e-ISSN 1607-3274 Радіоелектроніка, інформатика, управління. 2020. № 1
p-ISSN 2313-688X Radio Electronics, Computer Science, Control. 2020. № 1

UDC 004.622.612

SYNTHESIS METHOD OF TERNARY BENT-FUNCTIONS OF THREE VARIABLES

Sokolov A. V. – PhD, Senior Lecturer of the Department of Informatics and Control of Information Systems Protection, Odessa National Polytechnic University, Odessa, Ukraine.

ABSTRACT

Context. Such perfect algebraic constructions of many-valued logic as ternary bent-functions and their truth tables which are called as 3-bent-sequences, are used very often in modern cryptographic algorithms, in particular, in pseudorandom sequence generators. However, today there are no methods for synthesizing the ternary bent-functions class for a number of variables greater than two, which significantly limits the ability to scale the number of protection levels of the of pseudorandom sequence generators based on the ternary bent-functions. This circumstance generates the task of developing methods for the synthesis of ternary bent-functions, which is solved in this paper for the case of ternary bent-functions of three variables. The object of this research is the process of efficiency increasing of the cryptographic algorithms based on the functions of many-valued logic.

Objective. The purpose of the paper is to construct a method for the synthesis of the set of ternary bent-functions of three variables.

Method. The mathematical apparatus of the Reed-Muller transform (algebraic normal form) was used as the basis of the proposed constructive method for the synthesis of ternary bent-functions of three variables. So, on the basis of the established properties of the algebraic normal form of ternary bent-functions and limited enumeration, the search for ternary bent-functions up to affine terms is performed, after which we apply the procedure of reproduction.

Results. As a result of using of the proposed method for the synthesis of ternary bent-functions of three variables, 155844 3-bent-sequences were found up to an affine term, while the cardinality of the full set of found 3-bent-sequences is 12623364. The research performed made it possible to determine that in this set there are 3-bent-sequences of six different weight structures, on the basis of which 12 different triple sets can be compiled for use in pseudorandom sequence generators. A scheme for a cryptographically stable pseudorandom sequence generator based on the found set of 3-bent-sequences of length $N = 27$ is proposed. It is shown that the protection levels number of such a generator of pseudorandom sequences is $\Psi = 7.041 \cdot 10^{41}$ which is comparable with the protection levels number of modern block symmetric cryptographic algorithms, for example, AES-128.

Conclusions. The further development of modern cryptographic algorithms, in particular, cryptographically stable pseudorandom sequence generators, is largely based on the use of perfect algebraic constructions of many-valued logic. For the first time, a constructive method for the synthesis of ternary bent-functions of three variables is proposed. For the found set of ternary bent-functions, the distribution of weight structures is found, and the possible triple sets are established. Based on the constructed set of ternary bent-functions, a pseudorandom sequence generator scheme is proposed that has a protection levels number that is comparable with modern block symmetric cryptographic algorithms. We note that the constructed class of ternary bent-functions can also be used for the synthesis of cryptographically strong S-boxes, codes of constant amplitude, as well as error correction codes. As an actual area of further research, we can note the development of methods for the synthesis of ternary bent-functions of a larger number of variables.

KEYWORDS: cryptography, pseudorandom sequence generator, ternary logic, bent-function.

ABBREVIATIONS

PRSG is a pseudorandom sequence generator;
LFSR is a linear feedback shift register;
FCSR is a feedback with carry shift register;
BF is a ternary bent-function;
ANF is an algebraic normal form.

NOMENCLATURE

N is a length of 3-bent-sequence;

J_{full} is a cardinality of the full set of ternary sequences;

V_{3^L} is a Vilenkin-Chrestenson matrix of order 3^L, where $L \in \mathbb{N}$;

$\Omega_B(\omega)$ is a Vilenkin-Chrestenson transformants of the sequence B;

K^0, K^1, K^2 is a amounts of symbols “0”, “1” and “2” correspondingly;

Φ is a polynomial of ANF;

$F = \{f_i\}$ is an arbitrary ternary sequence in the time domain, where $i = 0,1,...,N-1$;

$A = \{a_i\}$ is an arbitrary ternary sequence in the Reed-Muller transformants domain, where $i = 0,1,...,N-1$;

L_N and L_N^{-1} are direct and inverse Reed-Muller transform matrices correspondingly;

$wt(T_i)$ is an algebraic degree of the corresponding ANF term T_i;

$\deg(\Phi)$ is an algebraic degree of nonlinearity;

$|V_k|$ is a number of primitive irreducible polynomials of degree k;

Ψ is a number of protection levels.

INTRODUCTION

The current stage of development of cryptographic methods of information protection is characterized by the introduction of cryptographically high-quality functions of many-valued logic [1]. At the same time, one of the most actual tasks is the development of ternary pseudorandom sequence generators (PRSG). Such generators are used in the tasks of quantum cryptography, and can also be used in implementations of cryptographic algorithms

DOI 10.15588/1607-3274-2020-1-9

based on many-valued logic functions on binary computers.

At present, the dynamically developing and applicable in practice is the construction of ternary PRSG [2], which is based on the use of LFSR or FCSR [3] and a special nonlinear element, which is most often used with perfect algebraic constructions such as 3-bent-functions. At the same time, the number of protection levels for the PRSG depends on the length of the 3-bent-function and on the cardinality of the set of available 3-bent-functions, which makes it necessary to develop methods for synthesizing large sets of ternary bent-functions.

At present, regular methods have been created for the synthesis of 3-bent-functions of two variables, nevertheless, there are no such methods for a larger number of variables, which significantly reduces the possibility of increasing the number of protection levels of PRSG based on ternary bent-functions.

The object of research is the process of improving the efficiency of cryptographic algorithms based on many-valued logic functions.

The subject of research is the methods for the synthesis of 3-bent-functions.

The purpose of the work is to construct a method for the synthesis of the set of ternary bent-functions of three variables.

1 PROBLEM STATEMENT

Let us consider the complete set of sequences of length $N = 27$ over the alphabet $\{0,1,2\} \leftrightarrow \left\{1, e^{j\frac{2\pi}{3}}, e^{j\frac{4\pi}{3}}\right\}$, which are the truth tables of all possible 3-functions of $k = 3$ variables. The cardinality of this set is equal to $J_{full} = 3^{27} = 7\,625\,597\,484\,987$.

The problem is to find in this set of sequences of length $N = 27$ such a sequences that are truth tables of ternary bent-functions of three variables, i.e. possess a uniform absolute values of Vilenkin-Chrestenson transformants.

2 REVIEW OF THE LITERATURE

The current stage in the development of information technology is characterized by the widespread introduction of the mathematical apparatus of many-valued logic functions into correcting coding [4] and information compression algorithms [5], as well as in the signal processing [6].

The current stage is also characterized by a rapid development of methods of many-valued logic functions and their implementation in cryptography. In particular, the use of cryptographically strong ternary PRSG, which are proposed to be used to increase the cryptographic strength of quantum information protection protocols, is proposed in [7, 8]. The authors of [9] proposed a scheme of effective PRSG based on ternary bent-functions presented in Fig. 1.

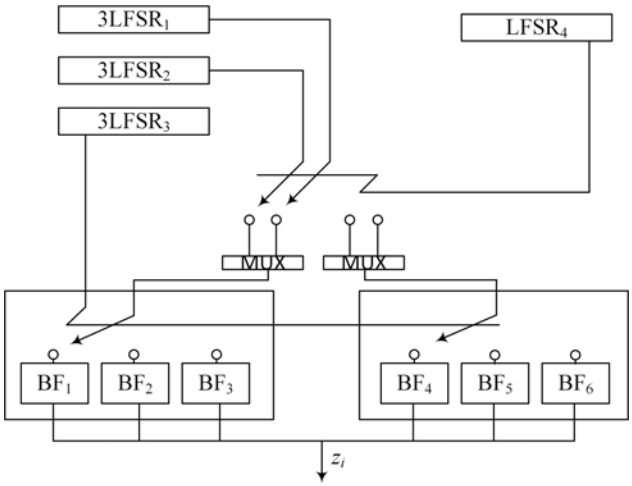

Figure 1 – Scheme of PRSG based on ternary bent-functions

The raw material for the operation of the scheme (Fig. 1) are such perfect algebraic constructions as ternary bent-functions that have a uniform absolute value of Vilenkin-Chrestenson transformants and, accordingly, the maximum possible value of nonlinearity.

The Vilenkin-Chrestenson spectrum of the discrete sequence above the alphabet $0 \to e^{j0^{\circ}}, 1 \to e^{j\frac{2\pi}{3}}, 2 \to e^{j\frac{4\pi}{3}}$ is found by multiplying the column vector containing the samples of the signal by the complex conjugate transformation matrix $\overline{V}$ [10].

In this case, the matrix of the Vilenkin-Chrestenson transform of order 3^L, $L \in \mathbb{N}$ is constructed over the alphabet $\{0,1,2\}$ using the recurrence formula [11], and then in order to perform the Vilenkin-Chrestenson transform it is translated into the exponential form, i.e. to the alphabet $\{e^{j0}, e^{j\frac{2\pi}{3}}, e^{j\frac{4\pi}{3}}\}$:

$$V_{3^L} = \begin{bmatrix} V_{3^{L-1}} & V_{3^{L-1}} & V_{3^{L-1}} \\ V_{3^{L-1}} & \left(V_{3^{L-1}}+1\right) \bmod 3 & \left(V_{3^{L-1}}+2\right) \bmod 3 \\ V_{3^{L-1}} & \left(V_{3^{L-1}}+2\right) \bmod 3 & \left(V_{3^{L-1}}+1\right) \bmod 3 \end{bmatrix}, \quad (1)$$

where

$$V_3 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 2 & 1 \end{bmatrix} \to \begin{bmatrix} e^{j0} & e^{j0} & e^{j0} \\ e^{j0} & e^{j\frac{2\pi}{3}} & e^{j\frac{4\pi}{3}} \\ e^{j0} & e^{j\frac{4\pi}{3}} & e^{j\frac{2\pi}{3}} \end{bmatrix}. \quad (2)$$

A generalized definition of a ternary bent-function was given in [11], according to which the existence of bent-functions of the many-valued logic of an odd number of variables was confirmed.

DOI 10.15588/1607-3274-2020-1-9

Definition 1. For a Vilenkin-Chrestenson matrix of order $N = q^k$, where q is a prime, a bent-sequence $B = [h_0, h_1, \cdots, h_i, \cdots, h_{N-1}]$ is a sequence over an alphabet $h_i \in \left\{ e^{j\frac{2\pi}{q}\nu} \right\}$, $\nu = 0,1,...,q-1$ if it has a uniform absolute values of Vilenkin-Chrestenson spectrum that can be represented in matrix form

$$\left|\Omega_B(\omega)\right| = \left|H \cdot \overline{V}_N\right| = const, \ \omega = \overline{0, N-1}, \qquad (3)$$

where V_N is the Vilenkin-Chrestenson matrix of order N over the alphabet $h_i \in \left\{ e^{j\frac{2\pi}{q}\nu} \right\}$, $\nu = 0,1,...,q-1$.

Currently, methods for the synthesis of 3-bent-sequences of two variables are known [12]. The research of the structure of this class of bent-sequences of cardinality $J = 486$ allowed to establish their possible weight structures, depending on which they are classified into 6 classes:

$$\begin{bmatrix} \{1,4,4\}(54); \\ \{4,1,4\}(54); \\ \{4,4,1\}(54); \end{bmatrix} \begin{bmatrix} \{5,2,2\}(108); \\ \{2,5,2\}(108); \\ \{2,2,5\}(108), \end{bmatrix} \qquad (4)$$

where the numbers in curly brackets show, respectively, the number of characters “0”, “1” and “2” in the 3-bent-sequence, and the numbers in parentheses indicate the number of 3-bent-sequences with the indicated structure.

In [9], it was established that, from the point of view of constructing an PRSG, the triple sets of 3-bent-sequences possess the best properties.

Definition 2. A set of three bent-sequences B_1, B_2, B_3 in the Vilenkin-Chrestenson basis is called a triple set if the concatenation of their truth tables in symbolic form is balanced, i.e. the number of characters “0” is equal to the number of characters “1” and is equal to the number of characters “2”, i.e. $K^0 = K^1 = K^2$.

Thus, the 3-bent-sequences from (4) determine two triple sets

$$\begin{bmatrix} \{\{1,4,4\},\{4,1,4\},\{4,4,1\}\}, \\ \{\{5,2,2\},\{2,5,2\},\{2,2,5\}\}. \end{bmatrix} \qquad (5)$$

Currently, in the literature there are no methods for the synthesis of 3-bent-sequences of three variables, and accordingly, their weight structures remain unknown, which makes it impossible to construct specific PRSG schemes based on 3-bent-sequences of length $N = 27$.

3 MATERIALS AND METHODS

The use of the exhaustive method for the synthesis of 3-bent-sequences, as it was done in [9], is ineffective for 3-bent-sequences of length $N = 27$, since the solution of this problem will be coupled with enumeration of the set of all ternary sequences of length $N = 27$, which consists of $J_{full} = 3^{27} = 7625597484987$ elements. At the same time, practice shows that the construction of purely regular methods for the synthesis of 3-bent-sequences is also difficult due to the complexity and unpredictability of this class of perfect algebraic constructions.

Nevertheless, the performed researches show that the synthesis of 3-bent-sequences of length $N = 27$ can be performed in the Reed-Muller transformants domain, i.e. in algebraic normal form (ANF) [13].

Definition 3. An algebraic normal form of a q-function is a polynomial Φ over Z_q of a degree $\deg(\Phi) < q$ with coefficients $a_i \in \{0,1,...,q-1\}$, containing the operations “Sum modulo q” and “Multiplication modulo q”.

On the basis of Definition 3 the definition of affine functions, which play a key role in cryptography is introduced.

Definition 4. Ternary functions whose ANF polynomial has degree $\deg(\Phi) \le 1$ are called as affine.

Thus, each ternary sequence $F = \{f_i\}$ is uniquely associated with the corresponding sequence of ANF coefficients $A = \{a_i\}$. Moreover, it was established in [3] that the transition to the Reed–Muller transformants domain and vice versa can be performed in matrix form:

$$A = F \cdot L_N, \quad F = A \cdot L_N^{-1}, \qquad (6)$$

where L_k^{-1} is the matrix of the inverse Reed-Muller transform, which is constructed in accordance with [13]; L_k is the Reed-Muller transform matrix.

For the length of the original sequence $N = 27$ the inverse Reed-Muller transform matrix has the form:

$$L_{27}^{-1} = \begin{bmatrix} 100000000000000000000000000 \\ 111000000000000000000000000 \\ 121000000000000000000000000 \\ 100100100000000000000000000 \\ 111111111000000000000000000 \\ 121121121000000000000000000 \\ 100200100000000000000000000 \\ 111222111000000000000000000 \\ 121212121000000000000000000 \\ 100000000100000000100000000 \\ 111000000111000000111000000 \\ 121000000121000000121000000 \\ 100100100100100100100100100 \\ 111111111111111111111111111 \\ 121121121121121121121121121 \\ 100200100100200100100200100 \\ 111222111111222111111222111 \\ 121212121121212121121212121 \\ 100000000200000000100000000 \\ 111000000222000000111000000 \\ 121000000212000000121000000 \\ 100100100200200200100100100 \\ 111111111222222222111111111 \\ 121121121212212212121121121 \\ 100200100200100200100200100 \\ 111222111222111222111222111 \\ 121212121212121212121212121 \end{bmatrix}, \qquad (7)$$

DOI 10.15588/1607-3274-2020-1-9

while the direct Reed-Muller transform matrix has the form

$$L_{27}=\begin{bmatrix}
100000000000000000000000000\\
021000000000000000000000000\\
222000000000000000000000000\\
000200100000000000000000000\\
000012021000000000000000000\\
000111222000000000000000000\\
200200200000000000000000000\\
012012012000000000000000000\\
111111111000000000000000000\\
000000002000000010000000000\\
000000000012000000021000000\\
000000000111000000222000000\\
000000000000100200000200100\\
000000000000021012000012021\\
000000000000222111000111222\\
000000000100100100200200200\\
000000000210210210120120120\\
000000000222222222111111111\\
200000000200000000200000000\\
012000000012000000012000000\\
111000000111000000111000000\\
000100200000100200000100200\\
000021012000021012000021012\\
000222111000222111000222111\\
100100100100100100100100100\\
021021021021021021021021021\\
222222222222222222222222222
\end{bmatrix}. \quad (8)$$

For example, let us consider some ternary sequence F of length $N=27$

$$F=[000011011110120212110212021], \quad (9)$$

for which, taking into account (6), using the Reed-Muller transform matrix L_{27}, we find the Reed-Muller transform coefficients vector

$$A=[000000001000011120121120100]. \quad (10)$$

Each element of the ANF vector (10) is one corresponding coefficient in the general form of the ANF 3-function of three variables

$$\begin{gathered}\Phi(x_1,x_2,x_3)=a_{000}+a_{001}x_3+a_{002}x_3^2+a_{010}x_2+\\ a_{011}x_2x_3+a_{012}x_2x_3^2+a_{020}x_2^2+a_{021}x_2^2x_3+a_{022}x_2^2x_3^2+\\ +a_{100}x_1+a_{101}x_1x_3+a_{102}x_1x_3^2+a_{110}x_1x_2+a_{111}x_1x_2x_3+\\ +a_{112}x_1x_2x_3^2+a_{120}x_1x_2^2+a_{121}x_1x_2^2x_3+a_{122}x_1x_2^2x_3^2+\\ +a_{200}x_1^2+a_{201}x_1^2x_3+a_{202}x_1^2x_3^2+a_{210}x_1^2x_2+a_{211}x_1^2x_2x_3+\\ +a_{212}x_1^2x_2x_3^2+a_{220}x_1^2x_2^2+a_{221}x_1^2x_2^2x_3+a_{222}x_2^2x_2^2x_3^2.\end{gathered} \quad (11)$$

Thus, taking into account (11), we can write the ANF of sequence (9):

$$\begin{gathered}\Phi(x_1,x_2,x_3)=x_2{}^2x_3{}^2+x_1x_2x_3+x_1x_2x_3{}^2+\\ +x_1x_2{}^2+2x_1x_2{}^2x_3+x_1{}^2+2x_1{}^2x3+x_1{}^2x_3{}^2\\ +x_1{}^2x_2+2x_1{}^2x_2x_3+x_1{}^2x_2{}^2.\end{gathered} \quad (12)$$

Substituting consistently all possible sets of $\{x_1,x_2,x_3\}$ in (12), we obtain the original truth table (9).

Let us check if sequence (9) is a 3-bent-sequence. For this, it is necessary to find the absolute values of its Vilenkin-Chrestenson transform coefficients

$$\begin{gathered}|\Omega_F(\omega)|=\{\sqrt{27}\sqrt{27}\sqrt{27}\sqrt{27}\sqrt{27}\sqrt{27}\sqrt{27}\\ \sqrt{27}\sqrt{27}\sqrt{27}\sqrt{27}\sqrt{27}\sqrt{27}\sqrt{27}\sqrt{27}\sqrt{27}\sqrt{27}\\ \sqrt{27}\sqrt{27}\sqrt{27}\sqrt{27}\sqrt{27}\sqrt{27}\sqrt{27}\sqrt{27}\sqrt{27}\sqrt{27}\}.\end{gathered} \quad (13)$$

Thus, sequence (9) is indeed a 3-bent-sequence.

4 EXPERIMENTS

Let us consider each ANF coefficient of the ternary sequence a_i, where i is the vector of their three coordinates, each of which indicates the degree of occurrence of the corresponding variable in the term. Let us denote by $wt(T_i)=\sum i$ the algebraic degree of the corresponding term.

As the algebraic degree of nonlinearity we call the maximum value among all degrees of terms included in the algebraic normal form of a ternary sequence $\deg(\Phi)=\max\limits_i\{wt(T_i)\}$.

The proposed constructive synthesis method for 3-bent-sequences is based on the use of the Reed-Muller transform domain and the following determined properties of ternary bent-functions.

Property 1. The sum of a 3-bent-sequence with an affine sequence is a 3-bent-sequence.

Property 2. The maximum algebraic degree of the term included in the 3-bent-sequence of length $N=27$ is $wt(T_i)=4$.

Thus, each element of the sequence $A=\{a_i\}$, $i=0,1,...,26$ corresponds to the ANF term of 3-function in general form, as shown in the Table 1. In the Table 1 affine terms are marked by the symbol "α", while terms whose algebraic degree exceeds the value $wt(T_i)>4$ are marked by the symbol "x". The remaining terms are marked by the symbol "*".

Analysis of the data presented in Table 1 shows that the number of terms marked by the symbol "*" is 19. Thus, we write the proposed constructive method for the synthesis of 3-bent-sequences of length $N=27$ in the form of following specific steps.

Step 1. Consider the sequence in the Reed-Muller transformants domain

$$\begin{gathered}A=\begin{bmatrix}a_{000} & a_{001} & a_{002} & a_{010} & a_{011} & a_{012} & a_{020}\\ \alpha & \alpha & * & \alpha & * & * & *\end{bmatrix}\\ \begin{bmatrix}a_{021} & a_{022} & a_{100} & a_{101} & a_{102} & a_{110} & a_{111} & a_{112} & a_{120} & a_{121}\\ * & * & \alpha & * & * & * & * & * & * & *\end{bmatrix}\\ \begin{bmatrix}a_{122} & a_{200} & a_{201} & a_{202} & a_{210} & a_{211} & a_{212} & a_{220} & a_{221} & a_{222}\\ \times & * & * & * & * & * & \times & * & \times & \times\end{bmatrix}.\end{gathered} \quad (14)$$

DOI 10.15588/1607-3274-2020-1-9

Table 1 – Correspondence of terms and coefficients of 3-function ANF

a_i	T_i	Marks	a_i	T_i	Marks
a_{000}	–	α	a_{112}	$x_1x_2x_3^2$	*
a_{001}	x_3	α	a_{120}	$x_1x_2^2$	*
a_{002}	x_3^2	*	a_{121}	$x_1x_2^2x_3$	*
a_{010}	x_2	α	a_{122}	$x_1x_2^2x_3^2$	x
a_{011}	x_2x_3	*	a_{200}	x_1^2	*
a_{012}	$x_2x_3^2$	*	a_{201}	$x_1^2x_3$	*
a_{020}	x_2^2	*	a_{202}	$x_1^2x_3^2$	*
a_{021}	$x_2^2x_3$	*	a_{210}	$x_1^2x_2$	*
a_{022}	$x_2^2x_3^2$	*	a_{211}	$x_1^2x_2x_3$	*
a_{100}	x_1	α	a_{212}	$x_1^2x_2x_3^2$	x
a_{101}	x_1x_3	*	a_{220}	$x_1^2x_2^2$	*
a_{102}	$x_1x_3^2$	*	a_{221}	$x_1^2x_2^2x_3$	x
a_{110}	x_1x_2	*	a_{222}	$x_2^2x_2^2x_3^2$	x
a_{111}	$x_1x_2x_3$	*	–	–	–

Substituting the next specific values over the alphabet $\{0,1,2\}$ instead of the symbols "*", and substituting instead of the symbols "α" and "x" the values 0, we obtain a specific ternary sequence in the Reed-Muller transformants domain. This sequence, by multiplying by the matrix of the inverse Reed-Muller transform L_{27}^{-1}, is transferred to the time domain, obtaining the candidate sequence F.

Step 2. We find the absolute values of the spectral coefficients of the Vilenkin-Chrestenson transform of the sequence F and check it for the compliance with the conditions of Definition 1. If it is a 3-bent-sequence, we save the corresponding sequence A, otherwise we discard it.

Step 3. If the end of the search is not reached among all possible sequences A, we go to Step 1, otherwise the search is completed.

Step 4. For each 3-bent-sequence found, we release 4 positions marked by the symbol "α", i.e. the positions corresponding to affine terms. Substituting into them all possible values from the alphabet $\{0,1,2\}$ we obtain, on the basis of each 3-bent-sequence, a set of $3^4 = 81$ 3-bent-sequences.

Note that since in Table 1 there are 19 values marked with the symbol "*", the total number of ternary sequences that must be enumerated in the proposed algorithm is $3^{19} = 1162261467$ instead of $J_{full} = 3^{27} = 7625597484987$ in the case of complete enumeration, which is in 6561 times less.

5 RESULTS

Performing Steps 1,...,3 of the developed algorithm allowed us to find 155844 3-bent-sequences of length $N = 27$ up to affine terms.

As an example, we can give one of the found 3-bent-sequences in the form of its ANF

$$B_1 = x_2^2x_3^2 + x_1x_2x_3^2 + x_1x_2^2x_3x_1^2x_3^2 + x_1^2x_2x_3 + x_1^2x_2^2, \quad (15)$$

as well as a sequence in time domain

$$B_1 = [000011011011102122011122120]. \quad (16)$$

Note that among the found 3-bent-sequences there are 468 3-bent-sequences with an algebraic degree $\deg\{B\} = 2$, 3744 3-bent-sequences with an algebraic degree $\deg\{B\} = 3$ and 151632 3-bent-sequences with an algebraic degree $\deg\{B\} = 4$.

Accordingly, based on the obtained set of 3-bent-sequences, by applying Step 4 of the proposed algorithm, it is possible to synthesize a set of 3-bent-sequences with cardinality $155844 \cdot 3^4 = 12623364$.

A research of the found class of 3-bent-sequences of length $N = 27$ allowed us to establish that they can be classified according to the 6 possible weight structure types

$$\begin{bmatrix} \{12,9,6\}(2103894); \\ \{9,6,12\}(2103894); \\ \{6,12,9\}(2103894); \end{bmatrix} \begin{bmatrix} \{9,12,6\}(2103894); \\ \{12,6,9\}(2103894); \\ \{6,9,12\}(2103894), \end{bmatrix} \quad (17)$$

where, similar to (4), the numbers in curly brackets show, respectively, the number of characters "0", "1" and "2" in the 3-bent-sequence, and the numbers in parentheses indicate the number of 3-bent-sequences with the indicated structure.

Based on 3-bent-sequences of weight structures (17), 12 possible triple sets can be constructed

$$\begin{bmatrix} \{\{6,9,12\},\{9,12,6\},\{12,6,9\}\}; \\ \{\{6,9,12\},\{12,6,9\},\{9,12,6\}\}; \\ \{\{6,12,9\},\{9,6,12\},\{12,9,6\}\}; \\ \{\{6,12,9\},\{12,9,6\},\{9,6,12\}\}; \\ \{\{9,6,12\},\{6,12,9\},\{12,9,6\}\}; \\ \{\{9,6,12\},\{12,9,6\},\{6,12,9\}\}; \\ \{\{9,12,6\},\{6,9,12\},\{12,6,9\}\}; \\ \{\{9,12,6\},\{12,6,9\},\{6,9,12\}\}; \\ \{\{12,6,9\},\{6,9,12\},\{9,12,6\}\}; \\ \{\{12,6,9\},\{9,12,6\},\{6,9,12\}\}; \\ \{\{12,9,6\},\{6,12,9\},\{9,6,12\}\}; \\ \{\{12,9,6\},\{9,6,12\},\{6,12,9\}\}. \end{bmatrix} \quad (18)$$

DOI 10.15588/1607-3274-2020-1-9

6 DISCUSSION

The obtained set of 3-bent-sequences of length $N = 27$ is valuable not only from the point of view of the theory of synthesis of perfect algebraic constructions, but also can serve as a basis for constructing effective PRSG according to a scheme similar to Fig. 1. In view of the use of 3-bent-sequences of greater length, even the use of one possible triple set can provide a significant level of cryptographic stability. The PRSG scheme based on 3-bent-sequences of length $N = 27$ is shown on Fig. 2.

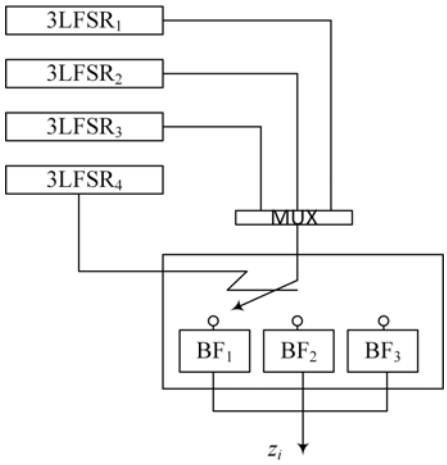

Figure 2 – PRSG scheme based on 3-bent-sequences of length $N = 27$ from one triple set

Let us determine the number of protection levels of the developed PRSG. For example, let the polynomials of the following mutually simple degrees to be chosen to construct the corresponding 3LFSR

$$\begin{cases} \deg\{f_1\} = 9; \\ \deg\{f_2\} = 8; \\ \deg\{f_3\} = 7; \\ \deg\{f_4\} = 5. \end{cases} \quad (19)$$

The number of primitive irreducible polynomials of degree $k = 9$ is $|V_9| = 1008$, of degree $k = 8$ is $|V_8| = 320$, of degree $k = 7$ is $|V_7| = 156$ and of degree $k = 5$ is $|V_8| = 22$ [14].

The initial state of $3LFSR_1$ can be selected by $3^9 - 1 = 19682$ different ways, $3LFSR_2$ by $3^8 - 1 = 6560$ ways, $3LFSR_3$ by $3^7 - 1 = 2186$ ways and $3LFSR_4$ by $3^5 - 1 = 242$ ways.

Moreover, the 3-bent-sequences themselves in the triple set can be selected by 2103894^3 ways. Thus, the number of protection levels of the constructed PRSG is defined as

$$\Psi = 1008 \cdot 320 \cdot 156 \cdot 22 \cdot 19682 \cdot 6560 \times \\ \times 2186 \cdot 242 \cdot 2103894^3 = 7.041 \cdot 10^{41}, \quad (20)$$

which is a significant value, and exceeds the number of protection levels of such a modern block symmetric cryptographic algorithm as AES-128 [15] and many other modern block symmetric chippers [16].

CONCLUSIONS

The scientific novelty lies in the fact that a method for the synthesis of 3-bent-sequences in the Reed-Muller transformants domain was developed. Using the developed method, a class of 3-bent-sequences of length $N = 27$ and cardinality $J = 12623364$ was constructed.

For the found class of 3-bent-sequences, six possible weight structures and 12 possible triple sets were discovered.

The practical significance consists in the fact that the synthesized class of 3-bent-sequences of length $N = 27$ was proposed to be used to construct the scheme of the ternary cryptographically strong PRSG. At the same time, the estimated number of protection levels of the constructed PRSG is $\Psi = 7.041 \cdot 10^{41}$, which is comparable with the number of protection levels of modern block symmetric cryptographic algorithms.

As a further area of research, it is worth to note the development of methods for the synthesis of 3-bent-sequences of longer lengths, as well as research of perfect algebraic constructions with larger values of q.

REFERENCES

1. Sokolov A. V., Zhdanov O. N. Prospects for the Application of Many-Valued Logic Functions in Cryptography, *Theory and Applications of Fuzzy Systems and Soft Computing : International Conference, 18–20 January 2018 : proceedings*. Kiev, 2018, pp. 331–339.
2. Ali Md. A., Ali E., Habib Md. A. et al. Pseudo Random Ternary Sequence and Its Autocorrelation Property Over Finite Field, *Computer Network and Information Security*, 2017, No. 9, pp. 54–63.
3. Epstain G. Multiple-valued logic design: an introduction. Boca Raton, CRC Press, 1993, 370 p.
4. Zhenxian F., Ying L. Ternary Error Correcting Codes, Chinese Science Abstracts Series A, 1995, P. 54.
5. Falkowski B. J., Olejnicka B. T. Multiple-valued and spectral approach to lossless compression of binary, gray scale and color biomedical images, *Multiple-Valued Logic : 32nd IEEE International Symposium, 15–18 May 2002 : proceedings*. Boston, 2002, pp. 136–142.
6. Falkowski B. J., Yan S. Application of Sign Hadamard-Haar Transform in Ternary Communication System, *International Journal of Electronics,* 1995, Vol. 79(5), pp. 551–559.
7. Gnatyuk S. O., Zhmurko T. O., Kinzeryavyy V. M. et al. Method of trit pseudorandom sequences generating for quantum cryptography systems, *Ukrainian Scientific Journal of Information Security*, 2015, Vol. 21, No. 2, P. 140–147.
8. Gnatyuk S. O., Zhmurko T. O., Kinzeryavy V.M. et al. Method for quality evaluation of trit pseudorandom sequence to cryptographic applications, *Information Technology and Security,* 2015, Vol. 3, No. 2(5), pp. 108–116.
9. Sokolov A. V., Zhdanov O. N., Barabanov N. A. Pseudo-random key sequence generator based on triple sets of bent-

DOI 10.15588/1607-3274-2020-1-9

functions, *Problems of physics, mathematics and technics*, 2016, No. 1(26), pp. 85–91.
10. Trachtman A. M., Trachtman V. A. Fundamentals of the theory of discrete signals on finite intervals. Moscow, Sov. radio, 1975, 208 p.
11. Zhdanov O. N., Sokolov A. V. A synthesis method of basic ternary bent-squares based on the triad shift operator, *System analysis and applied information science*, 2017, No. 1, pp. 77–85.
12. Sokolov A. V., Zhdanov O. N. Regular synthesis method of a complete class of ternary bent-sequences and their nonlinear properties, *Journal of Telecommunication, Electronic and Computer Engineering*, 2016, Vol. 8, No. 9, pp. 39–43.
13. Stankovic R. S., Astola J. T., Moraga C. Representation of Multiple-Valued Logic Functions, Morgan & Claypool Publishers, Synthesis lectures on digital circuits and systems, 2012, 153 p.
14. Burlekamp E. Algebraic Theory of Coding. Singapore, World Scientific Publishing Co, 2015, 501 p.
15. FIPS 197. Advanced encryption standard [Electronic resource], 2001, Access mode: http://csrc.nist.gov/publications/
16. Schneier B. Applied Cryptography. 2-nd edition. New York, John Wiley & Sons, 1996, 758 p.

Received 19.08.2019.
Accepted 03.12.2019.

УДК 004.622.612

МЕТОД СИНТЕЗУ ТРІЙКОВИХ БЕНТ-ФУНКЦІЙ ТРЬОХ ЗМІННИХ

Соколов А.В. – канд. техн. наук, старший викладач кафедри інформатики та управління захистом інформаційних систем, Одеський національний політехнічний університет, м. Одеса, Україна.

АНОТАЦІЯ

Актуальність. Останнім часом все частіше в сучасних криптографічних алгоритмах, зокрема, в генераторах псевдовипадкових послідовностей використовуються такі досконалі алгебраїчні конструкції багатозначної логіки, як трійкові бент-функції і їх таблиці істинності – 3-бент-последолвательності. Проте, сьогодні не існує методів синтезу класу трійкових бент-функцій для числа змінних більше двох, що істотно обмежує можливості масштабування числа рівнів захисту зазначених генераторів псевдовипадкових послідовностей. Дана обставина робить актуальним завдання розробки методів синтезу трійкових бент-функцій, яка вирішена в даній роботі для випадку трійкових бент-функцій трьох змінних. Об'єктом даного дослідження є процеси підвищення ефективності криптоалгоритмів на основі функцій багатозначної логіки.

Мета. Мета статті – побудувати метод синтезу множини трійкових бент-функцій трьох змінних.

Метод. В якості основи запропонованого конструктивного методу синтезу трійкових бент-функцій трьох змінних використано математичний апарат перетворення Ріда-Маллера (алгебраїчної нормальної форми). Так, на основі встановлених властивостей алгебраїчної нормальної форми трійкових бент-функцій і обмеженого перебору спочатку виконується пошук трійкових бент-функцій з точністю до афінних термів, після чого відбувається їх розмноження.

Результати. В результаті використання запропонованого методу синтезу трійкових бент-функцій трьох змінних знайдено 155844 бент-функції з точністю до афінного терма, в той час як потужність повної множини знайдених 3-бент-послідовностей складає 12623364. Проведені дослідження дозволили визначити, що в даній множині є 3-бент-послідовності шести різних вагових структур, на основі яких можуть бути складені 12 різних троїстих наборів для використання в генераторах псевдовипадкових послідовностей. Запропоновано схему криптографічно стійкого генератора псевдовипадкових послідовностей на основі знайденої множини 3-бент-послідовностей довжини $N = 27$. Показано, що число рівнів захисту такого генератора псевдовипадкових послідовностей складає $\Psi = 7.041 \cdot 10^{41}$, що можна порівняти з числом рівнів захисту сучасних блокових симетричних криптоалгоритмів, наприклад, AES-128.

Висновки. Подальший розвиток сучасних криптографічних алгоритмів, зокрема, криптографічно стійких генераторів псевдовипадкових послідовностей, багато в чому ґрунтується на застосуванні досконалих алгебраїчних конструкцій багатозначної логіки. В роботі вперше запропоновано конструктивний метод синтезу трійкових бент-функцій трьох змінних. Для знайденої множини трійкових бент-функцій встановлено розподіл вагових структур, а також виявлено можливі троїсті набори. На основі побудованої множини трійкових бент-функцій запропонована схема генератора псевдовипадкових послідовностей, який володіє числом рівнів захисту, яке можна порівняти з сучасними блоковими симетричними криптоалгоритмами. Відзначимо, що побудований клас трійкових бент-функцій також може бути застосований для синтезу криптографічно стійких S-блоків, кодів постійної амплітуди, а також коректуючих кодів. В якості актуального напрямку продовження проведених досліджень можна виділити побудову методів синтезу трійкових бент-функцій більшого числа змінних.

КЛЮЧОВІ СЛОВА: криптографія, генератор псевдовипадкових послідовностей, тризначна логіка, бент-функція.

УДК 004.622.612

МЕТОД СИНТЕЗА ТРОИЧНЫХ БЕНТ-ФУНКЦИЙ ТРЕХ ПЕРЕМЕННЫХ

Соколов А.В. – канд. техн. наук, старший преподаватель кафедры информатики и управления защитой информационных систем, Одесский национальный политехнический университет, г. Одесса, Украина.

АННОТАЦИЯ

Актуальность. В последнее время все чаще в современных криптографических алгоритмах, в частности, в генераторах псевдослучайных последовательностей, используются такие совершенные алгебраические конструкции многозначной логики, как троичные бент-функции и их таблицы истинности – 3-бент-последовательности. Тем не менее, сегодня не существует методов синтеза класса бент-функций для числа переменных более двух, что существенно ограничивает возможности по масштабированию числа уровней защиты указанных генераторов псевдослучайных последовательностей. Данное обстоя-

DOI 10.15588/1607-3274-2020-1-9

тельство делает актуальной задачу разработки методов синтеза троичных бент-функций, которая решена в данной работе для случая троичных бент-функций трех переменных. Объектом данного исследования являются процессы повышения эффективности криптоалгоритмов на основе функций многозначной логики.

Цель. Цель статьи – построить метод синтеза множества троичных бент-функций трех переменных.

Метод. В качестве основы предложенного конструктивного метода синтеза троичных бент-функций трех переменных использован математический аппарат преобразования Рида-Маллера (алгебраической нормальной формы). Так, на основе установленных свойств алгебраической нормальной формы троичных бент-функций и ограниченного перебора сначала выполняется поиск троичных бент-функций с точностью до аффинных термов, после чего происходит их размножение.

Результаты. В результате использования предложенного метода синтеза троичных бент-функций трех переменных найдено 155844 троичных бент-функций с точностью до аффинного терма, в то время как мощность полного множества найденных 3-бент-последовательностей составляет 12623364. Проведенные исследования позволили определить, что в данном множестве имеются 3-бент-последовательности шести различных весовых структур, на основе которых могут быть составлены 12 различных тройственных наборов для использования в генераторах псевдослучайных последовательностей. Предложена схема криптографически стойкого генератора псевдослучайных последовательностей на основе найденного множества 3-бент-последовательностей длины $N = 27$. Показано, что число уровней защиты такого генератора псевдослучайных последовательностей составляет $\Psi = 7.041 \cdot 10^{41}$, что соизмеримо с числом уровней защиты современных блочных симметричных криптоалгоритмов, например, AES-128.

Выводы. Дальнейшее развитие современных криптографических алгоритмов, в частности, криптографически стойких генераторов псевдослучайных последовательностей во многом основывается на применении совершенных алгебраических конструкций многозначной логики. В работе впервые предложен конструктивный метод синтеза троичных бент-функций трех переменных. Для найденного множества троичных бент-функций установлено распределение весовых структур, а также определены возможные тройственные наборы. На основе построенного множества троичных бент-функций предложена схема генератора псевдослучайных последовательностей, который обладает числом уровней защиты соизмеримым с современными блочными симметричными криптоалгоритмами. Отметим, что построенный класс троичных бент-функций также может быть применен для синтеза криптографически стойких S-блоков, кодов постоянной амплитуды, а также корректирующих кодов. В качестве актуального направления проведенных исследований можно выделить построение методов синтеза троичных бент-функций большего числа переменных.

КЛЮЧЕВЫЕ СЛОВА: криптография, генератор псевдослучайных последовательностей, троичная логика, бент-функция.

ЛІТЕРАТУРА / ЛИТЕРАТУРА

1. Sokolov A.V. Prospects for the Application of Many-Valued Logic Functions in Cryptography / A. V. Sokolov, O. N. Zhdanov // Theory and Applications of Fuzzy Systems and Soft Computing : International Conference, 18–20 January 2018 : proceedings. – Kiev, 2018. – P. 331–339.
2. Pseudo Random Ternary Sequence and Its Autocorrelation Property Over Finite Field / [Md. A. Ali, E. Ali, Md. A. Habib et al.] // Computer Network and Information Security. – 2017. – No. 9. – P. 54–63.
3. Epstain G. Multiple-valued logic design: an introduction / G. Epstain. – Boca Raton : CRC Press, 1993. – 370 p.
4. Zhenxian F. Ternary Error Correcting Codes / F. Zhenxian, L. Ying // Chinese Science Abstracts Series A. – 1995. – P. 54.
5. Falkowski B.J. Multiple-valued and spectral approach to lossless compression of binary, gray scale and color biomedical images / B. J. Falkowski, B. T. Olejnicka // Multiple-Valued Logic : 32nd IEEE International Symposium, 15–18 May 2002 : proceedings. – Boston, 2002. – P. 136–142.
6. Falkowski B. J. Application of Sign Hadamard-Haar Transform in Ternary Communication System / B. J. Falkowski, S. Yan // International Journal of Electronics. – 1995. – Vol. 79(5). – P. 551–559.
7. Метод генерування тритових псевдовипадкових послідовностей для систем квантової криптографії / [С. О. Гнатюк, Т. О. Жмурко, В. М. Кінзерявий та ін.] // Безпека інформації. – 2015. – Т. 21, № 2. – С. 140–147.
8. Метод оцінювання якості трійкових псевдовипадкових послідовностей для криптографічних застосувань / [С. О. Гнатюк, Т. О. Жмурко, В. М. Кінзерявий та ін.] // Information Technology and Security. – 2015. – Т. 3, № 2(5). – С. 108–116.
9. Соколов А.В. Генератор псевдослучайных ключевых последовательностей на основе тройственных наборов бент-функций / А. В. Соколов, О. Н. Жданов, Н. А. Барабанов // Проблемы физики, математики и техники. – 2016. – №1(26). – С. 85–91.
10. Трахтман А. М. Основы теории дискретных сигналов на конечных интервалах / А. М. Трахтман, В. А. Трахтман. – М. : Сов. радио, 1975. – 208 с.
11. Жданов О. Н. Метод синтеза базовых троичных бент-квадратов на основе оператора триадного сдвига / О. Н. Жданов, А. В. Соколов // Системный анализ и прикладная информатика. – 2017. – № 1. – С. 77 – 85.
12. Sokolov A. V. Regular synthesis method of a complete class of ternary bent-sequences and their nonlinear properties / A. V. Sokolov, O. N. Zhdanov // Journal of Telecommunication, Electronic and Computer Engineering. – 2016. – Vol. 8, No. 9. – P. 39–43.
13. Stankovic R. S. Representation of Multiple-Valued Logic Functions / R. S. Stankovic, J. T. Astola, C. Moraga. – Morgan & Claypool Publishers, Synthesis lectures on digital circuits and systems, 2012. –153 p.
14. Burlekamp E. Algebraic Theory of Coding / E. Burlekamp. – Singapore : World Scientific Publishing Co, 2015. – 501 p.
15. FIPS 197. Advanced encryption standard [Electronic resource]. – 2001. – Access mode: http://csrc.nist.gov/publications/
16. Schneier B. Applied Cryptography. 2-nd edition / B. Schneier. – New York : John Wiley & Sons, 1996. – 758 p.

DOI 10.15588/1607-3274-2020-1-9