computing@computingonline.net
www.computingonline.net

Print ISSN 1727-6209
On-line ISSN 2312-5381
International Journal of Computing

STUDIES ON PRACTICAL CRYPTOGRAPHIC SECURITY ANALYSIS FOR BLOCK CIPHERS WITH RANDOM SUBSTITUTIONS

Berik Akhmetov [1)], Sergiy Gnatyuk [1,2)], Vasyl Kinzeryavyy [2)], Khalicha Yubuzova [3)]

[1)] Yessenov University, Aktau, Kazakhstan, berik.akhmetov@yu.edu.kz
[2)] National Aviation University, Kyiv, Ukraine, s.gnatyuk@nau.edu.ua, v.kinzeryavyy@gmail.com
[3)] Satbayev University, Almaty, Kazakhstan, hali4a@mail.ru

Paper history:
Received 2 October 2019
Received in revised form 20 April 2020
Accepted 24 April 2020
Available online 14 June 2020

Keywords:
cryptology;
block cipher;
linear cryptanalysis;
differential cryptanalysis;
security verification;
random substitutions;
practical security.

Abstract: In up-to-date information and communication systems (ICS) cryptography is used for ensuring data confidentiality. The symmetric block ciphers (BC) are implemented in different ICS including critical applications. Today theory of analysis and security verification of BC with fixed substitution nodes against linear and differential cryptanalysis (LDC) is developed. There are also BC with substitution nodes defined by round keys. Random substitution nodes improve security of ciphers and complicate its cryptanalysis. But through it all, quantitative assessment is an actual and not simple task as well as the derivation of formulas for practical security verification for BC with random substitution nodes against LDC. In this paper analytical upper bounds of parameters characterized practical security of BC with random substitution nodes against LDC were given. These assessments generalize known analogs on BC with random substitution nodes and give a possibility to verify security improving against LDC. By using the example of BC Kalyna-128, it was shown that the use of random substitution nodes allows improving upper bounds of linear and differential parameters average probabilities in 2^{46} and 2^{90} times respectively. The study is novel as it is one of the few in the cryptology field to calculate analytical upper bounds of BC practical security against LDC methods as well as to show and prove that using random substitutions allows improving upper bounds of linear and differential parameters. The security analysis using quantitative parameters gives possibility to evaluate various BCs or other cryptographic algorithms and their ability to provide necessary and sufficient security level in ICS. A future research study can be directed on improving analytical upper bounds for analyzed LDC in context to practical security against LDC, as well as practical cryptographic security assessment for other BC with random substitutions against LDC and other cryptanalysis methods including quantum cryptanalysis (Shor, Grover, Deutsch-Jozsa algorithms).

1. INTRODUCTION

In modern information and communication systems (ICS) the most popular and effective methods for confidentiality (privacy) ensuring is symmetric cipher using. The symmetric block ciphers (BC) are implemented in different ICS including critical applications. The BCs are deterministic algorithms operating on fixed-length groups of bits (blocks), each BC consists of two related (paired) algorithms – one for data encryption and the other for ciphertext decryption. The most of BCs are vulnerable to linear and differential cryptanalysis (LDC) [1-3] and this theory is developed as well as BC practical security verification [4-6]. Linear cryptanalysis based on finding affine approximations to the action of a cipher [3]. Differential cryptanalysis (in the case of BC) refers to a set of techniques for tracing differences through the network of transformation, discovering where the cipher exhibits non-random behavior and exploiting such properties to recover the secret key [1, 2].

2. ANALYSIS OF RELATED WORKS

Many BCs during encryption use few different substitution tables with apriori fixed order of using (e.g., former Soviet encryption standard GOST 28147-89, modern Ukrainian encryption standard Kalyna, etc.). In research studies [7-9] authors have given analytical upper bounds of parameters characterized practical security of mentioned algorithms [10, 11] against LDC methods. There are also block ciphers with substitution nodes defined by round keys, for example ADE algorithm [12]. Logically, random substitutions using complicates BC cryptanalysis, but its quantitative assessment is hard task. From these considerations, the derivation of formulas for practical security verification for BC with random substitution nodes against linear and differential cryptanalysis is actual scientific task. The solving of this task will allow quantitative assessment of similar BC efficiency.

3. PROBLEM STATEMENT

In the paper [7] analytical upper bounds of average probabilities for linear and differential parameters of BC designed by Kalyna-128 scheme. Let us show the efficiency of random substitution nodes (the source of randomness can be true random as well as pseudo random) using for cipher designed by Kalyna-128 scheme with the additional round key in each round that influences on substitution tables choosing. Let us take a closer look at r-round BC $\mathfrak{I}$ with random substitutions nodes, a set of plain (cipher) texts $V_n = \{0,1\}^n$, a set of round keys $K = V_{n+q}$ and family of encryption transformation

$$F_k = f_{r,k_r} \circ \ldots \circ f_{1,k_1},\ k = (k_1, \ldots, k_r) \in K^r, \quad (1)$$

where $r = 2r' + 1$, $n = pt$, $q = pq'$, $p = 4p'$, t, p', r', q' are natural numbers, parameter $b = 2^{q'}$ defines quantity of different substitution tables, used in BC.

Round transformation $f_{i,k}(x)$ for any $x \in V_n$, $k \in K$, $i \in \overline{1, r}$ describes as follows

$$f_{i,k}(x) = \begin{cases} \varphi\left(x \oplus k^{(1)}, k^{(2)}\right), & \textit{if } \mathrm{i} \equiv 1 (\mathrm{mod} 2),\ i < r \\ \varphi\left(x \overset{\circ}{+} k^{(1)}, k^{(2)}\right), & \textit{if } \mathrm{i} \equiv 0 (\mathrm{mod} 2),\ i < r \\ s\left(x \oplus k^{(1)}, k^{(2)}\right), & \textit{if } \mathrm{i} = \mathrm{r} \end{cases}, \quad (2)$$

where $k^{(1)}$ and $k^{(2)}$ are parts of round key

$$k \ \left(k = \left(k^{(1)}, k^{(2)}\right),\ k^{(1)} \in V_n,\ k^{(2)} \in V_q\right).$$

Substitutions φ and s are defined by formulas (3) – (4):

$$\varphi(x, y) = s(x, y) M,\ x \in V_n,\ y \in V_q, \quad (3)$$

$$s(x, y) = \left(\mathrm{s}_{y_{p-1}}\left(x_{p-1}\right), \ldots, s_{y_0}\left(x_0\right)\right),$$

$$x = \left(x_{p-1}, \ldots, x_0\right), y = \left(y_{p-1}, \ldots, y_0\right), \quad (4)$$

where $x_j \in V_t$, $y_j \in V_{q'}$, s_{y_j} is substitution on the set V_t (by the index y_j is chosen one substitution table from possible b), $j \in \overline{0, p-1}$, M is invertible $p \times p$-matrix over the field $\mathrm{GF}\left(2^t\right)$, multiplication $s(x, y)$ and M in formula (3) performed over this field with binary vectors unification $s_{y_j}\left(x_j\right)$ with its elements.

In the formula (2) symbols "$\oplus$" and "$\overset{\circ}{+}$" are compatible with operations of coordinatewise adding for binary vectors with length n and following the algebraic operation

$$x \overset{\circ}{+} k = \left(x^{(1)} + k^{(1)}, \ldots, x^{(4)} + k^{(4)}\right), \quad (5)$$

where $x = \left(x^{(1)}, \ldots, x^{(4)}\right)$, $k = \left(k^{(1)}, \ldots, k^{(4)}\right)$, $x^{(v)}, k^{(v)} \in V_{tp'}$, $v \in \overline{1,4}$, and "$+$" is the symbol of addition mod $2^{tp'}$ operation on the set $V_{tp'}$.

As a reminder, the probability of differential parameter $\Omega = \left(\omega_0, \omega_1, \ldots, \omega_r\right) \in \left(V_n \setminus \{0\}\right)^{r+1}$ for BC $\mathfrak{I}$ with encryption key $(k_1, \ldots, k_r)$ is defined by following formula [13]:

$$DP^{(k_1,\ldots,k_r)}(\Omega) = \mathrm{P}\left(\bigcap_{i=1}^{r}\left\{X_i \oplus X_i' = \omega_i\right\} \mid X \oplus X' = \omega_0\right), \quad (6)$$

where X X' are independent random equiprobable binary vectors with length n:

$$X_i = \left(f_{i,k_i} \circ \ldots \circ f_{1,k_1}\right)(X),$$

$$X_i' = \left(f_{i,k_i} \circ \ldots \circ f_{1,k_1}\right)(X'),\ i \in \overline{1, r}.$$

The average value (6) for all $(k_1, \ldots, k_r) \in K^r$ is called the average probability of differential parameter Ω *(EDP)* and it can be defined by following formula [13]:

$$EDP(\Omega) = |K|^{-r} \sum_{(k_1,\dots,k_r)\in K^r} DP^{(k_1,\dots,k_r)}(\Omega). \quad (7)$$

Also, in accordance with [13, 14], the average probability of linear parameter $\Omega = (\omega_0, \omega_1, \dots, \omega_r)$ *(ELP)* for BC $\Im$ is defined by formula (8):

$$ELP(\Omega) = \prod_{i=1}^{r} l^{(i)}(\omega_{i-1}, \omega_i), \quad (8)$$

where for any $\alpha, \beta \in V_n$, $i \in \overline{1, r}$

$$l^{(i)}(\alpha, \beta) = 2^{-(n+q)} \sum_{k\in V_{n+q}} \left(2^{-n} \sum_{x\in V_n} (-1)^{\alpha x \oplus \beta f_{i,k}(x)} \right)^2. \quad (9)$$

Therefore, *the main target of this study* is practical cryptographic security assessment for BC with random substitution nodes (described by (1) – (5) formulas) against LDC methods by the derivation of analytical upper bounds of parameters (7) – (8). Target achieving will define the novelty of this work and show the efficiency of random substitution nodes using in BCs as well as it will prove that using random substitutions allows improving upper bounds of linear and differential parameters (and as a consequence improving practical security against LDC methods). Moreover, the security analysis using quantitative parameters will give possibility to evaluate various BCs (or other cryptographic algorithms) and their ability to provide necessary and sufficient security level in ICS.

4. UPPER BOUNDS OF DIFFERENTIAL PARAMETERS AVERAGE PROBABILITIES

As a reminder in accordance with [7] for any differential parameter Ω of BC $\Im$ with family of encryption transformation (1) following inequation is performed:

$$EDP(\Omega) \le \prod_{i=1}^{r} \max_{x\in V_n} d_x^{(i)}(\omega_{i-1}, \omega_i), \quad (10)$$

where for any $x, \alpha, \beta \in V_n$, $i \in \overline{1, r}$

$$d_x^{(i)}(\alpha, \beta) = |K|^{-1} \sum_{k\in K} \delta\left(f_{i,k}(x \oplus \alpha) \oplus f_{i,k}(x), \beta\right). \quad (11)$$

Let us consider BC $\Im$, described by formulas (1) – (5). From the viewpoint of round key for this BC described by equation $k = \left(k^{(1)}, k^{(2)}\right)$, $k^{(1)} \in V_n$, $k^{(2)} \in V_q$, let us transform (11) in the following manner

$$d_x^{(i)}(\alpha, \beta) = 2^{-(n+q)} \sum_{k\in V_{n+q}} \delta\left(f_{i,k}(x\oplus\alpha) \oplus f_{i,k}(x), \beta\right) =$$

$$= 2^{-q} \sum_{k^{(2)}\in V_q} \left(2^{-n} \sum_{k^{(1)}\in V_n} \delta\left(f_{i,\left(k^{(1)},k^{(2)}\right)}(x\oplus\alpha) \oplus f_{i,\left(k^{(1)},k^{(2)}\right)}(x), \beta \right) \right). \quad (12)$$

For finding upper bounds of parameter $EDP(\Omega)$ let us assess every multiplier of right part of inequation (10). Firstly, let us consider some designations. For any natural l designate $u+v$ the sum by modulo 2^l of binary integer numbers presented as vectors u and v ($u, v \in V_l$); symbol $v(u, v)$ designate bit of carrying in l-th bit by adding numbers u and v in the ring Z.

For any $j \in \overline{0, b-1}$, in accordance with [7], let us designate the following parameters:

$$d_{\oplus}^{(s_j)}(\alpha, \beta) = 2^{-t} \sum_{k\in V_t} \delta\left(s_j(k\oplus\alpha) \oplus s_j(k), \beta\right) \quad (13)$$

$$d_{+}^{(s_j)}(\alpha, \beta) = 2^{-t} \sum_{k\in V_t} \delta\left(s_j(k+\alpha) \oplus s_j(k), \beta\right) \quad (14)$$

$$\Delta_{\oplus} = \max\left\{ d_{\oplus}^{(s_j)}(\alpha, \beta) : \alpha, \beta \in V_t \setminus \{0\}, j \in \overline{0, b-1} \right\} \quad (15)$$

$$\Delta_{+} = \max\left\{ d_{+}^{(s_j)}(\alpha, \beta) : \alpha, \beta \in V_t \setminus \{0\}, j \in \overline{0, b-1} \right\}, \quad (16)$$

$$\Delta = \max\{\Delta_{\oplus}, \Delta_{+}\}. \quad (17)$$

Additionally, let us consider the following parameters:

$$\tilde{\Delta}_{\oplus} = b^{-1} \sum_{j=0}^{b-1} \max\left\{ d_{\oplus}^{(s_j)}(\alpha, \beta) : \alpha, \beta \in V_t \setminus \{0\} \right\}, \quad (18)$$

$$\tilde{\Delta}_{+} = b^{-1} \sum_{j=0}^{b-1} \max\left\{ d_{+}^{(s_j)}(\alpha, \beta) : \alpha, \beta \in V_t \setminus \{0\} \right\}, \quad (19)$$

$$\tilde{\Delta} = \max\left\{ \tilde{\Delta}_{\oplus}, \tilde{\Delta}_{+} \right\}, \quad (20)$$

$$\tilde{\tilde{d}}_{\oplus}(\alpha, \beta) = b^{-1} \sum_{j=0}^{b-1} d_{\oplus}^{(s_j)}(\alpha, \beta), \quad (21)$$

$$\tilde{\tilde{d}}_{+}(\alpha, \beta) = b^{-1} \sum_{j=0}^{b-1} d_{+}^{(s_j)}(\alpha, \beta), \quad (22)$$

$$\overset{\approx}{\Delta}_{\oplus} = \max\left\{\overset{\approx}{d}_{\oplus}\left(\alpha, \beta\right) : \alpha, \beta \in V_t \setminus \{0\}\right\}, \quad (23)$$

$$\overset{\approx}{\Delta}_{+} = \max\left\{\overset{\approx}{d}_{+}\left(\alpha, \beta\right) : \alpha, \beta \in V_t \setminus \{0\}\right\}, \quad (24)$$

$$\overset{\approx}{\Delta} = \max\left\{\overset{\approx}{\Delta}_{\oplus}, \overset{\approx}{\Delta}_{+}\right\}. \quad (25)$$

As a reminder, in accordance with [7] the value of vector $x = \left(x_{p-1}, \ldots, x_0\right)$ can be defined by the following formula:

$$wt\left(x\right) = \#\left\{j \in \overline{0, p-1} : x_j \neq 0\right\}, \quad (26)$$

where $x_j \in \mathrm{GF}(2^t)$, $j \in \overline{0, p-1}$. Index of matrix M ramification can be defined as follows [15, 16]:

$$B_M = \min\left\{wt\left(x\right) + wt\left(xM^{-1}\right) : x \in GF\left(2^t\right)^p \setminus \{0\}\right\} \quad (27)$$

Let us establish the following lemma.

Lemma 1. Let us consider BC $\Im$, described by formulas (1) − (5). While for any $x \in V_n$ the following assertions are performed:

1) if $i \equiv 1\left(\bmod 2\right)$, $i < r$, then

$$d_x^{(i)}\left(\omega_{i-1}, \omega_i\right) \leq \left(\overset{\approx}{\Delta}_{\oplus}\right)^{wt\left(\omega_i M^{-1}\right)}; \quad (28)$$

2) if $i = r$, then

$$d_x^{(i)}\left(\omega_{i-1}, \omega_i\right) \leq \left(\overset{\approx}{\Delta}_{\oplus}\right)^{wt\left(\omega_i\right)}; \quad (29)$$

3) if $i \equiv 0\left(\bmod 2\right)$, $i < r$, then

$$d_x^{(i)}\left(\omega_{i-1}, \omega_i\right) \leq \left(\overset{\approx}{\Delta}_{+}\right)^{wt\left(\omega_i M^{-1}\right)}; \quad (30)$$

4) if $i < r$, then

$$wt\left(\omega_i M^{-1}\right) = wt\left(\omega_{i-1}\right); \quad (31)$$

5) if $i = r$, then

$$wt\left(\omega_r\right) = wt\left(\omega_{r-1}\right). \quad (32)$$

Establishment. Let us consider $i \equiv 1\left(\bmod 2\right)$, $i < r$. Taking into account (2), formula (12) can be transformed as follows:

$$d_x^{(i)}\left(\omega_{i-1}, \omega_i\right) = 2^{-q} \sum_{k^{(2)} \in V_q}\left(2^{-n} \sum_{k^{(1)} \in V_n} \delta\left(\varphi\left(k^{(1)} \oplus \omega_{i-1}, k^{(2)}\right) \oplus \varphi\left(k^{(1)}, k^{(2)}\right), \omega_i\right)\right) =$$
$$= 2^{-q} \sum_{k^{(2)} \in V_q}\left(2^{-n} \sum_{k^{(1)} \in V_n} \delta\left(s\left(k^{(1)} \oplus \omega_{i-1}, k^{(2)}\right) \oplus s\left(k^{(1)}, k^{(2)}\right), \omega_i M^{-1}\right)\right).$$

From this by using formulas (4), (13) and (21) can be obtained the following

$$d_x^{(i)}\left(\omega_{i-1}, \omega_i\right) = \prod_{j=0}^{p-1}\left(2^{-q'} \sum_{k_j^{(2)} \in V_{q'}}\left(2^{-t} \sum_{k_j^{(1)} \in V_t} \delta\left(s_{k_j^{(2)}}\left(k_j^{(1)} \oplus \left(\omega_{i-1}\right)_j\right) \oplus s_{k_j^{(2)}}\left(k_j^{(1)}\right), \left(\omega_i M^{-1}\right)_j\right)\right)\right) =$$
$$= \prod_{j=0}^{p-1}\left(2^{-q'} \sum_{k_j^{(2)} \in V_{q'}}\left(d_{\oplus}^{\left(s_{k_j^{(2)}}\right)}\left(\left(\omega_{i-1}\right)_j, \left(\omega_i M^{-1}\right)_j\right)\right)\right) = \prod_{j=0}^{p-1}\left(\overset{\approx}{d}_{\oplus}\left(\left(\omega_{i-1}\right)_j, \left(\omega_i M^{-1}\right)_j\right)\right).$$
$$(33)$$

Considering that $\overset{\approx}{d}_{\oplus}\left(\left(\omega_{i-1}\right)_j, \left(\omega_i M^{-1}\right)_j\right) \leq 1$, the maximal value of (33) is received if $\left(\omega_{i-1}\right)_j = \left(\omega_i M^{-1}\right)_j = 0$, in this case $\overset{\approx}{d}_{\oplus}\left(\left(\omega_{i-1}\right)_j, \left(\omega_i M^{-1}\right)_j\right) = 1$ (if only for one j $\left(\omega_{i-1}\right)_j, \left(\omega_i M^{-1}\right)_j \neq 0$ ($j \in \overline{0, p-1}$)). Based on this, by using formula (23), it follows correctness of formulas (28) and (31):

$$d_x^{(i)}\left(\omega_{i-1}, \omega_i\right) = \prod_{j=0}^{p-1}\left(\overset{\approx}{d}_{\oplus}\left(\left(\omega_{i-1}\right)_j, \left(\omega_i M^{-1}\right)_j\right)\right) \leq \overset{\approx}{\Delta}_{\oplus}^{\,wt\left(\omega_i M^{-1}\right)},$$
$$wt\left(\omega_i M^{-1}\right) = wt\left(\omega_{i-1}\right).$$

In similar manner formulas (29) and (32) can be established.

Let us establish the formula (30). Let us consider $i \equiv 0\left(\bmod 2\right)$, $i < r$. Taking into account formula (2), formula (12) can be transformed as follows:

$$d_x^{(i)}\left(\omega_{i-1}, \omega_i\right) = 2^{-q} \sum_{k^{(2)} \in V_q}\left(2^{-n} \sum_{k^{(1)} \in V_n} \delta\left(\varphi\left(\left(x \oplus \omega_{i-1}\right) \mathring{+} k^{(1)}, k^{(2)}\right) \oplus \varphi\left(x \mathring{+} k^{(1)}, k^{(2)}\right), \omega_i\right)\right) =$$
$$= 2^{-q} \sum_{k^{(2)} \in V_q}\left(2^{-n} \sum_{k^{(1)} \in V_n} \delta\left(s\left(k^{(1)} \mathring{+} \left(\left(x \oplus \omega_{i-1}\right) \mathring{-} x\right), k^{(2)}\right) \oplus s\left(k^{(1)}, k^{(2)}\right), \omega_i M^{-1}\right)\right).$$
$$(34)$$

In research study [7] was established that for any fixed substitutions on the set V_t, $s\left(x\right) = \left(s_{m-1}\left(x_{m-1}\right), \ldots, s_0\left(x_0\right)\right)$, $x = \left(x_{m-1}, \ldots, x_0\right)$ by any $\alpha, \beta \in V_{mt}$ following inequation is correct:

$$d_{+}^{(s)}(\alpha,\beta) \overset{\text{def}}{=} 2^{-mt}\sum_{k\in V_{mt}}\delta\big(s(\alpha+k)\oplus s(k),\beta\big)\le(\Delta_{+})^{wt(\beta)}. \tag{35}$$

Analogically formula (35) can be transformed for the case when the table of substitutions s will be dependable on parameter y (see formula (4)).

Let us consider $s(x,y)=\big(s_{y_{m-1}}(x_{m-1}),\dots,s_{y_0}(x_0)\big)$ is random substitution on the set V_{mt}, $x=(x_{m-1},\dots,x_0)$, $y=(y_{m-1},\dots,y_0)$, $x_j\in V_t$, $y_j\in V_{q'}$, $j\in\overline{0,m-1}$ (parameter y_j defines the substitution table on the set V_t will be used, one of $2^{q'}$ the possible tables is chosen). Then for any $\alpha,\beta\in V_{mt}$ the following inequation is correct:

$$d_{+}^{(s)}(\alpha,\beta) \overset{\text{def}}{=} 2^{-mq'}\sum_{y\in V_{mq'}}\left(2^{-mt}\sum_{k\in V_{mt}}\delta\big(s(\alpha+k,y)\oplus s(k,y),\beta\big)\right)\le\left(\overset{\approx}{\Delta}_{+}\right)^{wt(\beta)}. \tag{36}$$

Let us establish inequation (36) by the method of mathematical induction by parameter m . For $m=1$ let us check correctness of inequation (36). Based on formulas (14), (22) and (24) can be obtained:

$$d_{+}^{(s)}(\alpha,\beta)=2^{-q'}\sum_{y\in V_{q'}}\left(2^{-t}\sum_{k\in V_t}\delta\big(s_y(\alpha+k)\oplus s_y(k),\beta\big)\right)=$$

$$=2^{-q'}\sum_{y\in V_{q'}}\left(d_{+}^{(s_y)}(\alpha,\beta)\right)=\overset{\approx}{d}_{+}(\alpha,\beta)\le\left(\overset{\approx}{\Delta}_{+}\right)^{wt(\beta)}$$

Next, let us make allowance for formula (36) is correct for all substitutions $\big(s_{y_{m-1}}(x_{m-1}),\dots,s_{y_1}(x_1)\big)$, where s_{y_j} is substitution on the set V_t, $y_j\in V_{q'}$, $j\in\overline{1,m-1}$.

For any $x=(x_{m-1},\dots,x_0)\in V_{mt}$, $y=(y_{m-1},\dots,y_0)\in V_{mq'}$ let us designate

$$\tilde{x}=(x_{m-1},\dots,x_1),\ \tilde{y}=(y_{m-1},\dots,y_1),$$
$$\tilde{s}\left(\tilde{x},\tilde{y}\right)=\big(s_{y_{m-1}}(x_{m-1}),\dots,s_{y_1}(x_1)\big).$$

Taking into account the equation $\alpha+k=\left(\tilde{\alpha}+\tilde{k}+\nu(\alpha_0,k_0),\alpha_0+k_0\right),\quad \alpha,k\in V_{mt}$, the following formula is correct:

$$d_{+}^{(s)}(\alpha,\beta)=2^{-q'}\sum_{y_0\in V_{q'}}\left(2^{-t}\sum_{k_0\in V_t}\delta\big(s_{y_0}(\alpha_0+k_0)\oplus s_{y_0}(k_0),\beta_0\big)\right)\times$$
$$\times 2^{-(mq'-q')}\sum_{\tilde{y}\in V_{mq'-q'}}\left(2^{-(mt-t)}\sum_{\tilde{k}\in V_{mt-t}}\delta\left(\tilde{s}\left(\tilde{\alpha}+\tilde{k}+\nu(\alpha_0,k_0),\tilde{y}\right)\oplus\tilde{s}\left(\tilde{k},\tilde{y}\right),\tilde{\beta}\right)\right)=$$
$$=\overset{\approx}{d}_{+\,\nu(\alpha_0,k_0)=1}(\alpha_0,\beta_0)\times 2^{-(mq'-q')}\sum_{\tilde{y}\in V_{mq'-q'}}\left(2^{-(mt-t)}\sum_{\tilde{k}\in V_{mt-t}}\delta\left(\tilde{s}\left(\tilde{\alpha}+\tilde{k}+1,\tilde{y}\right)\oplus\tilde{s}\left(\tilde{k},\tilde{y}\right),\tilde{\beta}\right)\right)+$$
$$+\overset{\approx}{d}_{+\,\nu(\alpha_0,k_0)=0}(\alpha_0,\beta_0)\times 2^{-(mq'-q')}\sum_{\tilde{y}\in V_{mq'-q'}}\left(2^{-(mt-t)}\sum_{\tilde{k}\in V_{mt-t}}\delta\left(\tilde{s}\left(\tilde{\alpha}+\tilde{k},\tilde{y}\right)\oplus\tilde{s}\left(\tilde{k},\tilde{y}\right),\tilde{\beta}\right)\right)=$$
$$=\overset{\approx}{d}_{+\,\nu(\alpha_0,k_0)=1}(\alpha_0,\beta_0)\times d_{+}^{\left(\tilde{s}\right)}\left(\tilde{\alpha}+1,\tilde{\beta}\right)+\overset{\approx}{d}_{+\,\nu(\alpha_0,k_0)=0}(\alpha_0,\beta_0)\times d_{+}^{\left(\tilde{s}\right)}\left(\tilde{\alpha},\tilde{\beta}\right). \tag{37}$$

Considering that $d_{+}^{\left(\tilde{s}\right)}\left(\tilde{\alpha}+1,\tilde{\beta}\right)\le\left(\overset{\approx}{\Delta}_{+}\right)^{wt\left(\tilde{\beta}\right)}$ and $d_{+}^{\left(\tilde{s}\right)}\left(\tilde{\alpha},\tilde{\beta}\right)\le\left(\overset{\approx}{\Delta}_{+}\right)^{wt\left(\tilde{\beta}\right)}$ by the hypothesis of induction, based on the formula (37), it is established correctness of inequation (36):

$$d_{+}^{(s)}(\alpha,\beta)\le\overset{\approx}{d}_{+}(\alpha_0,\beta_0)\times\left(\overset{\approx}{\Delta}_{+}\right)^{wt\left(\tilde{\beta}\right)}\le\left(\overset{\approx}{\Delta}_{+}\right)^{wt\left(\tilde{\beta}\right)+wt(\beta_0)}=\left(\overset{\approx}{\Delta}_{+}\right)^{wt(\beta)},$$

and it was the target of our establishment.

Let us transform equation (34), taking into account inequation (36):

$$d_{x}^{(i)}(\omega_{i-1},\omega_i)=d_{+}^{(s)}\left(\left(x\oplus\omega_{i-1}\right)\overset{\circ}{-}x,\omega_i M^{-1}\right)\le\left(\overset{\approx}{\Delta}_{+}\right)^{wt\left(\omega_i M^{-1}\right)}$$

By this means inequation (30) is correct. Lemma 1 is established.

Next, let us define an analytical upper security parameter (7) for BC, described by formulas (1) − (5).

Theorem 1. Let us consider r-round BC $\Im$, described by formulas (1) − (5). In this case the following inequation is correct:

$$EDP(\Omega)\le\overset{\approx}{\Delta}^{r'B_M+1}\le\tilde{\Delta}^{r'B_M+1}\le\Delta^{r'B_M+1}. \tag{38}$$

Establishment. On the basis of formulas (10), (23) − (25), (28) − (30) the following assessment is correct:

$$EDP(\Omega) \le \approx\Delta^{\sum_{i=1}^{r-1} wt\left(\omega_i M^{-1}\right)+wt(\omega_r)}. \quad (39)$$

While by the formulas (13) − (25) $\approx\Delta \le \tilde{\Delta} \le \Delta < 1$, then right part of inequation will be maximal only when $\sum_{i=1}^{r-1} wt\left(\omega_i M^{-1}\right) + wt(\omega_r)$ will be minimal. In research study [7] authors showed that $\sum_{i=1}^{r-1} wt\left(\omega_i M^{-1}\right) + wt(\omega_r) \ge r' B_M + 1$, and on this basis formula (38) is correct. Theorem 1 is established.

5. UPPER BOUNDS OF LINEAR PARAMETERS AVERAGE PROBABILITIES

For any $\alpha, \beta \in V_t$, $j \in \overline{0, b-1}$, taking into account [7], let us designate:

$$l^{(s_j)}(\alpha, \beta) = 2^{-t} \sum_{k \in V_t} \left(2^{-t} \sum_{x \in V_t} (-1)^{\alpha x \oplus \beta s_j (x \oplus k)} \right)^2, \quad (40)$$

$$\Lambda^{(s_j)}(\alpha, \beta) = 2^{-t} \sum_{k \in V_t} \left(2^{-t} \sum_{a \in \{0,1\}} \left| \sum_{x \in V_t : v(x,k)=a} (-1)^{\alpha x \oplus \beta s_j (x+k)} \right| \right)^2 \quad (41)$$

$$\Lambda_{\oplus} = \max\left\{ l^{(s_j)}(\alpha, \beta) : \alpha, \beta \in V_t \setminus \{0\}, j \in \overline{0, b-1} \right\} \quad (42)$$

$$\Lambda_{+} = \max\left\{ \Lambda^{(s_j)}(\alpha, \beta) : \alpha \in V_t, \beta \in V_t \setminus \{0\}, j \in \overline{0, b-1} \right\} \quad (43)$$

$$\Lambda = \max\left\{ \Lambda_{\oplus}, \Lambda_{+} \right\}. \quad (44)$$

Additionally, let us consider the following parameters:

$$\tilde{\Lambda}_{\oplus} = b^{-1} \sum_{j=0}^{b-1} \max\left\{ l^{(s_j)}(\alpha, \beta) : \alpha, \beta \in V_t \setminus \{0\} \right\} \quad (45)$$

$$\tilde{\Lambda}_{+} = b^{-1} \sum_{j=0}^{b-1} \max\left\{ \Lambda^{(s_j)}(\alpha, \beta) : \alpha \in V_t, \beta \in V_t \setminus \{0\} \right\} \quad (46)$$

$$\tilde{\Lambda} = \max\left\{ \tilde{\Lambda}_{\oplus}, \tilde{\Lambda}_{+} \right\}, \quad (47)$$

$$\approx l(\alpha, \beta) = b^{-1} \sum_{j=0}^{b-1} l^{(s_j)}(\alpha, \beta), \quad (48)$$

$$\approx\Lambda(\alpha, \beta) = b^{-1} \sum_{j=0}^{b-1} \Lambda^{(s_j)}(\alpha, \beta), \quad (49)$$

$$\approx\Lambda_{\oplus} = \max\left\{ \approx l(\alpha, \beta) : \alpha, \beta \in V_t \setminus \{0\} \right\}, \quad (50)$$

$$\approx\Lambda_{+} = \max\left\{ \approx\Lambda(\alpha, \beta) : \alpha \in V_t, \beta \in V_t \setminus \{0\} \right\}, \quad (51)$$

$$\approx\Lambda = \max\left\{ \approx\Lambda_{\oplus}, \approx\Lambda_{+} \right\}. \quad (52)$$

For finding upper bounds of parameter $ELP(\Omega)$ let us assess every multipliers of right part of inequation (8). Let us establish the following lemma.

Lemma 2. Let us consider BC $\mathfrak{I}$, described by formulas (1) − (5). While for any $x \in V_n$ the following assertions are performed:

1) if $i \equiv 1 \pmod 2$, $i < r$, then

$$l^{(i)}(\omega_{i-1}, \omega_i) \le \left(\approx\Lambda_{\oplus} \right)^{wt(\omega_i M)}; \quad (53)$$

2) if $i = r$, then

$$l^{(i)}(\omega_{i-1}, \omega_i) \le \left(\approx\Lambda_{\oplus} \right)^{wt(\omega_i)}; \quad (54)$$

3) if $i \equiv 0 \pmod 2$, $i < r$, then

$$l^{(i)}(\omega_{i-1}, \omega_i) \le \left(\approx\Lambda_{+} \right)^{wt(\omega_i M)}; \quad (55)$$

4) if $i < r$, then

$$wt(\omega_i M) = wt(\omega_{i-1}); \quad (56)$$

5) if $i = r$, then

$$wt(\omega_r) = wt(\omega_{r-1}). \quad (57)$$

Establishment. Let us consider $i \equiv 1 \pmod 2$, $i < r$. Taking into account equation (2), let us transform formula (9):

$$l^{(i)}(\omega_{i-1}, \omega_i) = 2^{-q} \sum_{k^{(2)} \in V_q} \left(2^{-n} \sum_{k^{(1)} \in V_n} \left(2^{-n} \sum_{x \in V_n} (-1)^{\omega_{i-1} x \oplus \omega_i \varphi\left(x \oplus k^{(1)}, k^{(2)}\right)} \right)^2 \right) =$$

$$= 2^{-q} \sum_{k^{(2)} \in V_q} \left(2^{-n} \sum_{k^{(1)} \in V_n} \left(2^{-n} \sum_{x \in V_n} (-1)^{\omega_{i-1} x \oplus (\omega_i M) \cdot s\left(x \oplus k^{(1)}, k^{(2)}\right)} \right)^2 \right).$$

Based on formulas (4), (40) and (48) can be obtained:

$$l^{(i)}(\omega_{i-1}, \omega_i) = \prod_{j=0}^{p-1} \left(2^{-q'} \sum_{k_j^{(2)} \in V_{q'}} \left(2^{-t} \sum_{k_j^{(1)} \in V_t} \left(2^{-t} \sum_{x_j \in V_t} (-1)^{(\omega_{i-1})_j x_j \oplus (\omega_i M)_j \cdot s_{k_j^{(2)}}\left(x_j \oplus k_j^{(1)}\right)} \right)^2 \right) \right) =$$

$$= \prod_{j=0}^{p-1} \left(2^{-q'} \sum_{k_j^{(2)} \in V_{q'}} \left(l^{\left(s_{k_j^{(2)}}\right)} \left((\omega_{i-1})_j, (\omega_i M)_j \right) \right) \right) = \prod_{j=0}^{p-1} \left(\tilde{\tilde{l}} \left((\omega_{i-1})_j, (\omega_i M)_j \right) \right).$$

(58)

Considering that $\tilde{\tilde{l}}\left((\omega_{i-1})_j, (\omega_i M)_j\right) \le 1$, the maximal value of (58) is received if $(\omega_{i-1})_j = (\omega_i M)_j = 0$, in this case $\tilde{\tilde{l}}\left((\omega_{i-1})_j, (\omega_i M)_j\right) = 1$ (if only for one j $(\omega_{i-1})_j, (\omega_i M)_j \ne 0$ ($j \in \overline{0, p-1}$)). Based on this, by using formula (50), it follows correctness of formulas (53) and (56):

$$l^{(i)}(\omega_{i-1}, \omega_i) = \prod_{j=0}^{p-1} \left(\tilde{\tilde{l}} \left((\omega_{i-1})_j, (\omega_i M)_j \right) \right) \le \tilde{\tilde{\Lambda}}_{\oplus}^{wt(\omega_i M)}$$

$$wt(\omega_i M) = wt(\omega_{i-1}).$$

In similar manner formulas (54) and (57) can be established.

Let us establish the formula (55). Let us consider $i \equiv 0 \pmod 2$, $i < r$. Taking into account formula (2), formula (9) can be transformed as follows:

$$l^{(i)}(\omega_{i-1}, \omega_i) = 2^{-q} \sum_{k^{(2)} \in V_q} \left(2^{-n} \sum_{k^{(1)} \in V_n} \left(2^{-n} \sum_{x \in V_n} (-1)^{\omega_{i-1} x \oplus \omega_i \varphi\left(x \mathbin{\mathring{+}} k^{(1)}, k^{(2)}\right)} \right)^2 \right) =$$

$$= 2^{-q} \sum_{k^{(2)} \in V_q} \left(2^{-n} \sum_{k^{(1)} \in V_n} \left(2^{-n} \sum_{x \in V_n} (-1)^{\omega_{i-1} x \oplus (\omega_i M) s\left(x \mathbin{\mathring{+}} k^{(1)}, k^{(2)}\right)} \right)^2 \right).$$

(59)

Let us consider $s(x, y) = \left(s_{y_{m-1}}(x_{m-1}), \dots, s_{y_0}(x_0)\right)$ is random substitution on the set V_{mt}, $x = (x_{m-1}, \dots, x_0)$, $y = (y_{m-1}, \dots, y_0)$, $x_j \in V_t$, $y_j \in V_{q'}$, $j \in \overline{0, m-1}$ (parameter y_j defines the substitution table on the set V_t will be used, one of $2^{q'}$ the possible tables is chosen). Then for any $\alpha, \beta \in V_{mt}$ the following inequation is correct:

$$l_+^{(s)}(\alpha, \beta) \stackrel{\text{def}}{=} 2^{-mq'} \sum_{y \in V_{mq'}} \left(2^{-mt} \sum_{k \in V_{mt}} \left(2^{-mt} \sum_{x \in V_{mt}} (-1)^{\alpha x \oplus \beta s(x+k, y)} \right)^2 \right) \le \left(\tilde{\tilde{\Lambda}}_+ \right)^{wt(\beta)}.$$

(60)

Let us establish inequation (60) by the method of mathematical induction by parameter m . For $m = 1$ let us check correctness of inequation (60). Based on formulas (41), (49) and (51) can be obtained:

$$l_+^{(s)}(\alpha, \beta) = 2^{-q'} \sum_{y \in V_{q'}} \left(2^{-t} \sum_{k \in V_t} \left(2^{-t} \sum_{x \in V_t} (-1)^{\alpha x \oplus \beta s(x+k, y)} \right)^2 \right) =$$

$$= 2^{-q'} \sum_{y \in V_{q'}} \left(2^{-t} \sum_{k \in V_t} \left(2^{-t} \sum_{a \in \{0,1\}} \left| \sum_{x \in V_t : \nu(x, k) = a} (-1)^{\alpha x \oplus \beta s_y(x+k)} \right| \right)^2 \right) = \tilde{\tilde{\Lambda}}(\alpha, \beta) \le \left(\tilde{\tilde{\Lambda}}_+ \right)^{wt(\beta)}.$$

Next, let us make allowance for formula (60) is correct for all substitutions $\left(s_{y_{m-1}}(x_{m-1}), \dots, s_{y_1}(x_1)\right)$, where s_{y_j} is substitution on the set V_t, $y_j \in V_{q'}$, $j \in \overline{1, m-1}$.

For any $x = (x_{m-1}, \dots, x_0) \in V_{mt}$, $y = (y_{m-1}, \dots, y_0) \in V_{mq'}$ let us designate:

$$\tilde{x} = (x_{m-1}, \dots, x_1),\ \tilde{y} = (y_{m-1}, \dots, y_1),$$

$$\tilde{s}\left(\tilde{x}, \tilde{y}\right) = \left(s_{y_{m-1}}(x_{m-1}), \dots, s_{y_1}(x_1)\right).$$

In accordance with equation $x + k = \left(\tilde{x} + \tilde{k} + \nu(x_0, k_0), x_0 + k_0\right)$, $\alpha, k \in V_{mt}$, the following formula is correct:

$$l_+^{(s)}(\alpha, \beta) = 2^{-q'} \sum_{y_0 \in V_{q'}} \left(2^{-t} \sum_{k_0 \in V_t} \left(2^{-t} \sum_{x_0 \in V_t} (-1)^{\alpha_0 x_0 \oplus \beta_0 s_{y_0}(x_0 + k_0)} \right)^2 \right) \times$$

$$\times 2^{-(mq'-q')} \sum_{\tilde{y} \in V_{(mq'-q')}} \left(2^{-(mt-t)} \sum_{\tilde{k} \in V_{(mt-t)}} \left(2^{-(mt-t)} \sum_{\tilde{x} \in V_{(mt-t)}} (-1)^{\tilde{\alpha} \tilde{x} \oplus \tilde{\beta} \tilde{s}\left(\tilde{x} + \tilde{k} + \nu(x_0, k_0), \tilde{y}\right)} \right)^2 \right) =$$

$$= \tilde{\tilde{\Lambda}}(\alpha_0, \beta_0) \times l_+^{\left(\tilde{s}\right)}\left(\tilde{\alpha}, \tilde{\beta}\right) \le \tilde{\tilde{\Lambda}}(\alpha_0, \beta_0) \times \left(\tilde{\tilde{\Lambda}}_+\right)^{wt(\tilde{\beta})} \le \left(\tilde{\tilde{\Lambda}}_+\right)^{wt(\tilde{\beta}) + wt(\beta_0)} = \left(\tilde{\tilde{\Lambda}}_+\right)^{wt(\beta)},$$

and it was the target of our establishment.

Based on inequation (60), the formula (55) is correct:

$$l^{(i)}\left(\omega_{i-1},\omega_i\right)=l_+^{(s)}\left(\omega_{i-1},\omega_i M\right)\leq \overset{\approx}{\Lambda}_+^{wt(\omega_i M)}.$$

Lemma 2 is established.

Theorem 2. Let us consider r-round BC $\Im$, described by formulas (1) − (5). In this case, the following inequation is correct:

$$ELP(\Omega)\leq \overset{\approx}{\Lambda}^{r'B_M+1}\leq \tilde{\Lambda}^{r'B_M+1}\leq \Lambda^{r'B_M+1}. \quad (61)$$

Establishment. Based on formulas (8), (50) − (55) the following assessment is correct:

$$ELP(\Omega)\leq \overset{\approx}{\Lambda}^{\sum_{i=1}^{r-1} wt(\omega_i M)+wt(\omega_r)}. \quad (62)$$

While by the formulas (40) − (52) $\overset{\approx}{\Delta}\leq\tilde{\Delta}\leq\Delta<1$, then the right part of inequation will be maximal only when $\sum_{i=1}^{r-1} wt\left(\omega_i M\right)+wt\left(\omega_r\right)$ will be minimal. In research study [7] authors showed that $\sum_{i=1}^{r-1} wt\left(\omega_i M\right)+wt\left(\omega_r\right)\geq r'B_M+1$, and on this basis formula (61) is correct. Theorem 2 is established.

6. EXPERIMENTS AND DISCUSSION

The main target of experimental study is efficiency assessment of random substitution nodes using in proposed and known BCs. Let us consider that in the paper [7] was described r-round BC $\Im'$ (designed based on Kalyna-128 cipher) with random substitutions nodes, a set of plain (cipher) texts $V_n=\{0,1\}^n$, a set of round keys $K=V_n$ and family of encryption transformation

$$F_k=f_{r,k_r}\circ\ldots\circ f_{1,k_1},\ k=(k_1,\ldots,k_r)\in K^r, \quad (63)$$

where t, p', r' are natural numbers, $p=4p'$, $r=2r'+1$, $n=pt$.

Round function $f_{i,k}$, for any $x\in V_n$, $k\in K$, $i\in\overline{1,r}$ can be described as follow:

$$f_{i,k}=\begin{cases}\varphi\left(x\oplus k\right), & if\ \mathrm{i}\equiv 1\left(\mathrm{mod}\,2\right),\ i<r\\ \varphi\left(x\overset{\circ}{+}k\right), & if\ \mathrm{i}\equiv 0\left(\mathrm{mod}\,2\right),\ i<r.\\ s\left(x\oplus k\right), & if\ \mathrm{i}=\mathrm{r}\end{cases} \quad (64)$$

Substitutions φ and s can be defined by formulas:

$$\varphi(x)=s(x)M,\ x\in V_n, \quad (65)$$

$$s(x)=\left(\mathrm{s}_{p-1}\left(x_{p-1}\right),\ldots,s_0\left(x_0\right)\right),\ x=\left(x_{p-1},\ldots,x_0\right), \quad (66)$$

where $x_j\in V_t$, s_j is substitution on the set V_t, $j\in\overline{0,p-1}$, M is invertible $p\times p$-matrix over the field $\mathrm{GF}\left(2^t\right)$, multiplication $s(x)$ and M in formula (65) performed over this field with binary vectors unification $s_j\left(x_j\right)$ with its elements. Symbols "$\oplus$" and "$\overset{\circ}{+}$" are compatible with operations of coordinatewise adding for binary vectors and mentioned algebraic operation (5).

In [7] it was established that for BC $\Im'$, described by (63) − (66), the following inequations are correct:

$$EDP(\Omega)\leq\Delta^{r'B_M+1}, \quad (67)$$

$$ELP(\Omega)\leq\Lambda^{r'B_M+1}. \quad (68)$$

If the round function $f_{i,k}$ of BC $\Im'$, described by (63) − (66), increased by additional round key influenced on substitution forming (see formula (4)), BC $\Im'$ will transform to BC $\Im$, described by (1) − (5). Taking into account equations (13) − (25) and (63) − (66), as well as inequations (38) and (61) analytical upper bounds of linear and differential parameters average probabilities of BC $\Im'$ will improve in $\left(\overset{\approx}{\Delta}/\Delta\right)^{r'B_M+1}$ and $\left(\overset{\approx}{\Lambda}/\Lambda\right)^{r'B_M+1}$ times respectively. It is important to note, the more quantity of substitution tables for BC $\Im'$, the better upper bounds of practical security against LDC [17].

Let us show the efficiency of random substitution nodes using in the context of BC Kalyna-128 [11] (the example of BC $\Im'$ with parameters $t=8$, $p'=4$, $r'=5$, $p=16$, $r=11$, $n=128$, in every rounds eight different substitution tables on the set V_8 are used (Table 1)).

Table 1. The parameters of substitution tables for BC Kalyna-128

Subs table	$\Delta_{\oplus}^{(s_j)}$	$\Delta_{+}^{(s_j)}$	$\Lambda_{\oplus}^{(s_j)}$	$\Lambda_{+}^{(s_j)}$
1	0,03125	0,0273438	0,0625	0,0425324
2	0,03125	0,03125	0,05493	0,0297253
3	0,03125	0,03125	0,0625	0,0297267
4	0,03125	0,0273438	0,0625	0,0551662
5	0,03125	0,03125	0,0625	0,0356412
6	0,03125	0,03125	0,0625	0,0353937
7	0,03125	0,03125	0,0625	0,0296712
8	0,03125	0,03125	0,0625	0,0625

In Table 1, there are parameters (15), (16), (42) and (43) for every substitution tables of BC Kalyna-128. In accordance with equations (15) − (17), (42) − (44) as well as inequations (67) and (68) can be obtained the following parameters: $\Delta = 0,031250$, $\Lambda = 0,0625$, $EDP(\Omega) \le 2^{-230}$, $ELP(\Omega) \le 2^{-184}$ ($r' = 5$, $B_M = 9$).

Let us admit that BC Kalyna-128 increased by round keys, and it defines each substitution tables for round. In this case BC $\Im$ can be obtained with parameters $q' = 3$, $q = 48$, and $b = 8$. For this BC inequations (38) and (61) can be used to calculate analytical upper bounds of practical security against LDC methods. Based on formulas (21) − (25), for described in BC Kalyna substitution tables [23], parameters (23) − (25) were calculated: $\overset{\approx}{\Delta}_{\oplus} = 0,015625$, $\overset{\approx}{\Delta}_{+} = 0,0107422$ and $\overset{\approx}{\Delta} = 0,015625$. For the same substitution tables based on formulas (48) − (52), parameters (50) − (52) were also calculated: $\overset{\approx}{\Lambda}_{\oplus} = 0,0159302$, $\overset{\approx}{\Lambda}_{+} = 0,0143183$ and $\overset{\approx}{\Lambda} = 0,0159302$.

Because $r' = 5$, $B_M = 9$, based on inequations (38) and (61), upper bounds of practical security for improved BC Kalyna-128 with random substitution nodes were calculated in context of LDC respectively: $EDP(\Omega) \le 2^{-276}$ and $ELP(\Omega) \le 2^{-274}$ [19-22]. As it is clear from calculations, upper bounds of linear and differential parameters average probabilities for improved BC Kalyna-128 (with random substitution nodes) is better in 2^{46} and 2^{90} times than original BC respectively.

Accordingly, analytical upper bounds of BC practical security against LDC methods were calculated as well as hypothesis that using random substitutions allows improving upper bounds of linear and differential parameters was proved. This proven hypothesis defines novelty of this work and practical value for modern cryptology.

7. CONCLUSIONS

In the paper analytical upper bounds of parameters, characterized practical security of BC $\Im$ with random substitution nodes against LDC methods were obtained.

It was established that random substitution nodes using in BC allow improving analytical upper bounds of linear and differential parameters average probabilities in $\left(\overset{\approx}{\Delta}/\Delta\right)^{r'B_M+1}$ and $\left(\overset{\approx}{\Lambda}/\Lambda\right)^{r'B_M+1}$ times respectively compared to analog assessments for similar BC with fixed substitution nodes.

By using the example of BC Kalyna-128, it was shown that the use of random substitution nodes allows improving upper bounds of linear and differential parameters average probabilities in 2^{46} and 2^{90} times respectively.

The study is novel as it is one of the few in the cryptology field to calculate analytical upper bounds of BC practical security against LDC methods as well as to show and prove that the use of random substitutions allows improving upper bounds of linear and differential parameters. The security analysis using quantitative parameters gives possibility to evaluate various BCs or other cryptographic algorithms and their ability to provide necessary and sufficient security level in ICS.

A future research study can be directed on improving analytical upper bounds for mentioned BC in context to practical security against LDC, as well as practical cryptographic security assessment for other BCs with random substitutions [25-29] against LDC and other cryptanalysis methods including quantum cryptanalysis [30-32] (Shor, Grover, Deutsch-Jozsa algorithms). Apart from these cases, the efficiency of the randomness source and its impact on the BC security can be studied.

8. REFERENCES

[1] E. Biham, A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *Journal of Cryptology*, vol. 4, issue 1, pp. 3-72, 1991.

[2] X. Lai, J.L. Massey, S. Murphy, "Markov ciphers and differential cryptanalysis," *Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques "Advances in Cryptology, EUROCRYPT-91",* Springer Verlag, 1991, pp. 17-38.

[3] M. Matsui, "Linear cryptanalysis methods for DES cipher," *Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques "Advances in Cryptology, EURO-CRYPT-93"*, Springer Verlag, 1994, pp. 386-397.

[4] S. Vaudenay, "Decorrelation: a theory for block cipher security," *Journal of Cryptology*, vol. 16, issue 4, pp. 249-286, 2003.

[5] J. Daemen, V. Rijmen, "Statistics of correlation and differentials in block ciphers," [Online]. Available at: http://eprint.iacr.org/2005/212

[6] M. Kanda, "Practical security evaluation against differential and linear cryptanalyses for Feistel ciphers with SPN round function," *Proceedings of the Selected Areas in Cryptography, SAC 2000*, Springer Verlag, 2001, pp. 324-338.

[7] A. Alekseychuk, L. Kovalchuk, E. Skrynnik, A. Shevtsov, "Assessment of practical security for block cipher "Kalyna" against differential, linear cryptanalysis and algebraic attacks based on homomorphism," *Applied Radio-electronics,* vol. 7, issue 3, pp. 203-209, 2008.

[8] H. Liu, A. Kadir, C. Xu, "Cryptanalysis and constructing S-box based on chaotic map and backtracking," *Applied Mathematics and Computation*, vol. 376, 125153, 2020, doi:10.1016/j.amc.2020.125153

[9] D. Yang, W.-F. Qi, H.-J. Chen, "Provable security against impossible differential and zero correlation linear cryptanalysis of some Feistel structures," *Designs, Codes, and Cryptography,* vol. 87, issue 11, pp. 2683-2700, 2019, doi:10.1007/s10623-019-00642-9

[10] GOST 28147-89, *Systems of information processing, Cryptographic security, Encryption algorithm,* Moscow, State Standard USSR, 1989.

[11] I. Gorbenko, V. Dolgov, R. Oliynykov, "Prospective block cipher "Kalyna" – basic issues and specifications," *Applied Radio-electronics,* vol. 6, issue 2, pp. 195-208, 2007.

[12] A. Kuznetsov, R. Sergienko, A. Maumko, "Symmetrical cryptographic algorithm ADE (Algorithm of Dynamic Encryption)," *Applied Radioelectronics,* vol. 6, issue 2, pp. 241-249, 2007.

[13] S. Gnatyuk, V. Kinzeryavyy, K. Kyrychenko, Kh. Yubuzova et al, "Secure hash function constructing for future communication systems and networks" *Advances in Intelligent Systems and Computing*, vol. 902, pp. 561-569, 2020.

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

[15] S. Gnatyuk, V. Kinzeryavyy, M. Iavich et al, "High-performance reliable block encryption algorithms secured against linear and differential cryptanalytic attacks," *CEUR Workshop Proceedings*, vol. 2104, pp. 657-668, 2018.

[16] J. Daemen, *Cipher and Hash Function Design Strategies based on Linear and Differential Cryptanalysis*, Ph.D. Thesis, Netherlands, 1995, 252 p.

[17] D. Xu and W. Chen, "A survey on cryptanalysis of block ciphers," *Proceedings of the 2010 International Conference on Computer Application and System Modeling (ICCASM 2010)*, Taiyuan, 2010, pp. 218-220.

[18] M. Wang, Y. Sun, E. Tischhauser, B. Preneel, "A model for structure attacks, with applications to PRESENT and Serpent," *Canteaut, A. (ed.) Proceedings of the Fast Software Encryption FSE 2012, Lecture Notes in Computer Science,* Springer, Heidelberg, vol. 7549, 2012, pp. 49-68.

[19] C. Blondeau, K. Nyberg, "New links between differential and linear cryptanalysis," *Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques "Advances in Cryptology, EUROCRYPT-2013"*, Springer Verlag, 2013, pp. 388-404.

[20] S. Das, J. U. Zaman, R. Ghosh, "Generation of AES S-boxes with various modulus and additive constant polynomials and testing their randomization," *Proc. Technol.*, vol. 10, pp. 957-962, 2013.

[21] P. Ping, J. Fan, Y. Mao, F. Xu, J. Gao, "A chaos based image encryption scheme using digit-level permutation and block diffusion," *IEEE Access*, vol. 6, pp. 67581-67593, 2018.

[22] S. Zhu, C. Zhu, W. Wang, "A novel image compression-encryption scheme based on chaos and compression sensing," *IEEE Access*, vol. 6, pp. 67095-67107, 2018.

[23] W. Feng, Y. He, H. Li, C. Li, "Cryptanalysis and improvement of the image encryption scheme based on 2D logistic-adjusted-sine map," *IEEE Access*, vol. 7, pp. 12584-12597, 2019.

[24] Y. Liu, X. Liu, Y. Zhao, "Security Crypt-analysis of NUX for the Internet of Things," *Security and Communication Networks,* vol. 2019, pp. 1-15, 2019.

[25] W.-Z. Yeoh, J. S. Teh, & M. I. Sazali, "μ^2: A lightweight block cipher," *Lecture Notes in Electrical Engineering,* vol. 603, 2020, pp. 281-290, doi:10.1007/978-981-15-0058-9_27

[26] S. Gnatyuk, B. Akhmetov, V. Kozlovskyi et al, "New secure block cipher for critical applications: Design, implementation, speed and security analysis," *Advances in Intelligent Systems and Computing,* vol. 1126, pp. 93-104, 2020.

[27] K. Jithendra, T. Shahana, "New Biclique cryptanalysis on full-round PRESENT-80 block cipher," *SN COMPUT. SCI.* vol. 1, article no. 94, 2020. https://doi.org/10.1007/s42979-020-0103-z

[28] Z. Liu, S. Han, Q. Wang et al., "New insights on linear cryptanalysis," *Sci. China Inf. Sci.* 63, 112104, 2020.

[29] H. Zodpe, A. Sapkal, "FPGA-Based high-performance computing platform for cryptanalysis of AES algorithm," *Advances in Intelligent Systems and Computing*, Springer, vol. 1025, pp. 637-646, 2020.

[30] M. Herrero-Collantes, J. C. Garcia-Escartin, "Quantum random number generators," *Rev. Mod. Phys.*, vol. 89, no. 1, 015004, 2017.

[31] P. Sušil, P. Sepehrdad, S. Vaudenay et al, "On selection of samples in algebraic attacks and a new technique to find hidden low degree equations," *Information Security and Privacy*, Cham: Springer, pp. 50-65, 2014.

[32] S. P. Jordan and Y. Liu, "Quantum cryptanalysis: Shor, Grover, and Beyond," *IEEE Security & Privacy*, vol. 16, no. 5, pp. 14-21, 2018.

***Berik B. Akhmetov**, PhD in Engineering, an Associate Professor, Rector of Yessenov University, (Aktau, Kazakhstan). Research interests: cybersecurity, cryptography and coding, secured information systems and technologies.*

***Sergiy O. Gnatyuk,** Doctor of Sciences in Cybersecurity, Associate Professor, Vice-Dean of Faculty for Cybersecurity, Computer and Software Engineering at National Aviation University (Kyiv, Ukraine). Research interests: QKD, cybersecurity, cryptography.*

***Vasyl M. Kinzeryavyy,** PhD in Cybersecurity, an Associate Professor of IT-Security Academic Department at National Aviation University (Kyiv, Ukraine). Research interests: construction and cryptanalysis of block ciphers and hash-functions, QKD, blockchain security.*

***Khalicha I. Yubuzova,** Master of Technical Sciences, Lecturer of the Academic Department "Cybersecurity, Information Processing and Storage" at Satbayev University (Almaty, Kazakhstan). Research interests: information security, cryptography, QKD, network technologies.*