

Table 1: The distributions of the parameters (74), (75), (76) for 4×4 s-boxes (a sample of 10000 substitutions)

The interval of values, I	The number of substitutions $s \in S^{V_8}$ such that			The interval of values, I	The number of substitutions $s \in S^{V_8}$ such that		
	$l^{(s)} \in I$	$d^{(s)} \in I$	$d'^{(s)} \in I$		$l^{(s)} \in I$	$d^{(s)} \in I$	$d'^{(s)} \in I$
0.000 – 0.049	0	0	0	0.500 – 0.549	41	332	1
0.050 – 0.099	0	0	0	0.550 – 0.599	1419	0	0
0.100 – 0.149	0	0	55	0.600 – 0.650	0	23	0
0.150 – 0.199	0	237	4514	0.650 – 0.699	0	0	0
0.200 – 0.249	0	0	0	0.700 – 0.749	0	0	0
0.250 – 0.299	6522	5725	4532	0.750 – 0.799	0	4	0
0.300 – 0.349	1842	1361	832	0.800 – 0.849	0	0	0
0.350 – 0.399	157	2306	63	0.850 – 0.899	0	0	0
0.400 – 0.449	0	12	3	0.900 – 0.949	0	0	0
0.450 – 0.499	0	0	0	0.950 – 1.000	19	0	0

Moreover, there exists a large set of s-boxes such that all three values (74), (75), and (76) are small. For example, if

$$s^{(0)} = \ldots = s^{(7)} = (1\ 2\ 7\ 10\ 3\ 4\ 11\ 14\ 6\ 15\ 5\ 9\ 8\ 12\ 13\ 0)$$

then $\Delta = 0.1875$, $\Delta' = 0.1250$, and $\Lambda = 0.2500$. In this case, by (77), we obtain the following bounds:

$$M_D(\mathfrak{T}) \le 2^{-59.57}, M_L(\mathfrak{T}) \le 2^{-42}.$$

Note that the last bounds didn't allow us to make any conclusions about the provable security of GOST against differential and linear cryptanalysis. But, as far as we know, they are the best estimates of practical security of GOST obtained by an accurate mathematical proof.

In Tables 2, 3, and 4 the distributions of the parameters (74), (75), and (76) are given, obtained for 2000 random substitutions from the symmetric group S^{V_8}. In this case, there exist also quite a lot of substitutions such that all three parameters (74) – (76) are rather small (for example, $l^{(s)} = 0.0295, d^{(s)} = 0.0234, d'^{(s)} = 0.0195$). But, during our calculations we did not find out any substitution $s \in S^{V_4}$ such that $l^{(s)} < 0.250$ and also any substitution $s \in S^{V_8}$ such that $l^{(s)} < 0.021$.

Table 2: The distribution of the parameter (74) for 8×8 s-boxes (a sample of 2000 substitutions)

The value, i	The number of substitutions $s \in S^{V_8}$ such that $d^{(s)} = i$
0.02343750	90
0.02734375	826
0.03125000	937
0.03515625	56
0.03906250	86
0.04687500	5

Table 3: The distribution of the parameter (75) for 8×8 s-boxes (a sample of 2000 substitutions)

The value, i	The number of substitutions $s \in S^{V_8}$ such that $d'^{(s)} = i$
0.01953125	6
0.02343750	965
0.02734375	868
0.03125000	148
0.03515625	11
0.03906250	1
0.04296875	1

In Tables 5, 6 the values of the upper bounds for parameters (17) and (18), calculated for a 32-round GOST-like cipher with the block size $n = 64$, are given. As we see from the tables, increasing the size of s-boxes or of the branch number B_A leads to essential decreasing of mentioned values.

Note that the bounds (25) and (28) don't depend on the branch number of the matrix. Moreover, as computer calculations show, the parameter $\Lambda_{\mathfrak{T}}$ in formulas (29), (30) does not depend on the s-boxes and tends to $1/3$ as $t \to \infty$. In this connection,

Table 4: The distribution of the parameter (76) for 8×8 s-boxes (a sample of 2000 substitutions)

The interval of values, I	The number of substitutions $s \in S^{V_8}$ such that $l^{(s)} \in I$
0.021411896 – 0.029510498	84
0.029541016 – 0.029541016	333
0.029663086 – 0.034942627	196
0.035156250 – 0.035156250	548
0.035278320 – 0.041168213	98
0.0412597660 – 0.0412597660	398
0.0413513180 – 0.0459060670	14
0.0478515631 – 0.0478515631	211
0.0484619140 – 0.0976562500	118

Table 5: The estimations of practical security of GOST-like ciphers against differential cryptanalysis

Parameters of the round function of a GOST-like cipher $\mathfrak{T}$ $(n = 64, r = 32)$			Upper bounds of $M_D(\mathfrak{T})$ computed	
t	$\Delta(\mathfrak{T})$	$\Delta'(\mathfrak{T})$	by (25)	by (27)
4	0.1875	0.1250	$2^{-50.72}$	$2^{-59.57}$
8	0.0234	0.0195	$2^{-113.76}$	$2^{-122.08}$

Table 6: The estimations of practical security of GOST-like ciphers against linear cryptanalysis

Parameters of the round function of a GOST-like cipher $\mathfrak{T}$ $(n = 64, r = 32)$				Upper bounds of $M_L(\mathfrak{T})$ computed	
t	$\Lambda(\mathfrak{T})$	$\Lambda_{\mathfrak{T}}$	B_A	by (28)	by (30)
4	0.2500	0.3359	9	2^{-42}	$2^{-113.32}$
8	0.0295	0.3333	5	$2^{-106.75}$	$2^{-63.40}$

an important problem is to strengthen the obtained bounds. Note that, in the case of linear cryptanalysis, an undesirable property of parameter $\Lambda^{(g)}$ (see formula (3)) causes essential difficulty. Namely, in contrast to the parameters (2) and (5), the value of $\Lambda^{(g)}(\alpha, \beta)$ can be not equal to null if $\alpha = 0$ and $\beta \neq 0$ (or vice versa). This property leads to difficulties in extension of the well-known active s-boxes counting technique developed for Marcov ciphers on the class of GOST-ciphers [7], [20], [23], [24]. Next a problem that seems even more difficult is to find non-trivial estimates of provable security for GOST-like ciphers against differential and linear cryptanalysis, by analogy with the methods developed for Marcov ciphers [25], [26].

At the conclusion, let us remark that some results of this paper can be generalized

on a wider class of group operations used in round transformations of block ciphers, and also on a wider class of attacks. More information about this can be found in [19], [21], [22] and bibliography given there.

Acknowledgment

The authors wold like to thank Victor Bezditny, Sergey Pal'chenko, and Artur Shevtsov for their help in obtaining the numerical results described in Section 5.

References

[1] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems", *Journal of Cryptology*, **4**, No. 1, pp. 3-72, 1991.

[2] M. Matsui, "Linear cryptanalysis methods for DES cipher", *Advances in Cryptology* – EUROCRYPT'93, LNCS **765**, pp. 386-397, Springer-Verlag, 1994.

[3] X. Lai, J.L. Massey, and S. Murphy, "Markov ciphers and differential cryptanalysis", *Advances in Cryptology* – EUROCRYPT'91, LNCS **547**, pp. 17-38, Springer-Verlag, 1991.

[4] A. Biryukov, "Block ciphers and stream ciphers: the state of the art", *Cryptology ePrint Archive*, Report **2010/232**, http://eprint.iacr.org/2004/094.

[5] S. Vaudenay, "Decorrelation: a theory for block cipher security", *Journal of Cryptology*, **16**, No. 4, pp. 249-286, 2003.

[6] J. Daemen J and V. Rijmen, "Statistics of correlation and differentials in block ciphers", *Cryptology ePrint Archive*, Report **2005/212**, http://eprint.iacr.org/2005/212.

[7] M. Kanda, "Practical security evaluation against differential and linear cryptanalysis for Feistel ciphers with SPN round function", *Selected Areas in Cryptography*, SAC 2000, LNCS **2012**, pp. 324-338, Springer-Verlag, 2001.

[8] GOST 28147-89. Information processing systems. Cryptographic protection. Algorithm for cryptographic transformation, Gosstandart SSSR, Moscow, 1989 [in Russian].

[9] C. Charnes, L. O'Connor, J. Pieprzyk, R. Safavi-Naini, and Y. Zhang, "Comments on soviet encryption algorithm", *Advaces in Cryptology* – EUROCRYPT'94, LNCS **950**, pp. 433-438, Springer-Verlag, 1995.

[10] C. Charnes, L. O'Connor, J. Pieprzyk, R. Safavi-Naini, and Y. Zhang, "Further comments on soviet encryption algorithm", Preprint 94-9, Department of Computer Science, The University of Wollongong, 1994.

[11] B. Schneier. "Applied cryptography", New York: John Wiley & Sons, 1996, pp. 331-334.

[12] H. Seki and T. Kaneko, "Differential cryptanalysis of reduced round of GOST", *Selected Areas in Cryptography*, SAC 2000, LNCS **2012**, pp. 315-323, Springer-Verlag, 2001.

[13] V.V. Shorin, V.V. Jelezniakov, and E.M. Gabidulin, "Linear and differential cryptanalysis of Russian GOST", Univ. Bielefeld, SFB 343 Diskrete Strukturen in der Mathematik, 2001. – Preprint., available from ftp.uni-bielefeld.de.

[14] N.T. Courtois, "Security evaluation of GOST 28147-89 in view of international standardization", *Cryptology ePrint Archive*, Report **2011/211**, http://eprint.iacr.org/2011/211.

[15] N.T. Courtois and M. Misztal, "Differential crytanalysis of GOST", *Cryptology ePrint Archive*, Report **2011/312**, http://eprint.iacr.org/2011/312.

[16] O. Staffelbach and W. Meier, "Cryptographic significance of the carry for ciphers based on integer addition", *Advances in Cryptology* – CRYPTO'90, LNCS **537**, pp. 601-615, Springer-Verlag, 1991.

[17] A.N. Alekseychuk and L.V. Kovalchuk, "Upper bounds of maximum values of average differential and linear characteristic probabilities of Feistel cipher with adder modulo 2^m", *Theory of Stochastic Processes*, **12**(28), Nos. 1-2, pp. 20-32, 2006.

[18] A.N. Alekseychuk, L.V. Kovalchuk, and S.V. Pal'chenko,"Cryptographic parameters of s-boxes that characterize the security of GOST-like block ciphers against linear and differential cryptanalysis", *Zakhist Inform.*, No. 2, pp. 12-23, 2007 [in Ukrainian].

[19] L.V. Kovalchuk, "Generalized Markov ciphers: evaluation of practical security against differential cryptanalysis", in: Proc. 5th All-Russian Sci. Conf. "Mathematics and Safety of Information Technologies" (MaBIT-06), 25-27 Oct. 2006, MGU, Moscow, pp. 595-599, 2006 [in Russian].

[20] M. Kanda, Y. Takashima, T. Matsumoto, K. Aoki, and K. Otha, "A strategy for constructing fast round functions with practical security against differential and linear cryptanalysis", *Selected Areas in Cryptography*, SAC 1998, LNCS **1556**, pp. 264-279, Springer-Verlag, 1999.

[21] A.N. Alekseychuk and A.S. Shevtsov, "Upper estimates of imbalance of bilinear approximations for round functions of block ciphers", *Cybernetics and Systems Analysis*, **46**, No. 3, pp. 376-385, 2010.

[22] L.V. Kovalchuk, "Upper-bound estimation of the average probabilities of integer-valued differentials in the composition of key adder, substitution block and shift operator", *Cybernetics and Systems Analysis*, **46**, No. 6, pp. 936-944, 2010.

[23] L.R. Knudsen, "Practically secure Feistel ciphers", *Fast Software Encryption*, FSE'94, LNCS **809**, pp. 211-221, Springer-Verlag, 1994.

[24] S. Vaudenay, "On the security of CS-cipher", *Fast Software Encryption*, FSE'99, LNCS **1636**, pp. 260-274, Springer-Verlag, 1999.

[25] L. Keliher, "Toward provable security against differential and linear cryptanalysis for Camellia and related ciphers", *International Journal of Network Security*, **5**, No. 2, pp. 167-175, 2007.

[26] S. Hong, S. Lee, J. Lim, J. Sung, D. Cheon, and I. Cho, "Provable security against differential and linear cryptanalysis for the SPN structure", *Fast Software Encryption*, FSE'00, LNCS **1978**, pp. 273-283, Springer-Verlag, 2000.

[27] J. Daemen, "Cipher and hash function design-strategies based on linear and differential cryptanalysis", Katholieke Univ. Leuven, Doctoral Dissertation, 1995.