# Studies on Cryptographic Security and Speed Analysis of New Advanced Block Cipher

Sergiy Gnatyuk[1] [0000-0003-4992-0564], Vasyl Kinzeryavyy[1] [0000-0002-7697-1503], Maksim Iavich[2] [0000-0002-3109-7971], Roman Odarchenko[1] [0000-0002-7130-1375], Rat Berdibayev[3] [0000-0002-8341-9645], Yuliia Burmak[4] [0000-0002-5410-6260]

[1] National Aviation University, Kyiv, Ukraine
s.gnatyuk@nau.edu.ua, v.kinzeryavyy@nau.edu.ua, odarchenko.r.s@ukr.net
[2] Scientific Cyber Security Association, Tbilisi, Georgia
m.iavich@scsa.ge
[3] Almaty University of Power Engineering and Telecommunications, Almaty, Kazakhstan
r.berdybaev@aues.kz
[4] Kyiv College of Communication, Kyiv, Ukraine
yu.burmac@ukr.net

**Abstract.** Today cryptographic methods use to provide confidentiality and integrity of the data. In other hand, there are many threats related to security breaches and restricted access data leakage in up-to-date information and communication technologies (ICT). The most popular and effective attacks are linear and differential cryptanalysis (LDC) as well as quantitative security assessment characterizing practical security against LDC is actual research task. Another valuable parameter is cryptographic data processing speed; as a rule it is decreasing in algorithms with high processing complexity. As time goes on some algorithms become worn out and outdated (i.e. DES, GOST 28147-89) as well as new more secure and high-speed algorithms are used in modern ICT (web-applications, IoT, blockchain, critical infrastructure). From this position, in this paper method of cryptographic security algorithms constructing for critical applications has been improved. This method uses substitution tables with increased capacity and randomized linear and non-linear operations. On the basis of this method, new advanced block cipher (BC) was proposed and its specifications were given. At the same time, analytical upper bounds of parameters characterized practical security of proposed BC against LDC were calculated. Besides, speed characteristics of developed BC were also evaluated. The results of experimental study showed that proposed cipher provides practical security against LDC with more high-speed in comparison with modern BC. Future research study can be related to practical cryptographic security assessment against other cryptanalysis methods.

**Keywords:** information security, cryptography, encryption, block cipher, cryptographic algorithm, practical security, linear and differential cryptoanalysis.



## 1. Introduction

The CIA triad is one of the most popular and valuable model of information security (cybersecurity) ensuring in information and communication technologies (ICT). It

contains three basic following characteristics: confidentiality, integrity and availability. Confidentiality and integrity provides by cryptographic methods and tools [1-3]. Particularly, integrity provides by hash-functions or EDS as well as confidentiality provides by using symmetric (secret key cryptography, SKC) [2] and assymetric (Public Key Crytpography, PKC) ciphers [3]. The encryption process by symmetric ciphers is faster approximately in $10^2$-$10^3$ times and it needs less computational capabilities.

Moreover, all cryptographic methods' the undeniable advantage is protection the data itself rather than access to it. The principal criterion of choosing cryptosystems is the security level against some categories of cyberattacks. But for some specifical targets, the cryptographic data processing speed (as in the case of PKC or some up-to-date applications based on SKC) plays a key role [4-5].

## 2. Related papers analysis and problem definition

Despite the diversity of modern cryptographic methods and tools, not all of them have required level of efficiency (security and speed) to provide guaranteed data protection. There are many threats related to security breaches and restricted access data leakage in up-to-date ICT. Also the development and cost reduction of ICT positively affects the effectiveness of cryptanalysis, one of the most effective methods of which is linear and differential cryptanalysis (LDC) [6-8].

In the paper [4] two high-performance reliable block ciphers (BC) were proposed and its speed and security against LDC was estimated in comparison with most effective modern BCs like AES, Kalyna etc. Latest research papers [7-11] are oriented on quantitative estimation of BC security against LDC.

As time goes on some algorithms become worn out and outdated (i.e. DES, GOST 28147-89). New more secure and high-speed algorithms are used in modern ICT (web-applications, IoT, blockchain, critical infrastructure). ICT development as well as cryptanalysis methods and tools enforces to cryptographic security methods improvements and creating new ciphers based on these [12-14]. From this viewpoint, the main purpose of this paper is to study the efficiency (security level and speed parameters) of the new advanced BC.

## 3. Mathematical background for method of cryptographic security algorithms constructing

Suppose $t'$, $p'$, $r'$, $q'$ are natural numbers, $t = 2t'$, $p = 2p'$, $r = 2r' + 1$, $n = tp$, $q = pq'$, $w = p$, $k = 2n$, $b = 2^{q'}$ (parameter $b$ defines the quantity of different substitution tables (substitutions), which can be used in the method). Then the $r$-rounded ciphering method $\Im$ with thesetof cleartext messages (messages to encrypt) $V_n = \{0,1\}^n$, the set of secret keys $V_k$ and the set of round keys $V_{n+q+w}$ can be described by following sequence of stages:

*Stage 1 – Round keys producing*

At this stage ther number of round keys $K_i$, $K_i \in V_{n+q+w}, i = \overline{1,r}$ is produced from the secret key $K$, $K \in V_k$.

*Step 1.1.* Decomposing secret key $K$, $K \in V_k$:

$$K = \left(B_{-4}, B_{-3}, B_{-2}, B_{-1}\right),\ B_j \in V_{n/2},\ j = \overline{-4,-1}. \quad (1)$$

*Step 1.2.* Producing vectors $B_j$, $B_j \in V_{n/2}$, $j = \overline{0,c-1}$, $c = \lceil 4r(n+q+w)/n \rceil$:

$$B_j = \begin{cases} \left(S\left(B_{j-4}, W_1, p'\right) \oplus \left(B_{j-2} <<< P_1\right) \oplus B_{j-1} \oplus Q_1\right) <<< B_{j-3} & , j \bmod 4 = 0 \\ \left(S\left(B_{j-3} \oplus B_{j-1}, W_2, p'\right) \oplus \left(B_{j-2} >>> P_2\right) \oplus Q_2\right) >>> B_{j-4} & , j \bmod 4 = 1 \\ \left(B_{j-4} \oplus \left(S\left(B_{j-3}\right) <<< P_3, W_3, p'\right) \oplus B_{j-1} \oplus Q_3\right) >>> B_{j-2} & , j \bmod 4 = 2 \\ \left(S\left(B_{j-4} <<< P_4, W_4, p'\right) \oplus B_{j-3} \oplus B_{j-2} \oplus Q_4\right) <<< B_{j-1} & , j \bmod 4 = 3 \end{cases}, \quad (2)$$

where $\oplus$ is the Boolean operation of binary vectors coordinate wise addition, $X <<< Y$ is the dynamic rotate left of bit sequence $X$ for $Y$ times, and $X >>> Y$ is the dynamic rotate right of the bit sequence $X$ for $Y$ times, $W_i$, $P_i$, $Q_i$ are some constants, $W_i$, $P_i$, $Q_i \in V_{n/2}$, $i = \overline{1,4}$.

The substitution $S$ is defined via following formula:

$$S(x, y, z) = \left(s_{y_{z-1}}(x_{z-1}), \ldots, s_{y_0}(x_0)\right),\ x = \left(x_{z-1}, \ldots, x_0\right), y = \left(y_{z-1}, \ldots, y_0\right), \quad (3)$$

where $x_j \in V_t$, $y_j \in V_{q'}$, $s_{y_j}$ is the substitution table for the set $V_t$ (one substitution table is chosen among $b$ possible variants by index $y_j$), $j \in \overline{0, z-1}$.

*Step 1.3.* Vectors $C_i, C_i \in V_e$, $i = \overline{1,r}$, $e = e'n/2$, $e' = \lceil 2(n+q+w)/n \rceil$ areformed by concatenation of vectors $B_j$, $B_j \in V_{n/2}$, $j = \overline{0,c-1}$, $c = \lceil 4r(n+q+w)/n \rceil$ in inverse order (to form one vector $C_i$ it should be used $e'$ number of vectors $B_j$):

$$C_i = \left(B_{c-1-(i-1)e'} \,\|\, B_{c-1-(i-1)e'-1} \,\|\, \ldots \,\|\, B_{c-1-(i-1)e'-e'+1}\right) \quad (4)$$

*Step 1.4.* Calculaion of round keys $K_i$, $K_i \in V_{n+q+w}, i = \overline{1,r}$:

$$K_i = \left(C_i >>> i\right) \bmod 2^{n+q+w}. \quad (5)$$

The obtained keys $K_i$, $K_i \in V_{n+q+w}, i = \overline{1,r}$ will be used for secret message encryprion and decryption.

*Stage 2 – Encryption procedure*

At this stage the secret message is encrypted $A = \left(A_1, A_2, A_3, \ldots, A_u\right)$, $A \in V_{n \cdot u}$, $A_j \in V_n$, $j = \overline{1,u}$, where $u$ is a natural number.

The encryption function of each $A_j \in V_n$, $j = \overline{1,u}$ is following:

$$F = f_{r, K_r} \circ \ldots \circ f_{1, K_1}. \quad (6)$$

The round function $f_{i,K_i}$ for all $x \in V_n$, $K_i \in V_{n+q+w}$, $i \in \overline{1,r}$ is described as follows:

$$f_{i,K_i}(x) = \begin{cases} \varphi\left(x \oplus k^{(1)}, k^{(2)}, k^{(3)}\right), if \quad i < r \\ S\left(x \oplus k^{(1)}, k^{(2)}, p\right), \quad if \quad i = r \end{cases}, \tag{7}$$

where $k^{(1)}$, $k^{(2)}$, $k^{(3)}$ are parts of round key $K_i$ ($k = \left(k^{(1)}, k^{(2)}, k^{(3)}\right)$, $k^{(1)} \in V_n$, $k^{(2)} \in V_q, k^{(3)} \in V_w$).

The substution $S$ is defined in (3) and the substitution $\varphi$ is defined by follow:

$$\varphi(x, y, h) = S(x, y, p)M(h), \; x \in V_n, \; y \in V_q, \; h \in V_w \tag{8}$$

where $x = \left(x_{p-1}, \ldots, x_0\right)$, $y = \left(y_{p-1}, \ldots, y_0\right)$, $x_j \in V_t$, $y_j \in V_{q'}$.

$M(h)$ is the invertible matrix $2p \times 2p$ over Galuis field $GF\left(2^{t'}\right)$, which depends on $h$, and the multiplication $S(x, y, p) = \left(s_{y_{p-1}}\left(x_{p-1}\right), \ldots, s_{y_0}\left(x_0\right)\right)$ on $M(h)$ in (8) is accomplished over this field in the following way:

1. Parameter $s_{y_j}\left(x_j\right)$ ($j \in \overline{0, p-1}$) is decomposed on 2 $t'$-bit parts.

($s_{y_j}\left(x_j\right) = \left(s_{y_j}\left(x_j\right)^{(1)}, s_{y_j}\left(x_j\right)^{(2)}\right)$, $s_{y_j}\left(x_j\right)^{(1)}, s_{y_j}\left(x_j\right)^{(2)} \in V_{t'}$).

2. The vector $B$ is formed from the part $s_{y_j}\left(x_j\right)$ ($j \in \overline{0, p}$):

$$B = s_{y_0}\left(x_0^{(1)}\right) || \, s_{y_0}\left(x_0^{(2)}\right) || \ldots || \, s_{y_{p-1}}\left(x_{y_{p-1}}{}^{(1)}\right) || \, s_{y_{p-1}}\left(x_{y_{p-1}}{}^{(2)}\right).$$

3. Vector $B$ and $M(h)$ multiplying is accomplished over binary vector identification $B_j$ $j \in \overline{0, 2p-1}$ ($B_j \in V_{t'}$) of the matrix $M(p)$ elements.

## 4. Security analysis

On the basis of paper [9], for the proposed method analytical upper bounds of the parameters that characterize its practical security against cyberattacks of LDC are obtained as following:

$$EDP(\Omega) \le \tilde{\Delta}_{\oplus}^{\,r'\lceil B_M/2\rceil+1} \le \Delta_{\oplus}^{\,r'\lceil B_M/2\rceil+1}, \tag{9}$$

$$ELP(\Omega) \le \tilde{\Lambda}_{\oplus}^{\,r'\lceil B_M/2\rceil+1} \le \Lambda_{\oplus}^{\,r'\lceil B_M/2\rceil+1}, \tag{10}$$

where $EDP(\Omega)$ is the average probability of differential characteristic $\Omega$, $ELP(\Omega)$ is the average probability of linear characteristic $\Omega$, $B_M$ is $M$ matrix branching index, and the parameters $\Delta_{\oplus}$, $\Lambda_{\oplus}$, $\tilde{\Delta}$, $\tilde{\Lambda}$ are defined via the following formulas:

$$\Delta_{\oplus} = \max\left\{d_{\oplus}^{(s_j)}(\alpha, \beta) : \alpha, \beta \in V_t \setminus \{0\}, j \in \overline{0, b-1}\right\}, \tag{11}$$

$$\Lambda_{\oplus} = \max\left\{l^{(s_j)}(\alpha, \beta) : \alpha \in V_t, \beta \in V_t \setminus \{0\}, j \in \overline{0, b-1}\right\}, \tag{12}$$

$$\tilde{\Delta}_{\oplus} = \max\left\{ b^{-1} \sum_{j=0}^{b-1} d_{\oplus}^{(s_j)}(\alpha, \beta) : \alpha, \beta \in V_t \setminus \{0\} \right\}, \quad (13)$$

$$\tilde{\Lambda}_{\oplus} = \max\left\{ b^{-1} \sum_{j=0}^{b-1} l^{(s_j)}(\alpha, \beta) : \alpha \in V_t, \beta \in V_t \setminus \{0\} \right\}. \quad (14)$$

In (11) – (14) $d_{\oplus}^{(s_j)}$ is the difference table of the substitution $s_j$ ( $j \in \overline{0, b-1}$) over the bitwise addition operation modulo 2 and $l^{(s_j)}(\alpha, \beta)$ are the tables of linear approximation of the substitution $s_j$ ( $j \in \overline{0, b-1}$) over this operation.

## 5. New advanced BC development

New advanced BC is developed on the basis of proposed method. Such parameters were chosen for he purposes of this BC: $t' = 8$, $t = 2t' = 16$ (substitution tables capacity), $p' = 4$, $p = 2p' = 8$, $r' = 4$, $r = 2r' + 1 = 9$ (number of rounds), $n = tp = 128$ (size of data block in bits), $q' = 3$, $q = pq' = 24$, $b = 2^{q'} = 8$ (8 substitution tables are used over the set $V_{16}$), $w = 8$, $k = 2n = 256$ (size of secret keys in bits).

The proposed cipher works with 128-bit data blocks and supports a 256 bits length secret key. When expanding a secret key, the required number of 160-bit round keys is generated ( $n + q + w = 128 + 24 + 8 = 160$ ). Data blocks and extended keys are represented as 8×2 byte matrix.

For proposed BC the *producing round key sprocedure* is accomplished via formulas (1) – (5).

At the first step one 256-bit round key $K$ is divided into 4 parts: $K = (B_{-4}, B_{-3}, B_{-2}, B_{-1})$ 64 bit lentgth for each.

Then at the second step 2 auxilliary 64-bit vectors are calculated $B_j$, $j = \overline{0, 44}$ ( $c = \lceil 4r(n+q+w)/n \rceil = 4 \cdot 9 \cdot (128 + 24 + 8)/128 = 45$ ). Here with it is used 64-bit constants $W_i$, $P_i$, $Q_i$, $i = \overline{1, 4}$ (see the values of these constants in the Table 1).
Also in step two the substitution $S$ uses 8 substitution tables $16 \times 16$ bits.

These substitution tables are set up using the calculation of the field inverse element $(C / X)^{-1} \in GF(2^{16})$ with the further execution of Affine transformation over the $GF(2)$

$$S(X) = M \cdot (C / X)^{-1} + V, \quad (15)$$

where $X, C, V \in GF(2^{16})$, and $M$ is the invertible square matrix over $GF(2)$, size of which is $16 \times 16$.

The parameters $C$, $V$ and $M$ are presented in hexadecimal values in the Table 2 (each row of matrix $M$ is presented as a single hexadecimal number).

**Table 1.** The values of 64-bit constants, which are used in the BC

| Constant | The hexadecimal value of constant |
|---|---|
| $W_1$ | E702 DDCB BDEC BDD5 |
| $W_2$ | 4AB4 2988 9FE1 017A |
| $W_3$ | 7BED 569B 1C78 2259 |
| $W_4$ | 15A7 5069 7EF5 439C |
| $P_1$ | 89FC BB23 4DB0 D712 |
| $P_2$ | 1970 CB03 479F E7B2 |
| $P_3$ | 2FA8 934D EB78 0517 |
| $P_4$ | 07C4 20F9 87D1 0ECA |
| $Q_1$ | 8713 DC71 F897 4562 |
| $Q_2$ | D896 3354 4110 80BA |
| $Q_3$ | 5CB1 AE69 0140 DB83 |
| $Q_4$ | A09B E122 36B4 C17A |

**Table 2.** Parameters $C$, $V$ та $M$, which were used for subs tables setting up over the set $V_{16}$

| Subs table index | *M* | *C* | *V* |
|---|---|---|---|
| 0 | {0652,0CA4,1948,3290,6520,CA40,9481,2903, 5206,A40C,4819,9032,2065,40CA,8194,0329} | 06FB | 09F0 |
| 1 | {32ED,65DA,CBB4,9769,2ED3,5DA6,BB4C,7699, ED32,DA65,B4CB,6997,D32E,A65D,4CBB,9976} | 6A8C | 760E |
| 2 | {32F0,65E0,CBC0,9781,2F03,5E06,BC0C,7819, F032,E065,C0CB,8197,032F,065E,0CBC,1978} | 7992 | 200B |
| 3 | {32FA,65F4,CBE8,97D1,2FA3,5F46,BE8C,7D19, FA32,F465,E8CB,D197,A32F,465F,8CBE,197D} | 01AC | 1E00 |
| 4 | {3975,72EA,E5D4,CBA9,9753,2EA7,5D4E,BA9C, 7539,EA72,D4E5,A9CB,5397,A72E,4E5D,9CBA} | 7AE3 | 6EDF |
| 5 | {3985,730A,E614,CC29,9853,30A7,614E,C29C, 8539,0A73,14E6,29CC,5398,A730,4E61,9CC2} | 697C | 40CD |
| 6 | {3B2B,7656,ECAC,D959,B2B3,6567,CACE,959D, 2B3B,5676,ACEC,59D9,B3B2,6765,CECA,9D95} | 4724 | 68FD |
| 7 | {3C54,78A8,F150,E2A1,C543,8A87,150F,2A1E, 543C,A878,50F1,A1E2,43C5,878A,0F15,1E2A} | 02EE | 75D5 |

In the third step the 192-bit vectors $C_i, C_i \in V_{192}$, $i = \overline{1,9}$ ($e' = \lceil 2(n+q+w)/n \rceil = 3$, $e = e'n/2 = 192$) are formed. Then 160-bit round keys $K_i$, $i = \overline{1,9}$ are formed.

For this BC *the encryption procedure* is accomplished over the formulas (6) – (8). See the pseudocode of the encryption procedure on the Fig.1.

The operation $AddKeyMod2(state, SubKey^{(1)})$ implies a bitwise modulo 2 addition of 2 corresponding bits of the round key $SubKey^{(1)}$ and the data block $state$.

$MixColumns(state)$ operation rempresents the linear transformation of matrix $state$. During this operation each 8-byte column of data block $state$ is considered as a polynomial over a field $GF(2^8)$ with 8 terms, which is multiplied by fixed polynom ( $c(x)$ raised to the power of 7 over the modulo $x^8+1$. As a polynomial $c(x)$ was chosen the following polinomial: $c(x)=3x^7+7x^6+x^5+3x^4+7x^3+4x^2+1Dx+1$ (factors are represented in hexadecimal format). As an irreducible polynomial the following polynomial was chosen: $m(x)=x^8+x^7+x^5+x^4+x+1$.

***Proposed BC encryption procedure***

Input: 128-bit datab lock $state$, 160-bit round keys

$SubKey_i=(SubKey_i^{(1)},SubKey_i^{(2)},SubKey_i^{(3)})$, $i=\overline{0,r}$,

$SubKey_i^{(1)}\in V_{128}$, $SubKey_i^{(2)}\in V_{24}$, $SubKey_i^{(3)}\in V_8$.

Output: 128-bit data block $state$.

1. $state=AddKeyMod2(state,SubKey_0^{(1)})$;
2. *For* $i=1,\ i<r,\ i++$ *do*
2.1. $state=SubBytes(state,SubKey_i^{(2)},8)$;
2.2. $state=ShiftRows(state,SubKey_i^{(3)})$;
2.3. $state=MixColumns(state)$;
2.4. $state=AddKeyMod2(state,SubKey_i^{(1)})$;
3. $state=SubBytes(state,SubKey_r^{(2)},8)$;
4. $state=ShiftRows(state,SubKey_r^{(3)})$;
5. $state=AddKeyMod2(state,SubKey_r^{(1)})$;
6. *return state*.

**Fig. 1.** The new BC encryprion procedure pseudocode

In $SubBytes(state,SubKey^{(2)},8)$ operation the tabular substitution of every 16 bits of the data block $state$ is performed.

This BC uses 8 tables over the set $V_{16}$, where in the choise of the particular table in each round depends on the part of round key $SubKey^{(2)}$ according to the formula (3).

The substitution tables were generated according to the formula (15), the parameters $C$, $V$ and $M$, used in generation are presented in Table 2. Substition tables datais selected so that there are no fixed points,and also that for each substitution table of BC the equality for the parameters is executed: $\Delta_{\oplus}=\Lambda_{\oplus}=2^{-14}$.

In $ShiftRows(state,SubKey^{(3)})$ operation depending on the part of the round keys $SubKey^{(3)}$ a byte wise shift of elements in the rows of the matrix $state$ is performed. The length of the round key $SubKey^{(3)}$ part is 8 bit, so each bit of current vector affects on the shift of corresponding row of the matrix $state$.

For instance, if the first bit of the vector $SubKey^{(3)}$ equals 1, then the values of the columns of the first matrix $state$ row are swapped, if the first bit of the vector $SubKey^{(3)}$ equals 0, then the values of columns are not changed. See *decryption procedure pseudocode* at the Fig. 2.

***Proposed BC decryption procedure***

Input: 128-bit data block $state$ ,160-bit round keys

$SubKey_i = \left(SubKey_i^{(1)}, SubKey_i^{(2)}, SubKey_i^{(3)}\right)$, $i = \overline{0, r}$,

$SubKey_i^{(1)} \in V_{128}$, $SubKey_i^{(2)} \in V_{24}$, $SubKey_i^{(3)} \in V_8$.

Output: 128-bit data-block $state$.

1. $state = AddKeyMod2\left(state, SubKey_r^{(1)}\right)$;
2. $For \quad i = 1, \quad i < r, \quad i{+}{+} \quad do$
2.1. $state = ShiftRows\left(state, SubKey_{r-i+1}^{(3)}\right)$;
2.2. $state = InvSubBytes\left(state, SubKey_{r-i+1}^{(2)}\right)$;
2.3. $state = AddKeyMod2\left(state, SubKey_{r-i}^{(1)}\right)$;
2.4. $state = InvMixColumns\left(state\right)$;
3. $state = ShiftRows\left(state, SubKey_1^{(3)}\right)$;
4. $state = InvSubBytes\left(state, SubKey_1^{(2)}\right)$;
5. $state = AddKeyMod2\left(state, SubKey_0^{(1)}\right)$;
6. $return \; state$.

**Fig. 2.** The new BC decryption procedure pseudocode

The $InvMixColumns\left(state\right)$ operation is a linear transformation of the matrix $state$, which is inverse to $MixColumns\left(state\right)$ operation. In this operation every 8-byte column of a data block $state$ is considered as a polynomial over a field $GF\left(2^8\right)$ with 8 terms, which is multiplied by the fixed polynomial $d\left(x\right)$ raised to the power of 7 modulo $x^8 + 1$.

The following polynomial is chosen as a polynomial $d\left(x\right)$: $d\left(x\right) = 7Ax^7 + A1x^6 + F8x^5 + EEx^4 + 29x^3 + 89x^2 + EBx + 51$ (factors are represented in hexadecimal format).

In the $InvSubBytes\left(state, SubKey^{(2)}\right)$ operation the tabular substitution of each 16 bit of data block $state$. This operation is inverse to $SubBytes\left(state, SubKey^{(2)}\right)$ operation, so it uses the inverse substitution tables in comparing with $SubBytes\left(state, SubKey^{(2)}\right)$ tables.

## 6. Experimental study and discussion

For experimental study purposes (security and speed assessment), developed BC was implemented as a console application.

The *sequences statistical properties*, created using this application (in the counter mode), were investigated in NIST STS statistical tests environments [15] as well as in DIEHARD technique. The statistical portraits of the proposed BC are shown in Fig. 3. For comparison purposes, the results of the sequences testing generated by proposed BC, GOST 28147-89, Kalyna, AES ciphers are given in Table 3.

**Table 3.** Sequense testing resuls using NIST STS

| Generator | Number of passed tests | |
|---|---|---|
| | 99% sequenses | 96% sequenses |
| BBS | 132 (70,2%) | 188 (100%) |
| Kalyna | 137 (72,9%) | 188 (100%) |
| GOST 28147-89 | 130 (69,1%) | 186 (98,9%) |
| AES | 133 (70,7%) | 188 (100%) |
| Proposed BC | 141 (75,0%) | 188 (100%) |

As can be seen from the results, proposed BC passed a comprehensive control over the NIST STS (Fig. 3) and DIEHARD techniques and showed no worse results than the ciphers above.

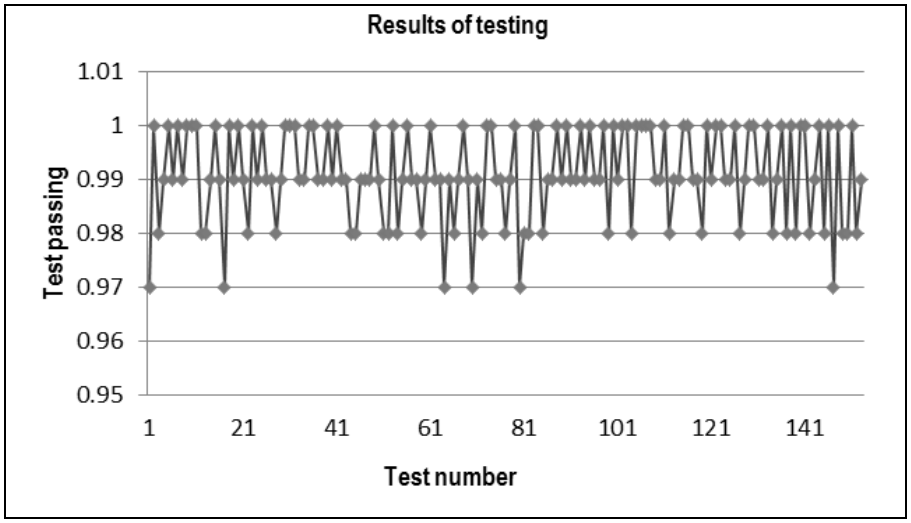


**Fig. 3.** Proposed BC testing results in NIST STS

The speed characteristics of ciphers are also studied. It has been shown experimentally that the proposed BC is faster than the GOST 28147-89 cipher approximately in 3.11 times, and 1,27 times or the Kalyna and AES ciphers (see Table 4). The research was conducted in the same conditions on Intel (R) Core (TM) i7-2600K CPU 3.4 GHz.

**Table 4.** The BCs speed characteristics comparison

| BC | Encryption speed (MB/s) |
|---|---|
| AES-256 | 64,93 |
| Kalyna-256 | 71,19 |
| GOST 28147-89 | 29,02 |
| Proposed BC | 90,48 |

Also the *security ratings* of the proposed BC over the methods of LDC are calculated. Accorfing to (9) – (14) formulas the parameters upper bounds values, characterizing this BC practical security against LDC methods are calculated: $\Delta_{\oplus} = \Lambda_{\oplus} = 2^{-14}$, $r' = 4$, $B_M = 9$ – $EDP(\Omega) \le 2^{-294}$, $ELP(\Omega) \le 2^{-294}$ and number of round keys $r = 9$. This results shows that if the $r \ge 9$ then the practical security of the proposed BC over the foregoing cryptoanalysis methods [18-21] is provided.

## 7. Conclusions and future research study

In this paper the cryptographic security method was developed, which can increase the effectiveness of cryptographic security by using new procedures sequence of operations in generating round keys and encryption (using substitution tables with increased capacity and randomized linear and non-linear operations).

On the basis of this method, symmetric BC was developed. The values of parameters upper bounds characterizing its practical resistibility to cyber attacks of LDC are calculated.

Under the same conditions, experimental studies were carried out to evaluate the speed characteristics of ciphers, which showed that proposed BC is faster than the GOST 28147-89 cipher approximately in 3.11 times, and 1,27 times for the Kalyna and AES ciphers.

Also, the statistical properties of the sequences generated by proposed BC were investigated. As a result, it was shown that this BC cipher passed a complex control of the NIST STS and DIEHARD techniques and showed no worse results than other ciphers.

Future research study can be related with practical cryptographic security assessment of proposed BC against other cryptanalysis methods [16-17].

## Acknowledgments

This scientific work was financially supported as a part of Ukrainian Young Scientists Project of Ministry of Education and Science of Ukraine as well as joint project of Shota Rustaveli National Science Foundation of Georgia and Science & Technology Center in Ukraine, Project N6321 [STCU-2016-08].

## References

1. Gnatyuk S., Akhmetov B., Kozlovskyi V., Kinzeryavyy V., Aleksander M., Prysiazhnyi D. “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.
2. Yeoh W. -., Teh J. S., & Sazali M. I. "$\mu^2$: A lightweight block cipher", Lecture Notes in Electrical Engineering, vol. 603, pp. 281-290, 2020.
3. A. Kuznetsov, I. Svatovskij, N. Kiyan and A. Pushkar'ov, "Code-based public-key cryptosystems for the post-quantum period", Proceedings of 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkiv, 2017, pp. 125-130.
4. S. Gnatyuk, V. Kinzeryavyy, M. Iavich, D. Prysiazhnyi, Kh. Yubuzova, "High-Performance Reliable Block Encryption Algorithms Secured against Linear and Differential Cryptanalytic Attacks", CEUR Workshop Proceedings, vol. 2104, pp. 657-668, 2018.
5. Gorbenko I., Kuznetsov A., Gorbenko Y., Vdovenko S., Tymchenko V. and Lutsenko M. "Studies on Statistical Analysis and Performance Evaluation For Some Stream Ciphers", International Journal of Computing, vol. 18 (1), pp. 82-88, 2019.
6. Zodpe H., Sapkal A. "FPGA-Based High-Performance Computing Platform for Cryptanalysis of AES Algorithm", Advances in Intelligent Systems and Computing, Springer, vol. 1025, pp. 637-646, 2020.
7. Yang D., Qi W.-F., Chen H. -J. "Provable security against impossible differential and zero correlation linear cryptanalysis of some feistel structures", Designs, Codes, and Cryptography, vol. 87(11), pp. 2683-2700, 2019.
8. Liu H., Kadir A., Xu, C. "Cryptanalysis and constructing S-box based on chaotic map and backtracking". Applied Mathematics and Computation, vol. 376, 125153, 2020.
9. A. Alekseichuk, L. Kovalchuk, E. Skrynnik, "Rating of practical resistance of Kalyna block cipher relative to the difference methods, linear cryptanalysis and algebraic attacks based on homomorphisms", Applied Radio Electronics, 2008, 7 (3), pp. 203-209.
10. C. Blondeau, K. Nyberg, "New Links between Differential and Linear Cryptanalysis", Proc. of Annual Intern. Conf. on the Theory and Applications of Cryptographic Techniques "Advances in Cryptology, EUROCRYPT-2013", Springer Verlag, pp. 388-404, 2013.
11. M. Kanda, "Practical security evaluation against differential and linear cryptanalyses for Feistel ciphers with SPN round function", Selected Areas in Cryptography, SAC 2000, Proceedings, Springer Verlag, 2001, pp. 324-338.
12. Hu Z., Gnatyuk S., Kovtun M., Seilova N. "Method of searching birationally equivalent Edwards curves over binary fields", Advances in Intelligent Systems and Computing, vol. 754, pp. 309-319, 2019.
13. O. Dawood, A. Rahma, A. Hossen, "The New Block Cipher Design (Tigris Cipher)", International Journal of Computer Network and Information Security (IJCNIS), vol. 7, No.12, pp.10-18, 2015.
14. Gnatyuk S., Kinzeryavyy V., Kyrychenko K., Yubuzova Kh., Aleksander M. and Odarchenko R. "Secure Hash Function Constructing for Future Communication Systems and Networks", Advances in Intelligent Systems and Computing, vol. 902, pp. 561-569, 2020.
15. A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications. NIST Special Publication 800-22, May 15, 2001, 164 p.
16. Y. Liu, X. Liu, Y. Zhao, "Security Cryptanalysis of NUX for the Internet of Things", Security and Communication Networks, vol. 2019, pp. 1-15, 2019.
17. S. P. Jordan and Y. Liu, "Quantum Cryptanalysis: Shor, Grover, and Beyond", IEEE Security & Privacy, vol. 16, no. 5, pp. 14-21, 2018.
18. Liu Z., Han S., Wang Q. et al, "New insights on linear cryptanalysis", Sci. China Inf. Sci. 63, 112104, 2020.

19. Yeoh W., Teh J. S., & Sazali M. I. "$\mu^2$: A lightweight block cipher", Lecture Notes in Electrical Engineering, vol. 603, pp. 281-290, 2020, doi:10.1007/978-981-15-0058-9_27
20. Liu H., Kadir A., Xu C. "Cryptanalysis and constructing S-box based on chaotic map and backtracking". Applied Mathematics and Computation, vol. 376, 125153, 2020.
21. 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.