computing@computingonline.net
www.computingonline.net

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

HEURISTIC METHODS FOR THE DESIGN OF CRYPTOGRAPHIC BOOLEAN FUNCTIONS

Illarion Moskovchenko [1,2], Alexandr Kuznetsov [2,3], Sergii Kavun [4], Berik Akhmetov [5], Ivan Bilozertsev [2,3], Serhii Smirnov [6]

[1] Ivan Kozhedub Kharkiv National Air Force University, Sumska str., 77/79, Kharkiv, 61023, Ukraine
[2] V. N. Karazin Kharkiv National University, Svobody sq., 6, Kharkiv, 61022, Ukraine,
illarion_moskovchenko@ukr.net, kuznetsov@karazin.ua, ivanbelozersevv.jw@gmail.com
[3] JSC "Institute of Information Technologies", Bakulin St., 12, Kharkiv, 61166, Ukraine
[4] Kharkiv University of Technology "STEP", Malom'yasnitska st. 9/11, 61010, Kharkiv, Ukraine, kavserg@gmail.com
[5] Yessenov University, 32 microdistricts, 130003, Aktau, The Republic of Kazakhstan, akhmetov@yu.edu.kz
[6] Central Ukrainian National Technical University, University Avenue 8, Kropyvnytskyi, 25006, Ukraine,
smirnov.ser.81@gmail.com

Paper history:
Received 20 November 2018
Received in revised form 28 June 2019
Accepted 10 September 2019
Available online 30 September 2019

Keywords:
heuristic methods;
cryptographic Boolean functions;
symmetric cryptography;
nonlinear substitute blocks.

Abstract: In this article, heuristic methods of hill climbing for cryptographic Boolean functions satisfying the required properties of balance, nonlinearity, autocorrelation, and other stability indicators are considered. A technique for estimating the computational efficiency of gradient search methods, based on the construction of selective (empirical) distribution functions characterizing the probability of the formation of Boolean functions with indices of stability not lower than required, is proposed. As an indicator of computational efficiency, an average number of attempts is proposed to be performed using a heuristic method to form a cryptographic Boolean function with the required properties. Comparative assessments of the effectiveness of the heuristic methods are considered. The results of investigations of the cryptographic properties of the formed Boolean functions in comparison with the best known assessments are given. On the basis of the conducted research, it can be concluded that the functions constructed in accordance with the developed method have high persistence indexes and exceed the known functions by these indicators.

1. INTRODUCTION

An important element of most modern symmetric ciphers are non-linear replacement blocks [1-7], which are described with the help of Boolean or, in general, vector cryptographic functions [6]. Indicators of the cryptographic strength of such functions (balance, nonlinearity, autocorrelation, etc.) directly affect the efficiency of symmetric ciphers, their resistance to most modern cryptanalytical attacks [5-15]. In particular, the algebraic properties of S-blocks of modern block ciphers are investigated in [5-7] and their influence on sustainability to algebraic cryptanalysis is shown. In [8-11], combinatorial properties of non-linear knots in the context of the security evaluation of various encryption modes and key schedules were investigated. In [12, 13], the influence of S-blocks on avalanche effects, differential and linear properties of block ciphers is investigated. The papers [14, 15] are dedicated to the study of the properties of nonlinear replacement nodes in modern stream ciphers in comparison with the "Strumok" algorithm proposed as a new standard of stream encryption in Ukraine [16].

Methods for constructing S-blocks are investigated by many authors, for example, in [17-20]. However, the most developed and widespread is the mathematical apparatus of cryptographic Boolean functions [21-28]. In particular, a new recursive construction of a Boolean function with maximum algebraic immunity is presented in [21]; in [22, 23] genetic algorithms for constructing Boolean functions with the required cryptographic properties are examined; in [24] the method of simulation of annealing is investigated; evolutionary methods are studied in [25, 26]; papers [27, 28] are dedicated to the heuristic methods of gradient search.

The purpose of this paper is to continue studies of the method of gradient descent, first proposed in [28], an assessment of its computational complexity in comparison with the closest analog in [27]. For this purpose, the necessary terms and definitions in Section 2 are introduced; the heuristic methods studied in [27, 28] are summarized in Section 3 and the calculated data for the required number of operations for the realization of gradient descent (Table I) is provided. Section 4 evaluates the properties of the gradient-lift method for the formation of high non-linear correlation-immune cryptographic Boolean functions. In section 5 a methodology for assessing the effectiveness of heuristic methods is proposed and the results of comparative studies are represented. In particular, it has been shown that the method of gradient descent in [28] for a significantly smaller number of iterations (in dozens of times) makes it possible to form cryptographic Boolean functions with the required indices of nonlinearity and autocorrelation. Section 6 presents the results of investigations of the cryptographic properties of the formed Boolean functions and compares them with the best known assessments. In conclusion, the obtained results are summarized and directions for further research are formulated briefly.

2. INDICES OF STABILITY OF CRYPTOGRAPHIC BOOLEAN FUNCTIONS

The basic concepts and definitions of the mathematical apparatus of Boolean algebra used in evaluating the effectiveness of non-linear nodes to replace symmetric ciphers were introduced in [21-28].

The Boolean function f of *n* variables is the function [21-28], variables is the function that maps from the field $GF(2^n)$ of all binary vectors $x = (x_1, \ldots, x_n)$ of length n to the field $GF(2)$. Usually Boolean functions are represented in algebraic normal form (ANF) and are considered as the sum of the products of the component coordinates.

The algebraic degree deg (f) is the degree of the longest summand of a function represented in an algebraic normal form. Algebraic degree reflects the resistance to analytical attacks, designed to reduce this function to cryptographically weak (linear).

The sequence of the function f is (1,-1) – a sequence, defined as $((-1)^{f(\alpha_0)}, (-1)^{f(\alpha_1)}, \ldots, (-1)^{f(\alpha_{2^n-1})})$ [21-28].

The truth table of a function f is (0,1) - a sequence, defined as $(f(\alpha_0), f(\alpha_1),\ f(\alpha_{2^n-1})\ )$ [21-28].

The sequence of the function *f* is *balanced* if its (0,1) -sequence ((1, -1) - sequence) contains the same number of zeros and ones (ones and minus ones). The function *f* is balanced if its sequence is balanced [21-28].

The balance of the function is an indicator of stability, reflecting the weakness of the output sequence to statistical attacks.

An affine function f is a function of the form $f = a_1x_1 \oplus \ldots \oplus a_nx_n \oplus c$, где $a_j,\ c \in GF(2)$, $j = 1, 2, \ldots, n$. Function *f* is called *linear*, if $c = 0$ [21-28].

The Hamming weight of the vector α ((0,1)-sequence α), denoted by $W(\alpha)$, is the number of ones in the vector (sequence) [21-28].

The Hamming distance d (f,g) between the sequences of two functions *f* and *g* is the number of positions in which the sequences of these functions are different [21-28].

The nonlinearity of the NS transformation is the minimum Hamming distance between the output sequence *S* and all output sequences of affine functions over a certain field [21-28]: $N_S = min \{d(S,\varphi)\}$, where φ - is the set of affine functions.

The nonlinearity of the function N_f is the minimal Hamming distance N_f between the function *f* and all affine functions over $GF\ (2^n)$ [21-28]: where φ is the set of affine functions.

For an arbitrary function *f*, the nonlinearity of N_f over $GF\ (2^n)$ can reach [21-28]: $N_f \le 2^{n-1} - 2^{n/2-1}$. For a balanced function *f* over $GF\ (2^n)$ ($n \ge 3$), the nonlinearity of N_f can reach [21-28]:

$$N_f \le \begin{cases} 2^{n-1} - 2^{n/2-1} - 2\ , n = 2k, \\ \lfloor\lfloor 2^{n-1} - 2^{n/2-1} \rfloor\rfloor, n = 2k+1, \end{cases},$$

where $\lfloor\lfloor x \rfloor\rfloor$ – is the maximal even integer less than or equal to *x*.

Non-linearity of the function is an indicator reflecting the stability of functions to correlative (linear) attacks.

The function *f* has a *correlation immunity* of order *k* if the output sequence of the function $y \in Y$ is statistically independent of any subset of *k* input coordinates [21-28]: $\forall \{x_1, \ldots, x_k\}$ $P(y \in Y / \{x_1, \ldots, x_k\} \in X) = P(y \in Y)$.

Equivalent definition of correlation immunity in terms of the Walsh transform [21-28]: the function *f* over the field $GF(2^n)$ has correlation immunity of order k, $CI(k)$ if its Walsh transform satisfies the equality $F(\omega) = 0$ for all $\omega \in V_n$ such as $1 \leq W(\omega) \leq k$: $\forall \omega \in V_n$, $F(\omega) = 0$, $CI(f) = k$.

The Walsh transformation $F(\omega)$ of the function f over the field $GF(2^n)$ is defined as the real-valued function [21-28]:

$$F(\omega) = 2^{-n} \sum\nolimits_x (-1)^{f(x) \oplus \langle \omega, x \rangle},$$

where $\omega \in V_n$, $f(x)$, $\langle \omega,x \rangle \in N$ ($\langle \omega,x \rangle$ -is the scalar product $w_1x_1 \oplus \ldots \oplus w_nx_n$) .

Correlation-immune function of the k-th order is a function possessing correlation immunity of the order of k. Balanced correlation-immune functions are called *elastic functions*.

Function f over the field GF (2^n) satisfies [21-28]:

- the propagation criterion relative to the vector α, PC(α), if function $f(\mathrm{x}) \oplus f(\mathrm{x} \oplus \alpha)$ is balanced, $x \in V_n$, where $x = (x_1, x_2, \ldots, x_n)$:

$$P(f(\mathrm{x}) = f(\mathrm{x} \oplus \alpha)) = \frac{1}{2};$$

- the propagation criterion of the k-th order, $KP(k)$, if the propagation criterion with respect to all vectors is satisfied $\alpha \in V_{\mathrm{n}}$ under $1 \leq W(\alpha) \leq k$:

$$P(f(\mathrm{x}) = f(x \oplus \alpha)) = \frac{1}{2} \ , \forall \alpha : 1 \leq W(\alpha) \leq k;$$

- strict avalanche criterion, SAC, if f satisfies the propagation criterion of degree 1:

$$P(f(\mathrm{x}) = f(\mathrm{x} \oplus \alpha)) = \frac{1}{2}, \ \forall \alpha : W(\alpha) = 1.$$

The degree of correlation immunity/propagation criterion reflects the stability of the functions to correlation attacks, designed to find the linear properties of this function [29-40].

Function f over GF (2^n) is called a bent function [21-28], if

$$2^{-n/2} \sum_{x \in V_n} (-1)^{f(x) \oplus \langle \beta, x \rangle} = \pm 1$$

for all $\beta \in V_n$.

The sequence of a bent function is called a *bent sequence*. For bent functions, the following assertions are valid [21-28]:

- $\langle \xi, \ell \rangle = \pm 2^{n/2}$ for any affine sequence ℓ of length 2^n;
- $f(x) \oplus f(x \oplus \alpha)$ is balanced $\forall \alpha \in V_n$, $W(\alpha) \neq 0$;
- $f(x) \oplus \langle \alpha, x \rangle$ takes the value of one $2^{n-1} \pm 2^{n/2-1}$ times $\forall \alpha \in V_n$;
- $f(x) \oplus h(x)$, where $h(x)$ – affine function, is also a bent function.

Autocorrelation function $\hat{r}(s)$ for $s \in 0 \ldots 2^n - 1$ is defined as

$$\hat{r}(s) = \sum_{x=0}^{2^n-1} \hat{f}(x) \hat{f}(x \oplus s) \quad .$$

The value of autocorrelation reflects the stability of the functions to the class of analytic attacks, designed to find a correlation between the fragments of the function [29-40].

The function f satisfies the propagation characteristic m if:

$$(1 \leq |s| \leq m) \Rightarrow |\hat{r}(s)| = 0.$$

Similarly, the autocorrelation AC (f) of the function f is defined as the module of the largest value of $\hat{r}(s)$:

$$AC(f) = \max_{s \neq 0} \left| \sum_{ч} \hat{f}(x) \hat{f}(x \oplus s) \right| = \max_{s \neq 0} |\hat{r}(s)| \quad .$$

Autocorrelation $\hat{r}(s)$ ensures the leakage of the information flow from the input to the output of the function [29-40].

3 HEURISTIC METHODS OF HILL CLIMBING

Heuristic methods of gradient search are investigated in this article. In particular, the method of gradient lift of W. Millan, A. Clark, E. Dawson, 1997 [27] and the method of gradient descent developed on its basis [28].

3.1 HEURISTIC METHOD OF GRADIENT LIFTING

The essence of the method is to increase the nonlinearity of an arbitrary Boolean function by complementing some position in the truth table of the original function. Each position of the truth table corresponds to unique input data. The method allows to create a complete list of such input data of the function, that the complementation of any output position corresponding to this input in the truth table will increase the nonlinearity of this function. The list of such positions in the truth table is denoted as 1 - *Improvement Set* of the function f (x), or 1 - IS_f [27].

Definition 1 [27]. $g(x) = f(x) \oplus 1$ for $x = x_a$ and $g(x) = f(x)$ for all other x. If $N_g > N_f$, then $x_a \in 1 - IS_f$.

In [27] a fast systematic method for determining the set $1 - IS_f$ of a given Boolean function is presented using its truth table and Walsh-Hadamard transforms. To find the set $1 - IS_f$ of a given Boolean function, it is first necessary to determine the values of Walsh-Hadamard transform coefficients that correspond to values close to the absolute value of the maximum coefficient, WH_{max}.

Definition 2. *f(x)* is a Boolean function with a Walsh-Hadamard transform *F (w)*, where WHmax denotes the maximum absolute value of F(w). One or more linear functions *Lw(x)* having a minimal distance to the function f(x), and for the data w, the equality $|F(w)| = WH_{max}$ will exist.

The following set is defined as:

$$W_1^+ = \{w\colon F(w) = WH_{max}\} \text{ and}$$

$$W_1^- = \{w\colon F(w) = -\, WH_{max}\}.$$

Also sets w for which the values of *WHT* are close to the maximum are defined:

$$W_2^+ = \{w\colon F(w) = WH_{max} - 2\},$$

$$W_2^- = \{w\colon F(w) = -\,(WH_{max} - 2)\},$$

$$W_3^+ = \{w\colon F(w) = WH_{max} - 4\}$$

$$\text{and } W_3^- = \{w\colon F(w) = -\,(WH_{max} - 4)\}.$$

When the truth table changes exactly in one place, all *WHT* values change to +2 or -2. It follows that to increase the nonlinearity all *WHT* values in the set W_1^+ must be changed to -2, all *WHT* values in the set W_1^- must be changed to 2 and also all *WHT* values in the set W_2^+ must be changed to -2, all *WHT* values in the set W_2^- must be changed to 2. If the first two conditions are obvious, then the following two conditions are required in order to have all other values of $|F(w)|$ smaller than WH_{max}. These conditions can be presented in the form of simple tests.

Theorem 1 [27]. The Boolean function $f(x)$ with *WHT* $F(w)$ is given, and sets are defined

$$W^+ = W_1^+ \cup W_2^+$$

and

$$W^- = W_1^- \cup W_2^-.$$

Then for some input x an element from the *Improvement Set* exists and the following two conditions are met: $f(x) = L_w(x)$ for all $w \in W^+$, and $f(x) \neq L_w(x)$ for all $w \in W^-$.

The criterion of gradient search is the maximization of the Hamming distance between the generated sequence and the sequences of linear functions. After updating the algebraic form of the Boolean function, similar operations are performed: the Walsh-Hadamard *WFT* transform is performed and the maximum values of the transformation coefficients are found; A set of *Improvement Set* is formed; there are elements of a sequence of functions that coincide with the elements of the sequence of the nearest linear form; inverting the matched elements and increasing the nonlinearity of the function, by "distance" from the nearest linear function. Next iterations similar to those discussed above are performed.

The conducted researches have shown that the considered method of gradient lifting is computationally expensive and, with a large number of arguments of the Boolean function, requires a significant number of repeated iterations. To reduce computational complexity, a gradient descent method with bent sequences is proposed in [28] as an input data.

3.2 HEURISTIC METHOD OF GRADIENT DESCENT

The proposed method of cryptographic Boolean functions constructing is a further development of the heuristic method of gradient lifting. This method is based on using the properties of nonlinear sequences. It differs from the well-known heuristic methods in the iterative procedure of complementing the positions of bent sequences for the gradient search for balanced Boolean functions according to the criterion of maximizing the Hamming distance between the generated sequences and the sequences of all linear functions, which makes it possible to search the Boolean functions with the required cryptographic properties with less computational efforts.

The main idea of the gradient descent method is the effective lowering of the nonlinearity of the given bent sequences for each of the $2^{n/2-1}$ obligatory complementations. Table 1 presents the calculated data for vector spaces V_4 - V_{12}. Column 2 shows the non-linearity (Walsh transform value) of the bent sequences considered as an input, column 3 shows the maximum achievable non-linearity (the maximum value of the Walsh transform) of the functions taken as an output, and column 4 indicates the number of bits that need to be changed in the bent sequences to obtain the desired result.

Table 1. Calculation Values for Vector Spaces V_4 - V_{12}

	The maximum achievable performance for bent functions		Maximum achievable performance for balanced functions / Best known result		The number of positions in the bent sequence that need to be changed
	N_f	$F(w)$	N_f	$F(w)$	
V_4	6	4	4/4	8/8	2 positions
V_6	28	8	26/26	12/12	4 positions
V_8	120	16	118/116	20/24	8 positions
V_{10}	496	32	494/492	36/40	16 positions
V_{12}	2016	64	2014/2010	68/76	32 positions

Fig. 1 shows the possible loss of nonlinearity in the complementation of the required number of positions of the bent sequence. To achieve the given upper bound of the nonlinearity, it is necessary to determine from the total number of positions x of the truth table to be complemented, the number of positions y the change of which entails a change of WH to +2, and the number of positions z the change of which entails a change of WH by -2, $x = y + z$. Table 2 presents the calculated data showing the necessary number of required complementations of the bent sequence for a given vector space in accordance with Theorem 2.1 of [27].

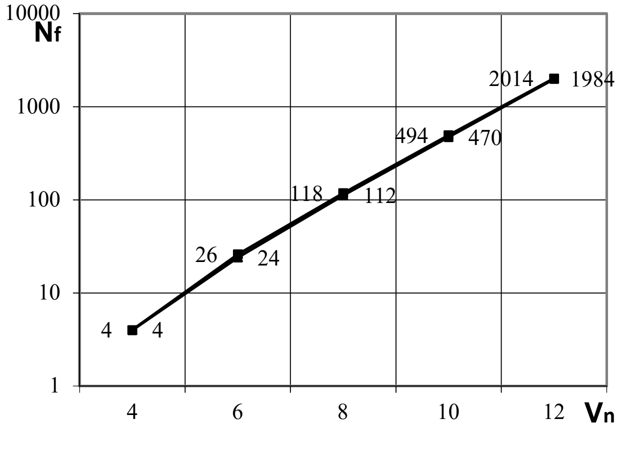

Figure 1 – Possible loss of nonlinearity in the case of complementation

After calculating the necessary number of complementations of the bent sequence, the Walsh-Hadamard transformation WH is performed in the first step of the heuristic search and the maximum Hamming distance to one or more sequences of linear functions $L_i(x)$ is determined. This operation corresponds to the selection of the zero value of Walsh-Hadamard transform coefficients WH, after which a set of linear functions constituting the *Improvement Set* is formed. Further, the elements of the bent function sequence are inverted, which coincide with the elements of sequences of linear functions from the *Improvement Set*. As a result, the imbalance of the function is reduced, but the non-linearity also decreases, i.e. the sequence of the function is not as far from the sequences of the linear functions $L_i(x)$. At the next iteration, all operations are repeated. Thus, as a criterion for gradient search for cryptographic functions, the proposed method is the minimization of the minimal Hamming distance of the generated sequence and sequences of linear functions.

Table 2. Estimates of the Necessary Number of Bent-Sequential Complications

	The number of positions in the bent sequence that need to be changed, *NeedSteps*	The value of nonlinearity must be changed		Required for this change, n^- and n^+
		N_f, from _ to _	$F(w)$, from _ to _	
V_4	2	6→4	4→8	n^- = 2 (changes from $F(w)$ = +2)
V_6	4	28→26	8→12	n^- = 3 (changes from $F(w)$ = +2) n^+ = 1 (changes from $F(w)$ = -2)
V_8	8	120→116	16→24	n^- = 6 (changes from $F(w)$=+2) n^+ = 2 (changes from $F(w)$=-2)
V_{10}	16	496→492	32→40	n^- = 10 (changes from $F(w)$=+2) n^+ = 6 (changes from $F(w)$=-2)
V_{12}	32	2016→2010	64→76	n^- = 19 (changes from $F(w)$=+2) n^+ = 13 (changes from $F(w)$=-2)

In general, the proposed method consists of three main stages.

At the first stage, gradient descent procedures are used, which allow to obtain a highly nonlinear sequence.

At the second stage, the renewal procedures of algebraic normal form of the function on the output sequence are used.

At the third stage, depending on the practical application environment, the modification procedure of the algebraic normal form of the function *f(x)* is used. This allows us to maintain the basic indicators of stability (balance and nonlinearity) by applying affine transformations, to improve either the dynamic properties of the nonlinear transformation or the correlation characteristics.

So, the developed method allows us to form balanced cryptographic functions with high nonlinearity. In this case, as shown in Fig. 1, the values of nonlinearity lie in a narrow range of values that depends on the dimension of the vector space.

It should be noted that for modern in-line ciphers, an important indicator of effectiveness is also the correlation immunity that characterizes the resistance of the encryption scheme to correlation attacks [41-44]. We will make the evaluations of nonlinearity and correlation immunity of Boolean functions that can be synthesized by the developed method.

4 EVALUATIONS OF NONLINEARITY AND CORRELATION IMMUNITY OF THE FORMED FUNCTIONS

For cryptographic Boolean functions, the relationship between the attainable degree of correlation immunity *m* and its nonlinearity N_f [30] is known:

$$N_f = 2^{n-1} - 2^{m+1}, \qquad (1)$$

it is true for

$$m \geq n/2 - 2. \qquad (2)$$

As it can be seen from (1), the degree increase in correlation immunity m leads to the decrease in nonlinearity, and vice versa. Therefore, developers of cryptographic protection facilities, depending on the conditions of practical use, have to find a compromise between the required nonlinearity and the desired degree of correlation immunity. The advantage of the developed method is the ability to build functions with different values of cryptographic indicators.

So, for example, in Table 3, the achievable degree of correlation immunity $CI_{\max}(k)$ with indication of the corresponding non-linearity $N_{f\min}$ is shown according to (1) and (2). In fact, the data in the table correspond to the lower limit of nonlinearity, guarantee obtained using the developed method. Table 4 shows the achievable degree of correlation immunity $CI_{\max}(k)$ with indication of the maximum possible nonlinearity for the balanced functions of $N_{f\max}$. That is, the upper limit of the functions nonlinearity using the developed method is given here. In Fig. 2 for clarity the table data is depicted by means of a graph.

Table 3. The lower limit of nonlinearity at given correlation immunity

	V_4	V_6	V_8	V_{10}	V_{12}
$CI_{\max}(k)$	1	2	3	4	5
$N_{f\min}$	4	24	112	480	1984

Table 4. The upper limit of nonlinearity at given correlation immunity

	V_4	V_6	V_8	V_{10}	V_{12}
$CI_{\max}(k)$	1	1	2	3	4
$N_{f\max}$	4	26	116	492	2010

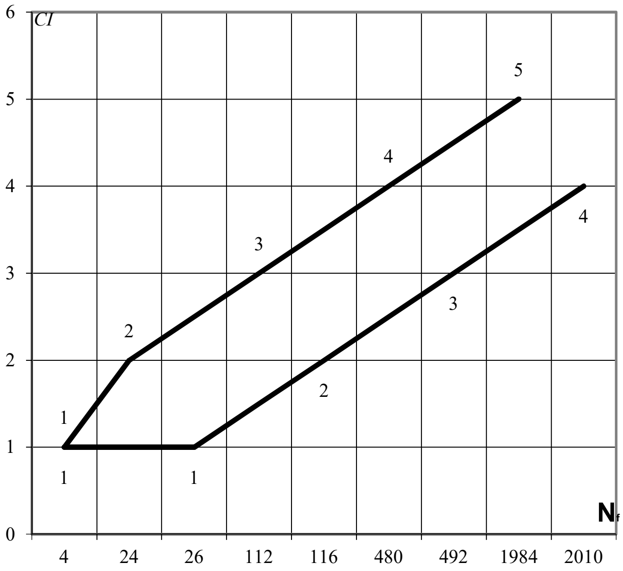

Figure 2 –Boundary indicators of correlation immunity

As the mentioned data analysis show, the application of the developed method allows to form the Boolean functions, which, in addition to high nonlinearity values can be potentially correlation-immune functions. When used in stream ciphers, they will be highly resistant to various cryptographic attacks. Thus, for example, the application of the developed method over the V_8 space allows us to form functions with the nonlinearity index $N_{f\min}$ = 112 and the degree of correlation immunity $CI_{\max}(3)$, which is the best result known up today.

It should be noted that the probabilistic search by heuristic methods is described by some random process, the specific implementation of which is a random variable - the values of the indices of the stability of the found function (see Section II).

The corresponding probabilities of the occurrence of the desired random events indicate the average number of attempts to succeed - the construction of a cryptographic Boolean function with the required properties. Thus, to evaluate the computational effectiveness of heuristic methods, i.e. it is necessary to assess the probability distribution of the formation of Boolean functions with different cryptographic indices.

5 METHODOLOGY OF ESTIMATION OF THE EFFICIENCY AND RESULTS OF THE RESEARCH

The proposed methodology uses the average number of attempts as an index of computational efficiency that will need to be performed using the heuristic method to generate a cryptographic function with the required indicators of stability.

In accordance with the main provisions of the theory of probability and mathematical statistics, the unknown distribution function of the random variable under consideration is determined due to the results of observations from the sample [29]. A sample of volume *L* for a random variable *A* is a sequence $X_1, X_2, ..., X_L$ of *L* independent observations of this quantity, that is, a set of values taken by *L* independent random variables $A_1, A_2, ..., A_L$ with the same distribution law $F_A(x)$ as the considered quantity *A*. In this case, the sample $X_1, X_2, ..., X_L$ is taken from the general aggregate of *A*, and the distribution law of the general population is understood as the distribution law of a random variable *A*. The values $X_1, X_2, ..., X_L$ are called sample values [29].

The following notation: SI_i - a random variable whose values represent the outcomes of a heuristic search is introduced - a numerical expression of the *i*-th indicator of the strength of a cryptographic Boolean function; $X_1, X_2, ..., X_L$ is the sample of the volume *L* of the random variable SI_i; $F_{SI_i}(x)$ is the distribution function of the random variable SI_i.

The values of the theoretical distribution functions $F_{SI_i}(x)$ that are the probabilities of events should be estimated $\{SI_i < x\}$, using the frequencies of these events from the sample of the volume *L*. v_x denotes the number of sample values less than *x*. Then the frequencies $\frac{v_x}{L}$ of sampling to the left of the point *x* in this sample are the frequencies of events $\{SI_i < x\}$. These frequencies are functions of *x* and are, respectively, empirical distribution functions $F^*_{SI_i}(x)$ of random variables SI_i obtained from this sample: $F^*_{SI_i}(x) = \frac{v_x}{L}$. The frequency of the event in L independent experiments is an estimate for the probability of this event, i.e.

$$F_{SI_i}(x) \approx F^*_{SI_i}(x) = \frac{v_x}{L}.$$

Using the distribution function $F_{SI_i}(x)$, the indicator of computational efficiency of heuristic methods as the average number K_{av} of attempts of probabilistic formation of a Boolean function with the required properties can be introduced as:

$$K_{av} = \frac{1}{F_{SI_i}(x)} \approx \frac{1}{F^*_{SI_i}(x)}.$$

If accept the assumption of statistical independence m of random variables SI_i, $i = 1,..,m$, then the probability of the formation of a cryptographic function with exponents $SI_i < x, i = 1,..,m$ will be determined by the probability of a joint event written through the product of the probabilities of independent events:

$$\prod_{i=1}^{m} F_{SI_i}(x).$$

The average number of attempts at probabilistic formation of a cryptographic function $SI_i < x, i = 1,..,m$ is calculated from the expression:

$$K_{av} = \frac{1}{\prod_{i=1}^{m} F_{SI_i}(x)} \approx \frac{1}{\prod_{i=1}^{m} F^*_{SI_i}(x)}.$$

Two main indicators are of greatest interest for cryptography: nonlinearity of N_f and autocorrelation of *AC* [21-28], and it is necessary to maximize nonlinearity and minimize auto-correlation. To estimate the computational efficiency for these two stability indicators, the last expression is rewritten in the form:

$$K_{av} = \frac{1}{\left(1 - F_{N_f}(x)\right) \cdot F_{AC}(x)} \approx \frac{1}{\left(1 - F^*_{N_f}(x)\right) \cdot F^*_{AC}(x)},$$

where: $F_{N_f}(x)$ and $F^*_{N_f}(x)$ - theoretical and empirical probabilities of an event $\{N_f \le x\}$;

$F_{AC}(x)$ и $F^*_{AC}(x)$ - theoretical and empirical probabilities of an event $\{AC \le x\}$;

Using the indicator K_{av}, comparative studies of the computational effectiveness of heuristic methods of probabilistic formation of cryptographic Boolean functions will be performed. As an object of investigation, the method of random generation [21-28], the method of gradient lifting and the heuristic method of gradient descent proposed in [27] will be used [28].

Fig. 2 shows histograms of frequencies of events $\{N_f = x\}$ for balanced Boolean functions constructed above V$_8$, sample size L =10000. As it can be seen from the given data, the heuristic method of gradient descent (IKK) allows for representing Boolean functions with indicators of nonlinearity $N_f \ge 114$ with probability 1, $N_f \ge 116$ with probability 0.5. The next method of gradient lifting (MSD) for computational efficiency allows one to generate cryptographic functions with nonlinearity indicators $N_f \ge 112$ with probability 1, $N_f \ge 114$ with probability 0.5 and $N_f \ge 116$ with probability 0.1. The method of random generation (RG) is generally ineffective, the most probable value of the nonlinearity is in the range 80..104.

Fig. 3 shows the frequencies of events $\{AC = x\}$ for balanced Boolean functions constructed over V_8, the sample size L =10000.

As the analysis shows, the heuristic method of gradient descent is highly competitive with the closest analogue - the method of gradient search. It allows for representing Boolean functions with a low autocorrelation index.

Fig. 4 shows the dependencies K_{av} for:

- the method of random generation with AC = 80 (RG, AC = 80);
- method of random generation with AC = 120 (RG, AC = 120);
- method of gradient lifting with AC = 24 (MCD, AC = 24);
- method of gradient lifting with AC = 32 (MCD, AC = 32);
- gradient descent method with AC = 24 (IKK, AC = 24);
- method of gradient descent with AC = 32 (IKK, AC = 24).

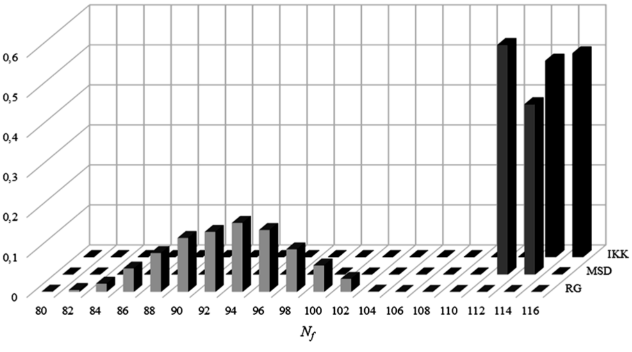

Figure 2 – Histograms of event frequencies $\{N_f = x\}$, sample size L = 10000

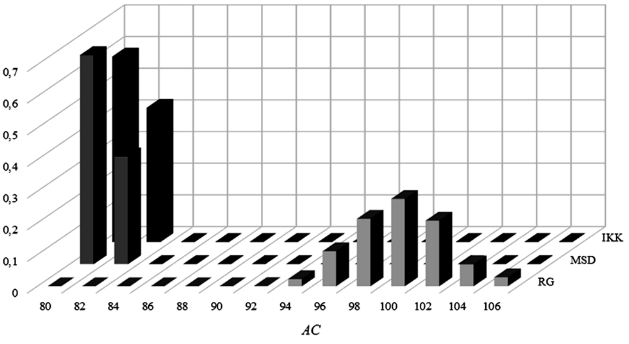

Figure 3 – Histograms of frequencies of events $\{AC = x\}$, sample size L = 10000

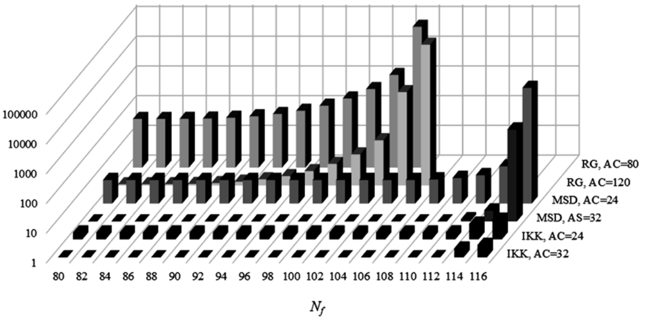

Figure 4 – Dependencies of the average number K_{av}

Analysis of the dependencies provided in Fig. 4 shows that the gradient descent method allows for representing Boolean functions with high cryptographic indices (nonlinearity and autocorrelation) for fewer attempts (on average). For example, the formation of a cryptographic function with AC = 24 and N = 116 for the random generation method is computationally unattainable due to the extremely high average number of attempts. For the same parameters, the gradient lifting method will require an average of about 8000 attempts. The method of gradient descent with the same parameters will require an average of 4 attempts, i.e. the average number of attempts has decreased 2000 times. When requirements to cryptographic properties of AC = 24 and N = 114, the method of gradient lifting will require an average of about 15 attempts, and the method of gradient descent – about 3.

6 CRYPTOGRAPHIC PROPERTIES OF FORMED BOOLEAN FUNCTIONS

We will conduct a comparative study of the properties of cryptographic Boolean functions with the best known analogues: the genetic algorithm [31], the NLT- and ACT-algorithms [32], which belong to the class of heuristic methods.

Table 5 presents the results of a comparative assessment of nonlinearity functions obtained using the developed method of gradient descent, the prototype method (heuristic method of gradient lifting) and the best known heuristic methods (all data except the last line are taken from [31]).

These data indicate that among the heuristic methods, the developed method allows for achieving the highest nonlinearity. High nonlinearity indicates a high degree of data mixing, which determines the resistance of crypto-transformations. For the first time, we managed to construct functions with the highest known nonlinearity among the heuristic methods: $N_f = 488$ for V_{10} and $N_f = 2002$ for V_{12}.

Table 5. Comparative assessment of nonlinearity functions

	V_6	V_8	V_{10}	V_{12}
Theoretical nonlinearity	26	118	494	2014
Method of random generation (RG) [31]	-	112	472	1954
Hill Climbing Method [27]	-	114	476	1960
Genetic Algorithm [31]	26	116	484	1976
NLT [32]	26	116	486	1992
ACT [32]	26	116	484	1986
Developed method [28]	26	116	488	2002

Table 6 shows the comparative characteristics of the best known methods that allow for representing functions with low autocorrelation values [31]. As it can be seen in this table, the developed method allows formation of functions with low autocorrelation values. Over V_8, the *NLT* and *ACT* methods allow for representing functions with AC = 16, but the nonlinearity is equal to 112. The developed method allows formation of functions with nonlinearity 116. Over all other vector spaces, the obtained values are comparable to the results for other methods.

Table 6. Comparative assessment of functions autocorrelation

	V_6	V_8	V_{10}	V_{12}
Zhang Zheng [33, 34]	16	24	48	96
Maitra [35, 36]	16	24	40	80
NLT [32]	16	16	64	144
ACT [32]	16	16	56	128
Developed method [28]	16	24	40	72

Figs. 5-9 show the spectral properties of Boolean functions formed in various ways. In parentheses are the indicators: (n, $deg(f)$, N_f, AC). This data shows that cryptographic Boolean functions constructed in accordance with the developed method [28] have the maximum attainable algebraic degree, high nonlinearity, and low autocorrelation. By the majority of resistance indicators, the formed functions are equal to known methods.

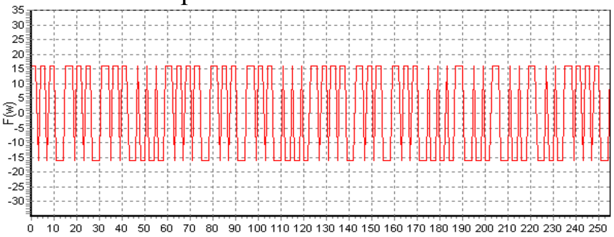

Figure 5 – Bent function [31-40]: (8, 4, 120, 0)

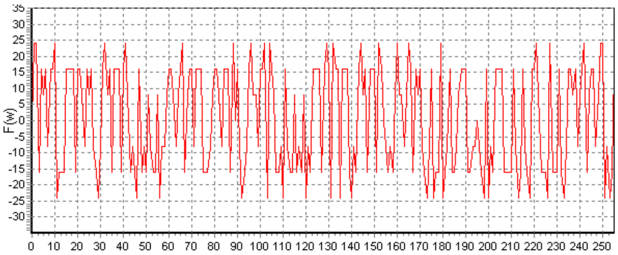

Figure 6 – Developed method [28]: (8, 7, 116, 24)

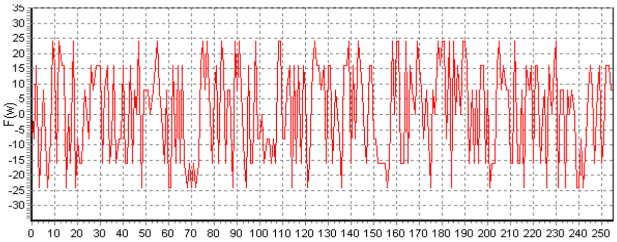

Figure 7 – Hill Climbing Method [28]: (8, 6, 116, 24)

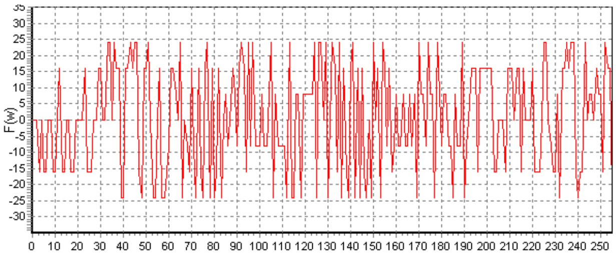

Figure 8 –Maitra-Pasalic Method [37]: (8, 6, 116, 80)

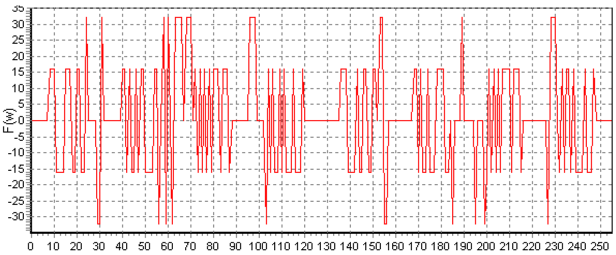

Figure 9 –Seberry-Zhang Method [38-40]: (8, 4, 112, 128)

7. CONCLUSIONS

Studies of the computational efficiency of heuristic methods that were conducted have shown that the methods of gradient search for an acceptable number of iterations allow for representing cryptographic Boolean functions with high nonlinearity and low autocorrelation. Formed functions are not inferior to the best known results for the rest of the cryptographic indicators.

The gradient descent method, first proposed by us in [28], is developed in this paper. In particular, we obtained estimates of the computational complexity of this method, and also carried out a comparison with the closest prototype, Hill Climbing Method. The gradient descent method proved to be more effective than the Hill Climbing Method in [27]. In particular, the results of experimental studies show that the method of gradient descent requires ten times smaller number of iterations, i.e. it is more effective in the computational aspect.

We have compared the cryptographic properties of Boolean functions formed by various methods. Comparisons were made with the following evolutionary computational approaches: the Hill Climbing method, the Simulated Annealing method, the Genetic Algorithm. Comparative studies of the cryptographic properties of Boolean functions have shown that the functions formed by the proposed computational method have high indicators: the nonlinearity index approaches the upper theoretical limit; the autocorrelation index is one of the lowest in comparison with other methods of synthesis; with equal indices of nonlinearity, the formed functions have the maximum attainable algebraic degree; all known methods of synthesis are inferior in spectral characteristics of functions. Thus, on the basis of the conducted studies, it can be concluded that the functions constructed in accordance with the developed method have high persistence indexes and exceed the known functions by these indicators.

8 PROSPECTS FOR FURTHER RESEARCH

A promising research direction is the development of a probabilistic model for the synthesis of non-linear replacement nodes with high cryptographic properties, experimental studies and substantiation of practical recommendations in order to implement the obtained results.

This research might be useful for the improvement of various methods of information security, as well as other practical use [45-52]. In particular, the obtained results can be used to build non-linear replacement nodes for modern block symmetric ciphers, including the formation of s-blocks of the Ukrainian national block encryption standard Kalyna (DSTU 7624: 2014) [3, 53], the cryptographic hashing algorithm Kupyna [54-56], as well as the recently approved stream encryption standard Strumok [16].

The estimates and calculated values given in this paper (see Tables 5 and 6) clearly confirm the conclusion that the developed gradient descent method is not inferior in basic cryptographic indicators (nonlinearity and autocorrelation) to the best known results. In addition, as it is seen in the diagrams (see Figs. 2, 3, 4) the developed method is significantly (several times) more efficient computationally. Thus, the obtained results have the great practical importance for the development of methods and computational algorithms for the formation of nonlinear nodes of modern symmetric cryptoalgorithms.

The proposed method for estimating the computational effectiveness of heuristic methods can be used for other methods, including using an extended set of indices of stability. This direction is an area of our further research.

9 REFERENCES

[1] *Information Technology. Security Techniques. Encryption Algorithms.* Part 3: Block ciphers. ISO/IEC 18033-3: 2010, 2010.

[2] *Advanced Encryption Standard,* Federal Information Processing Standards Publications FIPS-197, 2001.

[3] *A New Encryption Standard of Ukraine: The Kalyna Block Cipher.* Cryptology ePrint Archive: Report 2015/650. https://eprint.iacr.org/2015/650.

[4] *Information Technology. Cryptography Protection of Information. Block Ciphers.* National Standard of Russian Federation, GOST R 34.12-2015, 2015 (in Russian).

[5] O. O. Kuznetsov, Yu. I. Gorbenko, I. M. Bilozertsev, A. V. Andrushkevych, O. P. Narizhnyi, "Algebraic immunity of non-linear blocks of symmetric ciphers," *Telecommunications and Radio Engineering*, vol. 77, issue 4, pp. 309-325, 2018. DOI: 10.1615/TelecomRadEng.v77.i4.30

[6] B. N. Tran, T. D. Nguyen and T. D. Tran, "A new S-box structure to increase complexity of algebraic expression for block cipher cryptosystems," *Proceedings of the 2009 International Conference on Computer Technology and Development*, Kota Kinabalu, 2009, pp. 212-216.

[7] A. Kuznetsov, R. Serhiienko, D. Prokopovych-Tkachenko and Y. Tarasenko, "Evaluation of algebraic immunity of modern block ciphers," *Proceedings of the 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Kyiv, Ukraine, 2018, pp. 288-293. DOI: 10.1109/DESSERT.2018.8409146

[8] M. McLoone and J. V. McCanny, "High-performance FPGA implementation of DES using a novel method for implementing the key schedule," *IEE Proceedings-Circuits, Devices and Systems*, vol. 150, no. 5, pp. 373, Oct. 2003.

[9] A. Kuznetsov, I. Kolovanova and T. Kuznetsova, "Periodic characteristics of output feedback encryption mode," *Proceedings of the 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkov, 2017, pp. 193-198. DOI: 10.1109/ INFOCOMMST.2017.8246378

[10] S. Sulaiman, Z. Muda and J. Juremi, "The new approach of Rijndael key schedule," *Proceedings of the 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)*, Kuala Lumpur, 2012, pp. 23-27.

[11] L. May, M. Henricksen, W. Millan, G. Carter, and E. Dawson, "Strengthening the key schedule of the AES," *in Information Security and Privacy, Lecture Notes in Computer Science*, vol. 2384, Springer Berlin / Heidelberg, pp. 226-240, 2002.

[12] F. H. Nejad, S. Sabah and A. J. Jam, "Analysis of avalanche effect on advance encryption standard by using dynamic S-Box depends on rounds keys," *Proceedings of the 2014 International Conference on Computational Science and Technology (ICCST)*, Kota Kinabalu, 2014, pp. 1-5.

[13] H. Liu and C. Jin, "Lower bounds of differential and linear active S-boxes for 3D-like structure," *The Computer Journal*, vol. 58, no. 4, pp. 904-921, April 2015.

[14] A. Kuznetsov, Y. Gorbenko, A. Andrushkevych and I. Belozersev, "Analysis of block symmetric algorithms from international standard of lightweight cryptography ISO/IEC 29192-2," *Proceedings of the 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkov, 2017, pp. 203-206. DOI: 10.1109/INFOCOMMST.2017.8246380.

[15] I. Gorbenko, A. Kuznetsov, M. Lutsenko and D. Ivanenko, "The research of modern stream ciphers," *Proceedings of the 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkov, 2017, pp. 207-210. DOI: 10.1109/INFOCOMMST.2017. 8246381

[16] *Information Technologies. Cryptographic Data Security. Symmetric Stream Transformation Algorithm.* National Standard of Ukraine DSTU 8845:2019, 2019 (in Ukrainian).

[17] C. A. Wood, S. P. Radziszowski and M. Lukowiak, "Constructing large S-boxes with area minimized implementations," *Proceedings of the 2015 IEEE Military Communications Conference MILCOM'2015*, Tampa, FL, 2015, pp. 49-54.

[18] V. Gopi and E. Logashanmugam, "Design and analysis of nonlinear AES S-box and mix-column transformation with the pipelined architecture," *Proceedings of the 2013 International Conference on Current Trends in Engineering and Technology (ICCTET)*, Coimbatore, 2013, pp. 235-238.

[19] H. Wang, H. Zheng, B. Hu and H. Tang, "Improved lightweight encryption algorithm based on optimized S-box," *Proceedings of the 2013 International Conference on Computational and Information Sciences*, Shiyang, 2013, pp. 734-737.

[20] I. Das, S. Nath, S. Roy and S. Mondal, "Random S-box generation in AES by changing irreducible polynomial," *Proceedings of the 2012 International Conference on Communications, Devices and Intelligent Systems (CODIS)*, Kolkata, 2012, pp. 556-559.

[21] Y. Chen, W. Tian and Y. Zhang, "Construction for balanced boolean function with maximum algebraic immunity," *Proceedings of the 2014 7th International Conference on Advanced Software Engineering and its Applications*, Haikou, 2014, pp. 32-34.

[22] C. E, S. Liang and T. Zhang, "Construction method of boolean functions based on genetic algorithm," *Proceedings of the 2011 7th International Conference on Wireless Communications, Networking and Mobile Computing*, Wuhan, 2011, pp. 1-4.

[23] R. Asthana, N. Verma and R. Ratan, "Generation of Boolean functions using Genetic Algorithm for cryptographic applications," *Proceedings of the 2014 IEEE International Advance Computing Conference (IACC)*, Gurgaon, 2014, pp. 1361-1366.

[24] Bharti and D. K. Sharma, "Searching Boolean function using simulated annealing and hill climbing optimization techniques," *Proceedings of the 2016 International Conference on Advanced Communication Control and Computing Technologies (ICACCCT)*, Ramanathapuram, 2016, pp. 62-64.

[25] W. Millan, J. Fuller and E. Dawson, "New concepts in evolutionary search for Boolean functions in cryptology," *Proceedings of the* 2003 Congress on *Evolutionary Computation CEC'03*, 2003, vol. 3, pp. 2157-2164.

[26] S. Picek, C. Carlet, S. Guilley, J. F. Miller and D. Jakobovic, "Evolutionary algorithms for Boolean functions in diverse domains of cryptography," *Proceedings of the Evolutionary Computation*, vol. 24, no. 4, pp. 667-694, Dec. 2016.

[27] W. Millan, A. Clark, E. Dawson, "Smart hill climbing finds better Boolean functions,"

Proceedings of the Workshop on Selected Areas on Cryptography SAC'97, Springer-Verlag, 1997, pp. 50-63.

[28] Y. Izbenko, V. Kovtun and A. Kuznetsov, "The design of Boolean functions by modified hill climbing method," *Proceedings of the 2009 Sixth International Conference on Information Technology: New Generations*, Las Vegas, NV, 2009, pp. 356-361. DOI: 10.1109/ITNG.2009. 102

[29] *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*. NIST Special Publication 800-22, 2001.

[30] E. Pasalic and T. Johansson, "Further results on the relation between nonlinearity and resiliency of Boolean functions," *Proceedings of the IMA Conference on Cryptography and Coding (Lecture Notes in Computer Science)*. New York: Springer-Verlag, 1999, vol. 1746, pp. 35–45.

[31] J. A. Clark, J. L. Jacob, S. Stepney, S. Maitra, W. Millan, "Evolving Boolean functions satisfying multiple criteria," *Proceedings of the INDOCRYPT'02. Lecture Notes in Computer Science*, vol. 2551, Springer, 2002, pp. 246-259.

[32] W. Millan, A. Clark, E. Dawson, "An effective genetic algorithm for finding highly non-linear Boolean functions," *Proceedings of the First International Conference on Information and Communications Security, Lecture Notes in Computer Science*, vol. 1334. Springer-Verlag, Berlin Heidelberg New York, 1997, pp. 149-158.

[33] Y. Zheng and X. M. Zhang, "Improved upper bound on the nonlinearity of high order correlation immune functions," *Selected Areas in Cryptography-SAC'2000, Lecture Notes in Computer Science*, vol. 2012, pp. 264–274. Springer Verlag, 2000.

[34] X-M. Zhang and Y. Zheng, "GAC-the criterion for global avalanche characteristics of cryptographic functions," *Journal of Universal Computer Science*, vol. 1, issue 5, pp. 316–333, 1995.

[35] S. Maitra, "Highly nonlinear balanced Boolean functions with very good autocorrelation property," *Proceedings of the Workshop on Coding and Cryptography-WCC'2001*, Paris, January 8–12, 2001, *Electronic Notes in Discrete Mathematics*, vol. 6, Elsevier Science, 2001.

[36] S. Maitra, "Autocorrelation properties of correlation immune Boolean functions," *Proceedings of the INDOCRYPT 2001, Lecture Notes in Computer Science*, vol. 2247, pp. 242–253, Springer Verlag, December 2001.

[37] S. Maitra and E. Pasalic, "Further constructions of resilient Boolean functions with very high nonlinearity," *IEEE Transactions on Information Theory*, vol. 48, issue 7, pp. 1825–1834, July 2002.

[38] J. Seberry, X.-M. Zhang and Y. Zheng. "Nonlinearity and propagation characteristics of balanced Boolean functions," *Information and Computation*, vol. 119, no. 1, pp. 1-13, 1995.

[39] J. Seberry, X.M. Zhang, Y. Zheng, "On constractions and nonlinearity of correlation immune functions," *Proceedings of the Advances in Cryptology – EUROCRYPT'93, Lecture Notes in Computer Science*, vol. 765, Springer-Verlag, 1994, pp. 181-199.

[40] J. Seberry and X. Zhang. "Hadamar matrices, Bent functions and cryptography," *in J.H. Dinitz and D.R. Stinson, editors, Contemporary Design Theory: A Collection of Surveys, chapter 11*, pp. 431-559, John Wiley and Sons, Inc, 1995.

[41] A. S. Omar and O. Basir, "SIMON 32/64 and 64/128 block cipher: Study of cross correlation and linear span attack immunity," *Proceedings of the 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, Montreal, QC, 2017, pp. 1-6.

[42] C. Carlet and X. Chen, "Constructing low-weight d th-order correlation-immune Boolean functions through the Fourier-Hadamard transform," *IEEE Transactions on Information Theory*, vol. 64, no. 4, pp. 2969-2978, April 2018.

[43] Z. Wang and G. Gong, "Discrete Fourier transform of Boolean functions over the complex field and its applications," *IEEE Transactions on Information Theory*, vol. 64, no. 4, pp. 3000-3009, April 2018.

[44] A. Belazi, R. Rhouma and S. Belghith, "A novel approach to construct S-box based on Rossler system," *Proceedings of the 2015 International Wireless Communications and Mobile Computing Conference (IWCMC)*, Dubrovnik, 2015, pp. 611-615.

[45] N. Ferguson, et al., "Improved cryptanalysis of Rijndael," in *Fast Software Encryption, Lecture Notes in Computer Science*, vol. 1978, Springer Berlin / Heidelberg, 2001, pp. 213-230.

[46] K. Runovski, & H. Schmeisser, "On the convergence of Fourier means and interpolation means," *Journal of Computational Analysis and Applications*, vol. 6, issue 3, pp. 211-227, 2004.

[47] K. Verma and D. K. Sharma, "Calculation of non-linearity and algebraic degree of constructed Boolean function," *Proceedings of the 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, Bangalore, 2017, pp. 501-505.

[48] B. P. Tkach, & L. B. Urmancheva, "Numerical-analytic method for finding solutions of systems with distributed parameters and integral condition," *Nonlinear Oscillations*, vol. 12, issue

1, pp. 113-122, 2009. doi:10.1007/s11072-009-0064-6

[49] R. Chornei, V. M. Hans Daduna, & P. Knopov, "Controlled Markov fields with finite state space on graphs," *Stochastic Models*, vol. 21, issue 4, pp. 847-874, 2005. doi: 10.1080/15326340500294520

[50] G. Manjula and H.S. Mohan, "Constructing key dependent dynamic S-Box for AES block cipher system," *Proceedings of the 2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT)*, Bangalore, 2016, pp. 613-617.

[51] O. Oksiiuk and V. Chaikovska, "Authentication process threats in the cloud technologies," *Proceedings of the 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkiv, Ukraine, 2018, pp. 113-118. doi:10.1109/INFOCOMMST.2018.8632126

[52] R. Goyal, "Annihilator immunity of a bent function," *Proceedings of the 2017 International Conference on Intelligent Communication and Computational Techniques (ICCT)*, Jaipur, 2017, pp. 23-25.

[53] C. D. Akshima, M. Ghosh, A. Goel, S.K. Sanadhya, "Single key recovery attacks on 9-round Kalyna-128/256 and Kalyna-256/512," *in Kwon S., Yun A. (eds) Information Security and Cryptology – ICISC'2015, Lecture Notes in Computer Science*, Springer, Cham, vol. 9558, 2016.

[54] *A New Standard of Ukraine: The Kupyna Hash Function*. Cryptology ePrint Archive Report 2015/885. https://eprint.iacr.org/2015/885.

[55] J. Zou, L. Dong, "Cryptanalysis of the round-reduced Kupyna hash function," *Cryptology ePrint Archive Report 2015/959*, https://eprint.iacr.org/2015/959.pdf.

[56] O. Duman, *Application of Fault Analysis to Some Cryptographic Standards*, Master Thesis in the Concordia Institute for Information Systems Engineering, https://spectrum.library.concordia.ca/981334/1/Duman_MASc_f2016.pdf

***Illarion V. Moskovchenko**, Ph.D. in Mathematical Modeling and Computational Methods. Head of the Information and Computing Center of the Ivan Kozhedub Kharkiv National Air Force University. Areas of scientific interests: cryptology, methods of information security in computer systems.*

***Alexandr A. Kuznetsov,** Doctor of Sciences (Engineering), Full Professor, Academician of the Academy of Applied Radio-electronics Sciences, Professor of the Department security information systems and technologies of the V. N. Karazin Kharkiv National University.*

Areas of scientific interests: cryptography and authentication, steganography, cybersecurity.

***Sergii V. Kavun,** Doctor of Sciences (Economics), Full Professor, Rector of Kharkiv University of Technology "STEP". Areas of scientific interests: internet business applications, computing, online social networking, computer networks & systems, information management systems, computer security & protection.*

***Berik B. Akhmetov**, Ph.D. of Technical Sciences (Engineering), Rector of Yessenov University, The Republic of Kazakhstan. Areas of scientific interests: cryptography and coding, security information systems and technologies.*

***Ivan M. Bilozertsev,** Master of Technology degrees in Cyber-security with Honours from V. N. Karazin Kharkiv National University in 2018. Researcher of the Department security information systems and technologies of the V. N. Karazin Kharkiv National University. Areas of interests: security information systems.*

***Serhii A. Smirnov**, Candidate of Sciences (Engineering), Associate professor of Cybersecurity & Software Academic Department Central Ukrainian National Technical University, Ukraine, Kropyvnytskyi. Areas of scientific interests: applied cryptology.*