Differential Analysis of Non-Markov Ciphers

RUSLAN SKURATOVSKII
National Aviation University, Kiev, UKRAINE.
Interregional Academy of Personnel Management Kiev, UKRAINE.
and Igor Sikorsky Kiev Polytechnic Institute, av. Pobedy 37, UKRAINE.
[0000-0002-5692-6123]

Abstract: - In this article, for Markov ciphers, we prove that they are resistant to differential cryptanalysis and some statements made for MS are obtained. The upper estimates of the probabilities of integer differentials are significantly improved when compared to previously known results. Our differential cryptanalytic algorithm finds weak subkeys that have more than 80 bits and 128 bits for 128-bit keys.

Keywords: - Circuits for Cryptograhy, Systems Theory for Cryptography, Computational modeling, difference cryptanalysis, block ciphers, difference equations, Markov ciphers, non-Markov ciphers, generalized Markov ciphers, integer differential, construction of upper bounds for probabilities, differential cryptanalysis.

Received: March 26, 2022. Revised: November 28, 2022. Accepted: December 15, 2022. Published: February 7, 2023.

1. Introduction

We obtain an analytical estimation of the upper boundary of the Feistel-like block ciphers differential probabilities, resistance characteristics of unbalanced Feistel circuits to differential and linear cryptanalysis. Further, a formalized description and method of study of non-Markov symmetric block ciphers resistance to differential cryptanalysis are developed. New schemes of cascade block encryption are investigated and, in this case, we develop a method is used for evaluate the stability non-Markov ciphers. The estimates of *R*-block encryption schemes resistance to differential cryptanalysis are obtained. In addition, the crypto stability of the national standard of symmetric encryption GOST 28147: 2009 to fault attacks is considered. We both consider and compare different cryptanalysis methods [1].

2. Work Related Analysis

Differential cryptanalysis was proposed by Israeli experts Eli Biham and Adi Shamir to break cryptosystems like DES [2]. Differential cryptanalysis was further developed in the works of such well-known cryptanalysts as V. Rudnitsky, R. Berdibayev, R. Breus, N. Lada, and M. Pustovit, [3] and one of most new result is [4]. We have made this ranking a typical cipher according to the degree of susceptibility by the method of cryptanalysis. In papers of Howard M. Heys [5, 6, 7] the key dependency of differentials in block ciphers was investigated by examining the results of numerous experiments applied to the substitution-permutation network (SPN) [8,9] structure using 4-bit S-boxes.

3. Methods of Research

The focus of the research is block ciphers [11, 12] with a round function of the form

$$G_K(x) = L_m(S(x \oplus k_i)),$$

where k_i is a round key. These ciphers are considered from the view of their belonging to the class of Markov or the generalized Markov.

The subject of the research is the study of the above ciphers by the method of difference analysis, finding their properties, constructing estimates of the probabilities of integer differentials for round functions of the form that was mentioned earlier, processing and systematizing results.

The research methods are the construction of a model which is used to describe the concepts or statements that are being analyzed.

In discrete systems, both input and output signals are discrete signals. The variables in the discrete systems vary with time. In this type of system, the changes are predominantly discontinuous. The state of variables in discrete system changes only at a discrete set of points in time. Note that by a discrete system we mean a technical device or program that transforms a discrete sequence $x(n)$ into a discrete sequence $y(n)$ according to the determined algorithm. The algorithm for transforming the input sequence $x\ n$ to the output sequence $y(n)$ is described by the relation

$$R_y\left[y(n)\right] = R_x\left[x(n)\right],$$

where R_x and R_y are operators. Considering the type of operator, discrete systems can be divided into:

- linear or non-linear,
- stationary or non-stationary,
- physically realizable (causal) or unrealizable (non-causal).

Linearity. A discrete system is called **linear** if and only if its operator R satisfies additivity and homogeneity properties, namely if:

1. $R[x_1(n) + x_2(n)] = R[x_1(n)] + R[x_2(n)]$ for any $x_1(n)$ and $x_2(n)$, and

2. $R[a\times x(n)]=a\times R\left[x(n)\right]$,
$R[\alpha x(n)]=\alpha R\left[x(n)\right]$ for any α and $x(n)$.

These properties may be expressed as the single condition

$$R[a\times x_1(n)+b\times x_2(n)]=a\times R[x_1(n)]+b\times R[x_2(n)].$$

Note that the last condition implies the reaction of a linear system to a complex action is equal to the sum of reactions to individual actions taken with the same coefficients α and β.

Definition of Stationarity. A discrete system is called **stationary** (invariant in time) if its parameters do not change in time. In this case, the action applied to the input of the system will always lead to the same reaction, regardless of when the action is applied.

We introduce the notation

$$M=(\mu_0,...,\mu_r),$$

where $\mu_i : G\times G\to G$ with commutative group operations on the group G, $\mu_i(a,b)=a\circ_i b$, $a,b\in G$ and $i=\overline{0,...,r}$.

The magnitude of the input differences ω_0 and ω_1 are the differences which appear in the first and second rounds, correspondently.

Definition 3.1. The generalized differential characteristic (GDC) of cipher (1.1) is the sequence

$$(\Omega, M)=\Big((\omega_0,\mu_0),(\omega_1,\mu_1),\ldots,(\omega_{r+1},\mu_{r+1})\Big),$$

where $\omega_i\in G\setminus\{0_i\}$ and $i=\overline{0,...,r}$ [2].

4. Main Result

We denote by V_m the m-dimentional vector space.

For the Data Encryption Standard (DES) algorithm it is known [3, 10] that after finding 48-bits of the key [3,11] of the last round, the remaining 8-bits are found via a complete search. The following condition is necessary for a successful application of an attack by the RK method:

$$\exists\Delta x,\Delta y\in V_m\,\forall K\in(V_n)^2\,\forall x\in V_m:$$
$$P(E_K^{(r-1)}(x\oplus\Delta x)\oplus E_K^{(r-1)}(x)=\Delta y)=p,$$

where $p>>2^{-m}$ and the probability is taken for $x\in V_m$.

To describe the essence of the RK method, we make use of the following notation. Let the encrypting key $E_K(x)$ be a function determined by the equality

$$E_K(x)=E(K,x), \qquad (1)$$

where $x\in V_m$, $K\in(V_n)^r$, $K=(k_1,...,k_r)$, $k_i\in V_n$, $E_K(x)$ is the r-th block cipher and for any $K\in(V_n)^r$ display E_K, where $V_m\to V_m$ is a bijection.

Denote by

$$f_k(x)=f(k,x),\ x\in V_m,\ k\in V_n \qquad (2)$$

where $f_k : V_m\to V_m$ is the round function of the cipher E. Then, using our notation, we have that

$$E_K(x)=f_{k_r}\circ f_{k_{r-1}}\circ\ldots\circ f_{k_1}(x) \qquad (3)$$

holds, where $k_1,...,k_r$ is a sequence of round keys and r is number of rounds.

In addition, for $l=\overline{1,n}$, let

$$E_K^{(l)}(x)=f_{k_l}\circ f_{k_{l-1}}\circ\ldots\circ f_{k_1}(x). \qquad (4)$$

The definitions of the Markov cipher (MC) were given for the first time in the work [11].

Definition 4.1. (from [11]). The cipher is Markov if

$$P(\Delta Y=\beta\,|\,\Delta X=\alpha,\ X=Z) \qquad (5)$$

does not depend on Z, provided the subkeys are randomly distributed.

If the cipher is Markov, then ΔY then almost all of them are the same, they do not change with a change in the subkeys Z so the dependence cannot be established. This makes them resistant to Differential Cryptoanalysis.

Using our notation, where for convenience we set γ from Z and then the definition has the form

$$P(f_k(\gamma\oplus\alpha)\oplus f_k(\gamma)=\beta)=$$
$$=2^{-n}\sum_{k\in V_m}\delta(f_k(\gamma\oplus\alpha)\oplus f_k(\gamma),\beta). \qquad (6)$$

It is worth emphasizing that this probability does not depend on γ. If instead the probability did depend on γ, then the cipher is a non-Markov cipher. The γ in (6) can consequently be treated as an arbitrary element with V_m and, if $\gamma=0$ then we obtain the expression

$$2^{-n}\sum_{k\in V_m}\delta(f_k(\alpha)\oplus f_k(0),\beta).$$

The definition of MC can in such case be rewritten as follows.

Definition 4.2. A block G cipher [12, 13] with round function $f_k : V_n\to V_m, k\in V_n,$ is MC if

$$\forall \alpha, \beta \in V_m : 2^{-n} \sum_{k \in V_m} \delta(f_k(\gamma \oplus \alpha) \oplus f_k(\gamma), \beta) =$$
$$= 2^{-n} \sum_{k \in V_m} \delta(f_k(\alpha) \oplus f_k(0), \beta).$$

Corollary. If the cipher is Markovian, then ΔY then almost all of them are the same, they do not change with a change in the subkeys so the dependence cannot be established. This makes them resistant to Differential Cryptoanalysis. We check the possibility of a differential attack on AES and show the dependence of number of differetials in table 2.1.

Table 2.1. Dependence of the number of zero differentials depending on the round number.

Number of rounds	Number of Differentials
2	56180
3	12780
4	880
5	0
6	0
7	0
8	0
9	0

This means we get better method even in [10-13].

5. Generalized Markov Ciphers

Suppose that some mapping $f: V_n \times G \to G$ is given such that for each $k \in V_n$, the mapping $f(k,x) := f_k(x)$ is a bijection on G. We will associate the set M_x of matrices of dimension $|G| \times |G|$, $x \in G$ with this mapping. The elements of the matrix M_x are $a^x_{\alpha,\beta} \in [0,1]$, $\alpha, \beta \in G$, where $a^x_{\alpha,\beta} \in [0,1] = d^f_{\mu_1,\mu_2}(x;\alpha,\beta)$. It is assumed here that some linear order is fixed on a group G [25, 26]. If $G = V_m$, then the bit-vectors naturally correspond to the integers from 0 to $2^m - 1$. We denote by P the set of substitution matrices of dimension $|G| \times |G|$.

Definition 5.1. The mapping $f: V_n \times G \to G$ will be called a generalized Markov mapping (relative to operations μ_1, μ_2) if $\forall x, x' \in G$ and $\exists \pi, \pi' \in \mathrm{P}$ such that

$$\pi_x \cdot M_x = \pi'_{x'} \cdot M_{x'}, \qquad (7)$$

where multiplication is standard usual matrix multiplication and, in this case, is reduced to permutation of rows of the matrices M_x and M_y.

Definition 5.2. A block cipher E will be called a generalized Markov cipher (GMC) in restricted sense if their round functions $f_k(x) = f_k(k,x)$, $x \in V_m$, $k \in V_n$ are generalized Markov mappings (GMM) f_1, f_2 with corresponding operations μ_0, μ_1.

Proposition 5.3 (property of GMC). For a GMC f, using our notation, the equation is

$$\forall \beta \in G \quad \max_{\substack{x, \alpha \in V_n \\ \alpha \neq 0}} d^f_{\mu_1,\mu_2}(x;\alpha,\beta) = \max_{\substack{\alpha \in V_n \\ \alpha \neq 0}} d^f_{\mu_1,\mu_2}(0;\alpha,\beta).$$

The proof of this Lemma follows directly from the definition of GMC, namely since the columns of M_x and M_0 and the number β differ only by some permutation of their elements. In particular, the maximum element in the columns of M_x and M_0 is the same, as stated above.

Remark 5.4. *If $G = V_m$, $\mu_1 = \mu_2 = XOR$, $\pi = \pi' = Id$ and $\forall x, x' \in G$, then the definition coincides with the classical definition of Markov BC (see e.g. [10]).*

Note that Proposition 5.3 is equivalent to stating $\forall i = \overline{1,r}$ and $\forall x \in G \ \exists \sigma_{x,\mu_{i-1}}$, i.e. a permutation on G, such that $\forall \alpha, \beta \in G$ we have

$$d^f_{\mu_{i-1},\mu_i}(x;\alpha,\beta) = d^f_{\mu_{i-1},\mu_i}(0_{i-1};\sigma_{x,\mu_i}(\alpha),\beta) \qquad (8)$$

In particular, if $\mu_{i-1} = \mu_i = \mu$, then

$$d^f(x;\alpha,\beta) = d^f(0;\sigma_x(\alpha),\beta). \qquad (9)$$

The following Theorem demonstrates the performance of the GMC for some estimates like those previously obtained for the MC [16, 22, 23].

Theorem 5.5. For any GMC (with respect to operations μ_i), the following statements hold:

1. $\forall x, \omega' \in G$,
$\max_{\omega \in G} d^f_{\mu_{i-1},\mu_i}(x;\omega,\omega') = \max_{\omega \in G} d^f_{\mu_{i-1},\mu_i}(0;\omega,\omega')$,
$\forall i = \overline{1,r}$. (10)

2. $\forall x, \omega' \in G$,
$\max_{\omega \in G} d^f_{\mu_{i-1},\mu_i}(\omega,\omega') \le \max_{\omega \in G} d^f_{\mu_{i-1},\mu_i}(x;\omega,\omega') =$
$= \max_{\omega \in G} d^f_{\mu_{i-1},\mu_i}(0;\omega,\omega')$, $\forall i = \overline{1,r}$. (11)

3. $EDP(\Omega, M) \le \prod_{i=1}^{r} \max_{\omega \in G} d^f_{\mu_{i-1},\mu_i}(0;\omega,\omega_i)$. (12)

4. $\max_{\Omega} EDP(\Omega, M) \le \prod_{i=1}^{r} \max_{\substack{\omega,\omega' \in G \\ \omega' \neq 0_i}} d^f_{\mu_{i-1},\mu_i}(0;\omega,\omega')$. (13)

Proof: Firstly, (12) follows directly from the definition of GMC and by applying Proposition 5.3 since

$$\max_{\omega \in G} d^f_{\mu_{i-1},\mu_i}(x;\omega,\omega') = \max_{\omega_0} d^f_{\mu_{i-1},\mu_i}(0;\omega_0,\omega'),$$

where $\omega_0 = \sigma_{x,\mu_{i-1}}(\omega)$ for $x \in G$ and $i = \overline{1,r}$.

Next, note that (13) follows from (12) because

$$\max_{\omega \in G} d^f_{\mu_{i-1},\mu_i}(\omega,\omega') = \max_{\omega \in G} \frac{1}{|G|} \sum_{x \in G} d^f_{\mu_{i-1},\mu_i}(x;\omega,\omega') \le$$

$$\le \frac{1}{|G|} \sum_{x \in G} \max_{\omega \in G} d^f_{\mu_{i-1},\mu_i}(x;\omega,\omega') = \max_{\omega \in G} d^f_{\mu_{i-1},\mu_i}(0;\omega,\omega')$$

holds. Finally, (12) follows from item 1 of Proposition 5.3 and then (13) is a consequence (12), which concludes the proof.

5 Non-Markov ciphers and Examples

Two examples of non-Markov ciphers are the old GOST 211428 and the new Belarusian BelT 34.101.31-2007. So Differential Cryptanalysis can be applied to them.

At the current time, the general theory of evaluating the practical stability of Markov ciphers with respect to difference (or linear) cryptanalysis has been developed, where some of the fundamental works in this direction are [9, 10, 11, 12]. As a rule, when constructing estimates, several consequences of formula (17) are used, namely

$$\max_{\Omega} EDP(\Omega) \le \max_{\Omega_1} EDP(\Omega_1) \max_{\Omega_2} EDP(\Omega_2), \qquad (14)$$

where $\Omega = (\Omega_1, \Omega_2)$ and

$$\max_{\Omega} EDP(\Omega) \le (\max_{\omega_1,\omega_2 \ne 0} d^f(\omega_1,\omega_2))^r. \qquad (15)$$

Similarly, we have

$$\max_{\Omega} EDP(\Omega) \le \max_{\Omega} p_s^{\#\Omega}, \qquad (16)$$

where $\#\Omega$ is minimum possible number of active *S*-boxes in Ω, $p_s = \max_{s \in S} \max_{\omega_1,\omega_2} d^s(\omega_1,\omega_2)$, where *S* is the set of S-blocks of the cipher [5-7] (if its round function is a composition of linear transformations and a block of substitutions. As for non-Markov BC [19- 21], the property of Theorem 1 for them does not hold, which makes it difficult to obtain estimates of the form (1) - (3) by analogous methods. Instead, when constructing analogues of these estimates, it is necessary to consider the dependence in (7) on *x*.

Statement 5.1. (about the estimate for non-Markov block ciphers). For the value *EDP(Ω, M)* the following inequalities hold:

$$EDP(\Omega,M) \le \prod_{i=1}^{r} \max_{x \in G} d^f_{\mu_{i-1},\mu_i}(x;\omega_{i-1},\omega_i), \qquad (17)$$

$$\max_{\Omega,M} EDP(\Omega,M) \le \prod_{i=1}^{r} \max_{x \in G} \max_{\substack{\omega_{i-1},\omega_i \\ \omega_{i-1} \ne 0_{i-1} \\ \omega_i \ne 0_i}} d^f_{\mu_{i-1},\mu_i}(x;\omega_{i-1},\omega_i). \qquad (18)$$

Proof: For simplicity, we instead prove (17) for the two-round characteristic

$$(\Omega,M) = ((\omega_0,\mu_0),(\omega_1,\mu_1),(\omega_2,\mu_2))$$

and then deduce (18) as a direct consequence of (17). Note

$$EDP(\Omega,M) = \frac{1}{|G|} \sum_{x_0 \in G} d^f_{\mu_1,\mu_2}(x_0;\omega_1,\omega_2) d^f_{\mu_2,\mu_3}(x_1;\omega_2,\omega_3),$$

where $x_1 = f_{k_1}(x_0)$, $k_1 \in V_n$ is key of first round, then

$$EDP(\Omega,M) \le$$

$$\le \frac{1}{|G|} \sum_{x_0 \in G} \max_{x \in G} d^f_{\mu_1,\mu_2}(x;\omega_1,\omega_2) \cdot \max_{x \in G} d^f_{\mu_2,\mu_3}(x;\omega_2,\omega_3) =$$

$$= \max_{x \in G} d^f_{\mu_1,\mu_2}(x;\omega_1,\omega_2) \cdot \max_{x \in G} d^f_{\mu_2,\mu_3}(x;\omega_2,\omega_3),$$

which concludes the proof.

It is worth noting that the presence of an additional parameter $x \in G$ in (17) and (18) significantly complicates the construction of numerous estimates and, at the same time, makes the estimates obtained rougher, which in some cases may become trivial. Because of this one cannot generally use this approach in practice.

6. Construction of Upper Estimates for the Probabilities of the Integer Differential of the Round Functions Module 2

6.1 Conventions and approval

Firstly, let us introduce some notation. For any $n \in N$, let $V_n = \{0,1\}^n$ an array of n-dimensional vectors. If $n = pu, p \ge 2$ then $\forall x \in V_n$ we can represent such an x as $x = (x^{(p)},...,x^{(1)}), x^{(1)} \in V_u, i = \overline{1,p}$.

Denote by $L_m : V_n \to V_n$ the mapping which produces a left shift by m-bits of the vector V_n. On the set V_n, we define the following subsets:

$$\Gamma_m(\gamma) = \{\beta \in V_n \mid \exists k \in V_n : L_m(k \oplus \gamma) - L_m(k) = \beta\};$$

$$\Gamma^{-1}_m(\beta) = \{\gamma \in V_n \mid \exists k \in V_n : L_m(k \oplus \gamma) - L_m(k) = \beta\};$$

then a bijective mapping $S : V_n \to V_n$ is defined

$$\forall x \in V_n : S(x) = (S^{(p)}(x^{(p)}),...,S^{(1)}(x^{(1)}), x^{(i)} \in V_u, i = \overline{1,p}.$$

We also denote by

$$\tilde{x} = (x^{(p)},...,x^{(2)}) \in V_{n-u}; \tilde{S} : V_{n-u} \to V_{n-u},$$

where $S(x) = (S^{(p)}(x^{(p)}),...,S^{(2)}(x^{(2)}))$.

Further, we introduce

$$\tau(k,\alpha) = \begin{cases} 0, \ if \ S^{(1)}\left(k \oplus \alpha\right) \geq S^{(1)}(k), \\ 1, \ else; \end{cases}.$$

Let $\Delta^{(1)}_{\oplus+} = \max\limits_{\alpha,\gamma \in V_n \setminus \{0\}} \max\{I_1, I_2\} =$

$$= \max_{\alpha,\gamma \in V_n \setminus \{0\}} \max\{2^{-u} \sum_{k^{(1)} \in V_u : \tau(k^{(1)},\alpha^{(1)})=0} \delta(S^{(1)}(k^{(1)} \oplus$$

$$\oplus \alpha^{(1)}) - S^{(1)}(k^{(1)}), \gamma_j^{(1)}), 2^{-u} \sum_{k^{(1)} \in V_u : \tau(k^{(1)},\alpha^{(1)})=1} \delta(S^{(1)}(k^{(1)} \oplus$$

$$\oplus \alpha^{(1)}) - S^{(1)}(k^{(1)}), \gamma_j^{(1)})\}$$

and, in addition, for any $\beta \in V_n$ with

$$\beta = q \cdot 2^m + r, \ 0 \leq q < 2^t - 1, \ 0 \leq r < 2^m - 1$$

we introduce the following notation to work with elements of the set $\Gamma_m^{-1}(\beta)$:

$$\gamma_1 = \gamma_1(\beta) = \beta \cdot 2^t + q, \ \gamma_2 = \gamma_2(\beta) = \gamma_1 + 1,$$
$$\gamma_3 = \gamma_3(\beta) = \gamma_1 - 2^t, \ \gamma_4 = \gamma_4(\beta) = \gamma_1 - 2^t + 1$$

$\forall j = \overline{1,p}$ and assuming that

$d^{S^{(j)}}_{\oplus+} = \max\limits_{\alpha,\beta \in V_n \setminus \{0\}} 2^{-u} \sum \delta(S^{(j)}(k \oplus \alpha) - S^{(j)}(k), \beta)$.

then $\Delta_{\oplus+} = \max\limits_{i=1,p} d^{S^{(j)}}_{\oplus+}$.

Finally, we will use round functions, which are the composition of a key adder, a substitution block and a shift operator with form

$$G_k(x) = L_m(S(x \oplus k_i)). \qquad (19)$$

6.2 Berson's result

When obtaining further results, we will use the main result, which we reformulate here using our notation in a more convenient form. Using our notation, the following holds.

Theorem 6.1. For any $m \in N, \ \gamma \in V_n, \ \gamma = q \cdot 2^t + r,$ with $0 \leq r < 2^t - 1,$ we have

$\Gamma_m(\gamma) \subset \{\beta, \ \beta + 1, \ \beta - 2^m, \beta - 2^m + 1\},$

with $\beta = q + r \cdot 2^m$ and all operations are performed $\bmod 2^n$.

7 Construction of upper bounds for the probabilities of integer differentials of round functions

Theorem 7.1. Let $t \geq u, p \geq 2$. If the round function has the form (19) as in [15], then the inequality

$$\forall \alpha, \beta \in V_n \setminus \{0\} : d^G_{\oplus+}(\alpha,\beta) \leq \max\{2\Delta_{\oplus+}, 4\Delta^{(1)}_{\oplus+}\}$$

holds.

Proof: Average probabilities of integer round differentials for functions of the form (3.1) have form

$$d^G_+(x;\alpha;\beta) = 2^{-n} \sum_{k \in V_n} \delta(L_m(S((x+\alpha) \oplus k)) - \\ - L_m(S(x \oplus k)), \beta). \qquad (20)$$

Examples of such probabilities for cipher Threefish we have in table 3.1. It is the mean (behind the keys) probability of the differential of the mapping at the point x

$$d^G_+(\alpha;\beta) = 2^{-2n} \sum_{x,k \in V_n} \delta(L_m(S((x+\alpha) \oplus k)) - \\ - L_m(S(x \oplus k)), \beta). \qquad (21)$$

Let $\mu(x;\alpha) = (x+\alpha) \oplus x \oplus \alpha$, then

$$d^G_+(x;\alpha;\beta) = 2^{-n} \sum_{k \in V_n} \delta(L_m(S((x+\alpha) \oplus k)) - \\ - L_m(S(x \oplus k)), \beta) = 2^{-n} \sum_{k \in V_n} \delta(L_m(S(x \oplus \alpha \oplus k \oplus \mu(x;\alpha)))).$$

Let us introduce further notation to simplify, namely

$$x \oplus k = k'; \alpha \oplus \mu(x;\alpha) = \alpha' = \alpha'(x;\alpha); k = k'.$$

We then write our expression using the new notation as

$$d^G_+(x;\alpha;\beta) = 2^{-n} \sum_{k \in V_n} \delta(L_m(S(\alpha' \oplus k)) - L_m(S(k), \beta)) = \\ = d^G_{\oplus+}(0;\alpha;\beta).$$

So, we deduce that

$$\max_{\alpha \in V_n \setminus \{0\}} d^G_+(x;\alpha;\beta) = \max_{\alpha' \in V_n \setminus \{0\}} d^G_{\oplus+}(0;\alpha;\beta).$$

hence $d^S_{\oplus+} \leq d^{S^{(i)}}_{\oplus+}$, which concludes the proof.

Table. 3.1 The value of the upper limits of the probability of the appearance of zero differentials depending on the number of the round

Round number	The value of the upper limit of the probability of differentials
2	2^{-21}
3	$2^{-33.1689}$
4	$2^{-33.1689}$
5	$2^{-33.1689}$
6	$2^{-33.1689}$
7	$2^{-33.1689}$
8	$2^{-33.169-}$
9	$2^{-33.1690}$

Remark 6.2. Theorem 6.1 admits generalization to the case of several subsets $\{1,...,k\}$ and several G'.

The national standard for block ciphering GOST 28147-89 is UMC in a broad sense is related to the bitwise addition operation. Indeed, in this case with $G = V_{64}$ and $G' = V_{32}$,

$$d^f(x;\alpha,\beta) = \psi(\alpha,\beta)d^{\phi}(x';\alpha',\beta'),$$

where $\psi(\alpha,\beta) = \delta(\alpha_2,\beta_1)$, $x'(x) = x_2$, $\alpha'(\alpha,\beta) = \alpha_2$, ϕ_k is a round transformation, which is a generalized Markov mapping (see e.g. [16, 17, 18, 19, 23]).

7. Conclusion

An upper estimate of the probability of integer differential of round functions has been found. This result can be implemented for analysis of crypto stability of block cipher in relation to round crypto analysis. Note that our method and bounds can be extended on stream ciphers [21].

References

[1] Susan K Langford and Martin E Hellman. “Differential-linear cryptoanalisis”. In: *Annual International Cryptology Conference.* Springer, Berlin, Heidelberg, 1994, pp. 17-25.

[2] Biham E., Shamir A. Differential cryptoanalysis of DES-like cryptosystems. — 1990. — P. 7.

[3] Coppersmith, Don. The Data Encryption Standard (DES) and its strength against attacks (англ.) // IBM Journal of Research and Development (англ.)рус. : journal. — 1994. — May (vol. 38, no. 3). — P. 243. — doi:10.1147/rd.383.0243.

[4] V. Rudnitsky, R. Berdibayev, R. Breus, N. Lada, and M. Pustovit, “Synthesis of reverse two-bit dual-operated strictly straight cryptographic coding on the basis of another operation”, Advanced Information Systems, vol. 3, no. 4, pp. 109–114, Dec. 2019.

[5] H.M. Heys, "Key Dependency of Differentials: Experiments in the Differential Cryptanalysis of Block Ciphers Using Small S-boxes", Cryptology ePrint Archive, Report 2020/1349, International Association of Cryptologic Research, available at https://eprint.iacr.org, 2020.

[6] H. Liao and H.M. Heys, "An Integrated Hardware Platform for Four Different Lightweight Ciphers", Proceedings of IEEE Canadian Conference on Electrical and Computer Engineering (CCECE 2015), Halifax, Nova Scotia, May 2015. (Also presented at NECEC 2014.)

[7] C. Wang and H.M. Heys, "Performance Characterization of AES Datapath Architecture in 90-nm Standard Cell CMOS Technology", Journal of Signal Processing Systems, Springer, vol. 75, no. 3, pp. 217-231, Jun. 2014.

[8] Debdeep Mukhopadhyay. “An improved fault based attack of the advanced encryption standard”. In: *International Conference on Cryptography in Africa.* Springer, Heidelberg, 2009, pp. 421-434.

[9] Michael Tunstall and Debdeep Mukhopadhyay. “Differential fault analysis of the advanced encryption standard using a single fault”. In: *IFIP international workshop on information security and practices.* Springer, Berlin, Heidelberg, 2009, pp. 224-233.

[10] X. Zhang, H.M. Heys, and C. Li, "FPGA Implementation and Energy Cost Analysis of Two Lightweight Involutional Block Ciphers Targeted to Wireless Sensor Networks", Mobile Networks and Applications (MONET) Journal, ACM/Springer, vol. 18, no. 2, pp. 222-234, Apr. 2013.

[11] NIST FIPS Pub. “197: Advanced encryption standard (AES)”. In: *Federal information processing standards* 197.441 (2001).

[12] Ruslan Skuratovskii. “An Application of Metacyclic and Miller-Moreno *p*-Groups to Generalization of Diffie-Hellman Protocol”. In: *Proceedings of the Future Technologies Conference.* Springer, 2020, pp. 869–876.

[13] Xuejia Lai and James L. Massey. “Markov Ciphers and Differential Cryptanalysis”. In: *Workshop on the Theory and Application of Cryptographic Techniques.* Springer, Berlin, Heidelberg, 1991, pp. 17-38.

[14] Xuejia Lai and James L Massey. “A Proposal for a New Block Encryption Standard”. In: *Workshop on the Theory and Application of Cryptographic Techniques.* Springer, Berlin, Heidelberg, 1991, pp. 389-404.

[15] Joan Daemen and Vincent Rijmen. “Statistics of correlation and differentials in block ciphers”. In: *IACR ePrint archive 212* (2005).

[16] Eli Biham and Adi Shamir. “Differential Fault Analysis of Secret Key Cryptosystems”. In: *Annual international cryptology conference.* Springer, Berlin, Heidelberg, 1997, pp. 513-525.

[17] Tomas A Berson. “Differential cryptanalysis mod 2^32 with applications to MD5”. In: *Advances in Cryptography - EUROCRYPT '92, Workshop on the Theory of Application of Cryptographic Techniques.* Lecture Notes in Computer Science 658, Springer, Berlin, Heidelberg, 1992, pp. 71-80.

[18] Andrey Bogdanov, Christina Boura, Vincent Rijmen, Meiqin Wang, Long Wen and Jingyan Zhao. “Key difference invariant bias in block ciphers”. In: *International Conference on the Theory and Application of Crytography and Information Security.* Springer, Berlin, Heidelberg, 2013, pp. 357-376.

[19] Christof Beierle, Jérémy Jean, Stefan Kölbl, Gregor Leander, Amir Moradi, Thomas Peyrin, Yu Sasaki, Pascal Sasdrich and Siang Meng Sim. “The SKINNY family of block ciphers and its low-latency variant MANTIS”. In: *Annual International Cryptography Conference.* Springer, Berlin, Heidelberg, 2016, pp. 123-153.

[20] Roberto Avanzi. “The QARMA block cipher family. Almost MDS matrices over rings with zero divisors, nearly symmetric even-mansour constructions with non-involutory central rounds, and search heuristics for low-latency S-boxes”. In: *IACR Transactions on Symmetric Cryptology* (2017), pp. 4-44.

[21] Available at www.springerlink.com: Eli Biham, Orr Dunkelman Differential Cryptanalysis of Stream Ciphers. Paper 2007,

[22] Ruslan Skuratovskii, Yevgen Osadchyy and Volodymyr Osadchyy. “The timer compression of data and information”. In: *2020 IEEE Third Conference on Data Stream Mining and Processing (DSMP).* IEEE, 2020, p. 455-459.

[23] Ruslan Skuratovskii. “Employment of minimal generating sets and structure of sylow 2-subgroups alternating groups in block ciphers”. In: *Advances in Computer Communication and Computational Sciences.* Springer, Singapore, 2019, pp. 351-364

[24] Ruslan Skuratovskii and Aled Williams. “Irreducible bases and subgroups of a wreath product in applying to diffeomorphism groups acting on the Möbius band”. In: *Rendiconti del Circolo Mathematico di Palermo Series 2* 70.2 (2021), pp. 721-739.

[25] Ruslan Skuratovskii. “A method for fast timer coding of texts”. In: *Cybernetrics and Systems Analysis* 49.1 (2013) pp. 133-138.

[26] Ruslan Skuratovskii, Volodymyr Osadchyy and Yevgen Osadchyy. “The timer inremental compression of data and information”. In: *WSEAS Transactions on Mathematics* 19 (2020), pp. 398-406.

[27] Anna V Iatsyshyn, Valeriia O Kovach, Yevhen O Romanenkoa and Andrii V Iatsyshyn. "Cloud services application ways for preparation of PhD". In: *CEUR Workshop Proceedings* (2019), pp. 197-216.

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

The authors equally contributed in the present research, at all stages from the formulation of the problem to the final findings and solution.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

No funding was received for conducting this study.

Conflict of Interest

The authors have no conflicts of interest to declare that are relevant to the content of this article.