ISSN 2707-1898 (print)

Український журнал інформаційних технологій
Ukrainian Journal of Information Technology
http://science.lpnu.ua/uk/ujit
https://doi.org/10.23939/ujit2023.02.041
Article received 30.07.2023 p.
Article accepted 26.10.2023 p.
UDK 004.056.5

Correspondence author
A. V. Sokolov
radiosquid@gmail.com

UDC 004.056.5

O. V. Bakunina[1], N. M. Balandina[1], A. V. Sokolov[2]

[1] National University "Odesa Law Academy", Odesa, Ukraine
[2] Odesa Polytechnic National University, Odesa, Ukraine

SYNTHESIS METHOD FOR S-BOXES BASED ON GALOIS FIELD TRANSFORM MATRICES

Cryptographic methods today are a crucial tool for constructing information security systems. At the same time, to solve the problem of encrypting large amounts of information, block or stream symmetric ciphers are mainly preferred because of their efficiency and proven cryptographic strength, including against perspective quantum cryptanalysis. The effectiveness of modern symmetric ciphers largely depends on the cryptographic S-boxes applied in their construction, the quality of which largely determines the degree of implementation of the concepts of diffusion and confusion by the cryptographic algorithm, while the presence of large sets of cryptographically high-quality S-boxes is also important, in the terms of their application as a long-term key. Today, the Nyberg construction is well-known and widely applied in ciphers, including widespread AES block symmetric cipher. This construction allows you to synthesize high-quality S-boxes that harmoniously satisfy the main criteria for cryptographic quality, however, the set of S-boxes synthesized using this construction is small, which makes the task of developing new methods for synthesizing large sets of cryptographically high-quality S-boxes highly relevant. At the same time, as research shows, the constructions of extended Galois fields are a promising raw material for solving this problem. In this paper, the Galois field transform matrices of order N=256 are constructed for all isomorphic representations of the extended Galois field GF(256) which are analogous to the Reed-Muller transform but for the case of many-valued logic functions. As part of the research, the isomorphism invariant row numbers of the Galois field transform matrices are identified, which allows to obtain bijective S-boxes, as well as bijective S-boxes that correspond to the main criteria for cryptographic quality of component Boolean functions such as algebraic degree of nonlinearity, distance of nonlinearity, error propagation criterion, and criterion of minimization of correlation of output and input vectors of the S-box. At the same time, the cardinality of the set of synthesized S-boxes is ~23 times higher than the cardinality of the set of S-boxes of the Nyberg construction, which allows them to be used as a long-term key. The proposed S-boxes can become the basis for improving the effectiveness of existing symmetric cryptographic algorithms and developing new ciphers.

Keywords: cryptography; Boolean function; many-valued logic function; cryptographic quality.

Introduction / Вступ

The main component of almost any information protection system today is a cryptographic component, which makes it impossible to read encrypted information without a cryptographic key. At the same time, while asymmetric cryptographic algorithms, due to their significant computational complexity, are used in practice mostly to solve the task of key distribution and digital signature, the symmetric ciphers remain the main component used to encrypt large amounts of protected data. Block and stream symmetric ciphers are characterized as fast, proven cryptographic strength and easy-to-implement algorithms.

In turn, the main component of modern ciphers, which largely determines the level of diffusion and confusion [1] they provide, is the cryptographic S-box. To date, to estimate the degree of implementation of the concept of diffusion and confusion by the cryptographic S-box, as well as the degree of its resistance to the main attacks of cryptanalysis, an approach is used based on the representation of the S-box in the form of its component Boolean functions, to which, subsequently, a set of cryptographic criteria is applied. The main criteria for S-box cryptographic quality are the following: the criterion for maximizing the algebraic nonlinearity, the criterion for maximizing the distance of the nonlinearity, the strict avalanche criterion, and the criterion for minimizing the correlation of the output and input vectors.

An important task is the synthesis of cryptographic S-boxes that would harmoniously correspond to the listed criteria for cryptographic quality, which can be achieved by using the constructions of Galois fields. An example of such a well-known method is the Nyberg construction, however, this method allows obtaining only small cardinalities of high-quality S-boxes, which makes the task of de-

veloping new methods for the synthesis of S-boxes based on Galois field constructions relevant.

Object of research – is the process of increasing the effectiveness of modern cryptographic algorithms.

Subject of research – is methods for synthesizing cryptographic S-boxes based on the constructions of Galois fields.

The purpose of the research – is to develop a method for synthesizing cryptographically high-quality S-boxes of length $N = 256$ based on Galois field transform matrices.

To achieve this purpose, the following main *research objectives* are identified:

1. Construct Galois field transform matrices of order $N = 256$ for all isomorphic representations of the Galois field $GF(256)$.

2. Research the structure of the constructed matrices and determine their rows that can serve as raw material for constructing cryptographically high-quality bijective S-boxes.

3. Develop a method for constructing cryptographic S-boxes based on the Galois field transform matrices in the form of specific steps.

4. Estimate the values of the cryptographic quality indicators and the cardinality of the set of constructed S-boxes.

Materials and methods of research. To date, there are several approaches for estimating the cryptographic quality of S-boxes, in particular, based on their representation using component Boolean functions [2], as well as using component functions of many-valued logic, for which special cryptographic quality criteria are applied, for example, [3].

In this paper, to estimate the cryptographic quality of the synthesized S-boxes, we use the generally accepted approach, which is based on the representation of S-boxes in the form of their component Boolean functions. Since the length of the proposed S-boxes is $N = 256$, they can be represented as $k = 8$ component Boolean functions, while the overall cryptographic quality of the S-box is determined by the weakest of them. Among the many existing criteria for the cryptographic quality of component Boolean functions, we have selected the following set of basic criteria:

1. Algebraic degree of nonlinearity, which is defined as the largest number of conjunctions in terms of the algebraic normal form of a component Boolean function [4]. In this case, the vector of coefficients at the terms of the algebraic normal form of a Boolean function can be constructed using the Reed-Muller transform as

$$A = f \cdot L_N, \tag{1}$$

where f is the truth table of the Boolean function over the alphabet $\{0,1\}$, L_N is the Reed-Muller transform matrix, which can be constructed in accordance with the following recursive formula

$$L_1 = [1], \quad L_{2N} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \otimes L_N = \begin{bmatrix} L_N & 0 \\ L_N & L_N \end{bmatrix}, \tag{2}$$

where $\otimes$ denotes the Kronecker product.

2. The nonlinearity distance of a Boolean function, which can be defined as the minimum of the Hamming distance between its component Boolean functions and all codewords of the affine code [5]

$$N_S = \min\left\{\operatorname{dist}(f_i, \varphi_j)\right\}, \ i = 1,...,k, \ j = 1,...,2^{k+1}, \tag{3}$$

where f_i is a component Boolean function; φ_j are the codewords of the affine $A(N,k)$-code, $\operatorname{dist}(\bullet)$ is the operator for the Hamming distance evaluation.

3. Correspondence to the error propagation criterion [5], for the evaluation of which we use the minimum and maximum values of the weight of the derivatives of the component Boolean functions

$$D_u f(x) = f(x) \oplus f(x \oplus u), \tag{4}$$

along all directions $\forall u \in V_k$, $wt(u) = 1$, where V_k is a linear vector space of vectors of length k, $wt(\bullet)$ is the operator for evaluation of the Hamming weight. The ideal case, when all derivatives (4) are balanced, i.e., their Hamming weights are equal to $N/2$, means that the component Boolean function corresponds to the strict avalanche criterion, i.e., the probability of changing its output when changing the value of any of its inputs is equal to 0.5.

4. Criterion for minimizing the correlation of the output and input vectors [5]. To estimate the correspondence of the S-box to this criterion, we use the maximum along the absolute values of the correlation coefficients $\max\left\{\left|r_{i,j}\right|\right\}$ of the correlation matrix $R = \left\|r_{i,j}\right\|$, which determines the degree of the linear relationship between the output y and input x vectors of the S-box

$$r_{i,j} = 1 - \frac{\sum_{m=1}^{N} (x_{m,i} \oplus y_{m,j})}{N/2}, \ i, j = 0,...,k-1, \tag{5}$$

where the symbol $\oplus$ denotes mod2 summation.

Analysis of recent research and publications. Quite a lot of modern publications are devoted to the issues of synthesis of S-boxes of a given length that would correspond to the specified criteria of cryptographic quality, where a wide variety of algorithms are used for their construction: starting from algorithms for their synthesis based on de Bruijn sequences, as, for example, it is proposed in [6], ending with methods for the synthesis of S-boxes based on the theory of dynamic chaos [7], [8], [9], [10], some of which are characterized by a significant level of cryptographic quality, for example, [11].

Nevertheless, in practice, for the construction of cryptographic algorithms, the most essential are S-boxes, which would have a balanced set of cryptographic quality indicators, which is most easily achievable using Galois field constructions. For example, in the cryptographic algorithm AES [12], which, to date, is de facto the most popular and widely used cryptographic algorithm in the World, the Nyberg construction is used, based on the operation of finding the inverse element in the extended Galois field $GF(2^8)$. A lot of research is devoted to the cryptographic properties of S-boxes, in particular [13], while the paper [3] is devoted to the research of the cryptographic properties of S-boxes of the Nyberg construction [2] in the case of their representation using many-valued logic functions.

Anyhow, the Nyberg construction is characterized by the small cardinalities of S-boxes that can be synthesized, which does not allow them to be used as a long-term key, which is important in a number of cryptographic applications.

In this paper, we show that the possibilities of synthesizing S-boxes over extended Galois fields are not exhausted and the cardinalities of sets of synthesized S-boxes using extended Galois fields can be increased by developing new constructions of cryptographically high-quality S-boxes based on the Galois field transform matrices for the extended Galois field $GF(2^8)$.

Research results and their discussion / Результати дослідження та їх обговорення

The theory and practice of synthesizing the algebraic normal form (ANF) of many-valued logic functions (q-functions) or so-called Galois filed expressions [14] are dynamically developing in modern cryptography.

Definition 1 [14]. A function of q-valued logic of k variables is a mapping $\{0,1,2,...,q-1\}^k \to \{0,1,2,...,q-1\}$.

When $q=2$ we obtain Boolean functions.

Further, from the point of view of the practice of constructing S-boxes, we will consider many-valued logic functions with values of $q=2^k$.

In [14] it is shown that any function of many-valued logic can be uniquely (up to isomorphism) represented over a Galois field $GF(2^k)$ using a polynomial containing the operations "Addition in the Galois field $GF(2^k)$ ", "Multiplication in the Galois field $GF(2^k)$ ".

In this case, specific aspects of finding the ANF for the case of extended Galois fields $GF(2^2)$ and $GF(2^4)$ are considered in [15].

The transition to the Galois field expressions can be performed according to the following formula

$$\begin{bmatrix} A = g \cdot L_N, \\ g = A \cdot L_N^{-1}, \end{bmatrix} \quad (6)$$

where g is the truth table of the Boolean function, $A \in GF(2^k)$ is the Galois filed expression vector.

It is known [14] that for the case of many-valued logic functions of a $k=1$ variable, the construction of the Galois field inverse transform matrix L_N^{-1}, $N=q^k$ over the Galois field $GF(2^k)$ can be performed in accordance with the following construction

$$L_1^{-1} = \begin{bmatrix} \alpha_0^0 & \alpha_0^1 & \cdots & \alpha_0^{q-1} \\ \alpha_1^0 & \alpha_1^1 & \cdots & \alpha_1^{q-1} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{q-1}^0 & \alpha_{q-1}^1 & \cdots & \alpha_{q-1}^{q-1} \end{bmatrix}, \quad (7)$$

where $\alpha_i \in GF(2^k), i=0,1,...,q-1$ are the elements of the extended Galois field.

For the case of many-valued logic functions, in contrast to the case of Reed-Muller transform matrix for Boolean functions (2), the direct and inverse Galois field transform matrices do not coincide, i.e. $L_N \neq L_N^{-1}$, thus the direct Reed-Muller transform matrix can be found using one of the algorithms for finding inverse matrices in extended Galois fields [16].

Note, however, that different isomorphic representations of Galois fields $GF(2^k)$, imply different implementations of the multiplication operation (as well as exponentiation and division operations derived from it) in accordance with the rule determined by the irreducible polynomial $\psi(z)$ based on which the Galois field $GF(2^k)$ is constructed.

Thus, for a Galois field $GF(2^k)$, a many-valued logic function can have a number of different isomorphic mappings in the ANF domain, which corresponds to the number of irreducible polynomials of degree k, on the basis of which Galois field arithmetic can be built.

In this case, the number of existing irreducible polynomials of degree k whose coefficients belong to the Galois field $GF(2)$ is determined in accordance with the formula [17]

$$|\Psi_k| = \frac{1}{k} \sum_{d \,//\, k} \mu(d) 2^{(k/d)}, \quad (8)$$

where d are the divisors of the degree value k; $\mu(d)$ is the Möbius function; notation $d//k$ means that d divides k by an integer.

So, for the case of the Galois field $GF(2^8)$ we are considering, in accordance with (8), the number of irreducible polynomials is equal to $|\Psi_8| = 30$, while the decimal equivalents of these polynomials have the following form

$$\begin{aligned} \Psi_8 = \{&283,285,299,301,313,319,333,351,355,357, \\ &361,369,375,379,391,\ 395,397,415,419,425,433, \\ &445,451,463,471,477,487,499,501,505\}. \end{aligned} \quad (9)$$

As an example, we present in Fig. in the form of grayscale images (where the color of each pixel corresponds to the value of the matrix element in the Galois field $GF(2^8)$ in the range from 0 – black, to 255 – white) of the first six matrices of the Galois field transform for isomorphic representations of the Galois field $GF(2^8)$ built on the basis of the irreducible polynomials

$$\begin{aligned} \psi_1(z) &= 283_{10} = 100011011_2 = z^8 + z^4 + z^3 + z + 1, \\ \psi_2(z) &= 285_{10} = 100011101_2 = z^8 + z^4 + z^3 + z^2 + 1, \\ \psi_3(z) &= 299_{10} = 100101011_2 = z^8 + z^5 + z^3 + z + 1, \\ \psi_4(z) &= 301_{10} = 100101101_2 = z^8 + z^5 + z^3 + z^2 + 1, \\ \psi_5(z) &= 313_{10} = 100111001_2 = z^8 + z^5 + z^4 + z^3 + 1, \\ \psi_6(z) &= 319_{10} = 100111111_2 = z^8 + z^5 + z^4 + z^3 + z^2 + z + 1. \end{aligned} \quad (10)$$

Analysis of the data represented on Fig. 1 shows that the Galois field transform matrix structure strongly depends on the chosen isomorphism of the selected extended Galois field $GF(2^8)$.

The research performed have shown that the rows of the Galois field transform matrix are characterized by sufficiently high values of the main indicators of cryptographic quality, therefore they can be used for the tasks of constructing high-quality S-boxes.

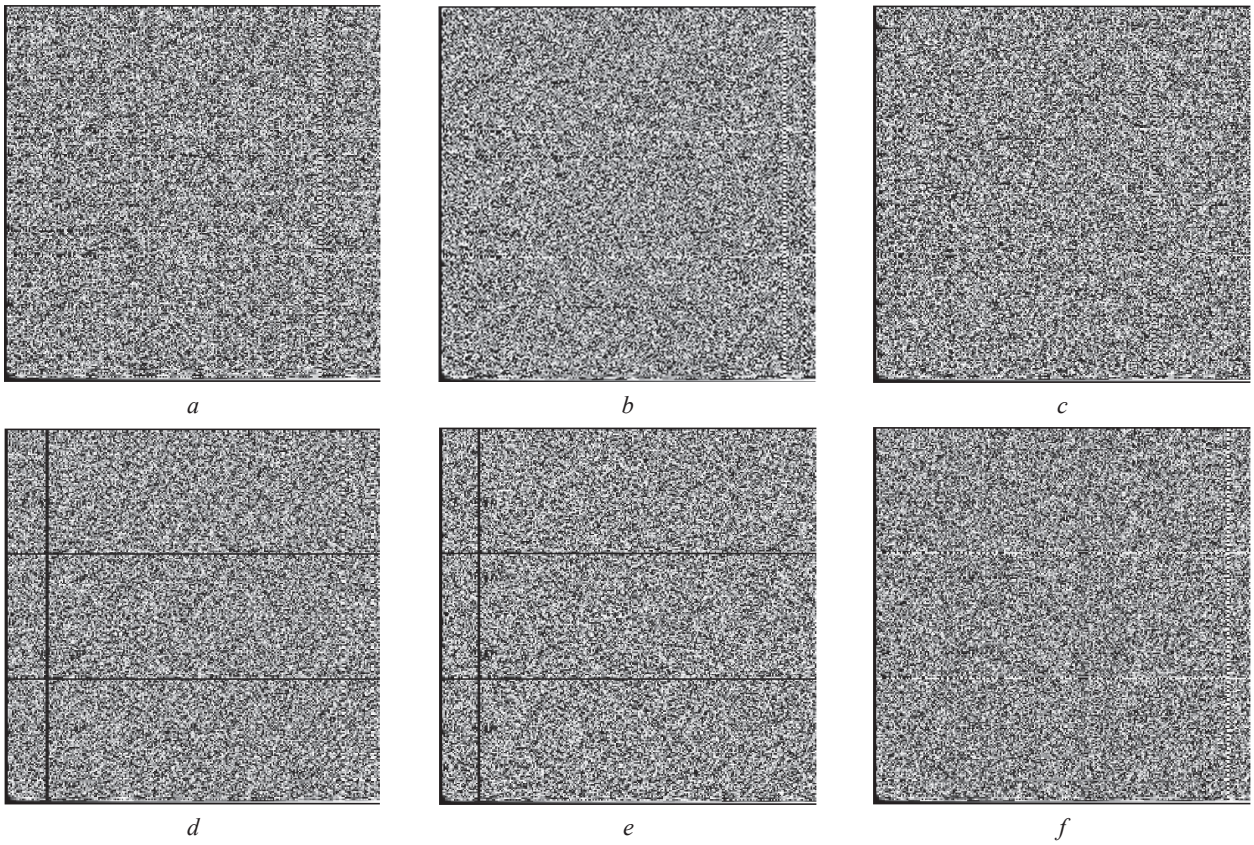

Fig. Examples of Galois field transform matrices for polynomials ψ_1 (a.), ψ_2 (b.), ψ_3 (c.), ψ_4 (d.), ψ_5 (e.), and ψ_6 (f.) / Приклади матриць GF-перетворення для поліномів ψ_1 (a.), ψ_2 (b.), ψ_3 (c.), ψ_4 (d.), ψ_5 (e.) і ψ_6 (f.)

A detailed research of the structure of the Galois field transform matrices of the order $N = 256$ over all isomorphic representations of the Galois field $GF(2^8)$ made it possible to establish that only half of the rows of these matrices contain all elements of the Galois field $GF(2^8)$, which means that it is suitable for constructing bijective S-boxes. The numbers of these rows are invariant to the isomorphism of the Galois field $GF(2^8)$ and are given in the form of the following expression

$$\begin{gathered}\Upsilon' = \{2,3,5,8,9,12,14,15,17,20,23,24,27,29,30,32,\\ 33,38,39,42,44,45,47,48,50,53,54,57,59,\\ 60,62,63,65,68,72,74,75,77,78,80,83,84,\\ 87,89,90,92,93,95,98,99,102,104,105,107,\\ 108,110,113,114,117,119,122,123,125,128,129,132,\\ 134,135,138,140,143,144,147,149,150,\\ 152,153,155,158,159,162,164,165,167,168,170,\\ 173,174,177,179,180,182,183,185,189,192,\\ 194,195,197,198,200,203,204,207,209,\\ 210,212,213,215,218,219,224,225,227,228,\\ 230,233,234,237,240,\\ 242,243,245,248,249,252,254,255\}.\end{gathered} \quad (11)$$

However, not all rows from (11) of the Galois field transform matrices have the same level of cryptographic quality. Research performed has identified 24 row numbers that, regardless of isomorphism, provide the construction of S-boxes with the best level of cryptographic quality.

$$\begin{gathered}\Upsilon = \{2,3,5,8,9,15,17,29,33,38,42,57,65,74,75,83,113,\\ 129,132,147,149,165,194,225\}.\end{gathered} \quad (12)$$

When using the set of rows (12) for the task of constructing S-boxes, their cryptographic quality is exceptionally stable regardless of isomorphism.

Thus, we can write the proposed method for constructing cryptographic S-boxes based on the Galois field transform matrices in the form of specific steps:

Step 1. Select the initial parameters of the method, which are: the length of the S-box N and the corresponding extended Galois field $GF(2^k)$, $k = \log_2 N$; a specific irreducible polynomial that defines the rules of arithmetic in an extended field $GF(2^k)$.

Step 2. On the basis of (7) construct the inverse Galois field transform matrix L_N^{-1}.

Step 3. Using one of the well-known matrix inversion algorithms in extended Galois fields [16] on the basis of the inverse Galois field transform matrix L_N^{-1}, find the direct Galois field transform matrix L_N.

Step 4. Select the rows of the Galois field transform matrix containing all elements of the extended Galois field $GF(2^k)$.

Step 5. Representing the rows of the Galois field transform matrix selected in *Step 4* in the form of S-boxes of length N, estimate the level of their compliance with the main cryptographic quality criteria, as a result of which, select the S-boxes that best correspond to the criteria that are considered as the crucial when upgrading or designing a cryptographic algorithm.

Discussion of research results. In view of the practical significance and demand for use in modern symmetric ciphers and hash functions of cryptographic S-boxes that perform byte-by-byte transform of input data, the following method parameters were chosen for the experiment: S-box length $N = 256$, all possible isomorphic representations of the main Galois field $GF(2^8)$ based on irreducible polynomials (9).

In Table 1 we present the results of experimental research on the correspondence of S-boxes constructed on the basis of the proposed method to the main criteria of cryptographic quality. At the same time, in Table 1, the following notation is adopted: ψ denotes the decimal equivalent of an irreducible polynomial used to construct the Galois field transform matrix; $\deg(S)$ denotes the values of the algebraic degree of nonlinearity of S-boxes constructed in a given isomorphic representation of the Galois field $GF(2^8)$; N_S denotes the nonlinearity distance of S-boxes constructed in a given isomorphic representation of the Galois field $GF(2^8)$; $wt(D_u f)$ denotes the values of the weights of the directional derivatives of the component Boolean functions of S-boxes for a given isomorphic representation of the Galois field $GF(2^8)$; $|r_{i,j}|$ denotes the values of the correlation coefficient matrices for S-boxes for a given isomorphic representation of the Galois field $GF(2^8)$. In the research, the results of which are shown in Table 1 the Galois field transform matrix rows determined in (12) were selected.

Analysis of the data presented in Table 1 allows us to conclude that the cryptographic quality of S-boxes based on the rows of the Galois field transform matrices is high and stable. In terms of the cryptographic quality of their component Boolean functions, the constructed S-boxes are not inferior when compared with the Nyberg construction S-box. Moreover, the total number of S-boxes for all isomorphic representations of the $GF(2^8)$ is equal to $J = |\Upsilon| \cdot |\Psi| = 24 \cdot 30 = 720$. Research have shown that the number of unique S-boxes among this set is 691, which is ~23 times greater than the number of S-boxes of the Nyberg construction in the same extended Galois field.

We also note that the algebraic degree of nonlinearity of S-boxes based on Galois field transform matrices depends on the selected row number of the matrix on the basis of which the S-box is constructed. In Table 2 we show the values of the algebraic degrees of nonlinearity depending on the row number (12).

Table 1. Values of cryptographic quality indicators for constructed S-boxes / Значення показників криптографічної якості для побудованих S-блоків

ψ	$\deg(S)$	N_S	$wt(D_u f)$	$\lvert r_{i,j} \rvert$
283	5…7	112	108…156	0…0.1250
285	5…7	112	108…156	0…0.1250
299	5…7	112	108…156	0…0.1250
301	5…7	112	108…156	0.0156…0.1250
313	5…7	112	108…156	0…0.1250
319	5…7	112	108…156	0.0156…0.1250
333	5…7	112	108…156	0…0.1250
351	5…7	112	108…156	0…0.1250
355	5…7	112	108…156	0…0.1250
357	5…7	112	108…156	0…0.1250
361	5…7	112	108…156	0…0.1250
369	5…7	112	108…156	0…0.1250
375	5…7	112	108…156	0…0.1250
379	5…7	112	108…156	0…0.1250
391	5…7	112	108…156	0…0.1250
395	5…7	112	108…156	0…0.1250
397	5…7	112	108…156	0…0.1250
415	5…7	112	108…152	0.0156…0.1250
419	5…7	112	108…156	0…0.1250
425	5…7	112	108…156	0.0156…0.1250
433	5…7	112	108…156	0.0156…0.1250
445	5…7	112	108…156	0…0.1250
451	5…7	112	108…156	0…0.1250
463	5…7	112	108…156	0…0.1250
471	5…7	112	108…156	0…0.1250
477	5…7	112	108…156	0…0.1250
487	5…7	112	108…156	0.0156…0.1250
499	5…7	112	108…156	0…0.1250
501	5…7	112	108…156	0…0.1250
505	5…7	112	108…156	0…0.1250

Table 2. Values of the algebraic degree of nonlinearity depending on the row number of the Galois field transform matrix / Значення алгебраїчного степеня нелінійності залежно від номера рядка матриці GF-перетворення

$\upsilon_i \in \Upsilon$	2	3	5	8	9	15	17	29	33	38	42	57
$\deg(S)$	7	7	7	5	7	5	7	5	7	5	5	5
$\upsilon_i \in \Upsilon$	65	74	75	83	113	129	132	147	149	165	194	225
$\deg(S)$	7	5	5	5	5	7	5	5	5	5	5	5

Let us consider an example of an S-box based on the second row of the Galois field transform matrix in the Galois field $GF(2^8)$ whose arithmetic is determined by an irreducible polynomial $\psi_1(z) = 283_{10} = z^8 + z^4 + z^3 + z + 1$, which we represent as the following algebraic construction

S_1	0	1	2	3	4	5	6	7	8	9	*A*	*B*	*C*	*D*	*E*	*F*
0	00	01	8E	F4	47	A7	7A	BA	AD	9D	DD	98	3D	AA	5D	96
1	D8	72	C0	58	E0	3E	4C	66	90	DE	55	80	A0	83	4B	2A
2	6C	ED	39	51	60	56	2C	8A	70	D0	1F	4A	26	8B	33	6E
3	48	89	6F	2E	A4	C3	40	5E	50	22	CF	A9	AB	0C	15	E1
4	36	5F	F8	D5	92	4E	A6	04	30	88	2B	1E	16	67	45	93
5	38	23	68	8C	81	1A	25	61	13	C1	CB	63	97	0E	37	41
6	24	57	CA	5B	B9	C4	17	4D	52	8D	EF	B3	20	EC	2F	32
7	28	D1	11	D9	E9	FB	DA	79	DB	77	06	BB	84	CD	FE	FC.
8	1B	54	A1	1D	7C	CC	E4	B0	49	31	27	2D	53	69	02	F5
9	18	DF	44	4F	9B	BC	0F	5C	0B	DC	BD	94	AC	09	C7	A2
A	1C	82	9F	C6	34	C2	46	05	CE	3B	0D	3C	9C	08	BE	B7
B	87	E5	EE	6B	EB	F2	BF	AF	C5	64	07	7B	95	9A	AE	B6
C	12	59	A5	35	65	B8	A3	9E	D2	F7	62	5A	85	7D	A8	3A
D	29	71	C8	F6	F9	43	D7	D6	10	73	76	78	99	0A	19	91
E	14	3F	E6	F0	86	B1	E2	F1	FA	74	F3	B4	6D	21	B2	6A
F	E3	E7	B5	EA	03	8F	D3	C9	42	D4	E8	75	7F	FF	7E	FD

(13)

The nonlinearity distance of the S-box (13) is equal to $N_{S_1} = 112$, its algebraic degree of nonlinearity value is $\deg(S_1) = 7$.

We present the matrix of weights of S-box (13) component Boolean functions derivatives

e_j	$wt(D_{1,k})$	$wt(D_{2,k})$	$wt(D_{3,k})$	$wt(D_{4,k})$	$wt(D_{5,k})$	$wt(D_{6,k})$	$wt(D_{7,k})$	$wt(D_{8,k})$
10000000	128	116	120	124	136	112	116	116
01000000	116	124	144	144	112	116	116	128
00100000	124	128	120	132	116	116	128	116
00010000	128	128	132	124	116	128	116	124
00001000	128	116	116	124	128	116	124	128
00000100	116	132	120	140	116	124	128	128
00000010	132	124	136	140	124	128	128	116
00000001	124	136	124	136	128	128	116	132

, (14)

as well as its matrix of correlation coefficients

$$R = \begin{bmatrix} 0.016 & 0 & -0.016 & 0.047 & 0.094 & 0.016 & 0.094 & 0.047 \\ 0 & 0.094 & 0.094 & 0.047 & 0.016 & 0.094 & 0.047 & 0.016 \\ -0.016 & 0.094 & 0.063 & 0 & -0.094 & 0.063 & -0.109 & 0.078 \\ 0.047 & 0.047 & 0 & 0.031 & 0.063 & 0.031 & -0.109 & -0.031 \\ 0.094 & 0.016 & -0.094 & 0.063 & -0.063 & -0.063 & 0.125 & 0.094 \\ 0.016 & 0.094 & 0.063 & 0.031 & -0.063 & 0.125 & 0.094 & 0.094 \\ 0.094 & 0.047 & -0.109 & -0.109 & 0.125 & 0.094 & 0.094 & 0.016 \\ 0.047 & 0.016 & 0.078 & -0.031 & 0.094 & 0.094 & 0.016 & 0.094 \end{bmatrix}. \quad (15)$$

Thus, the set of constructed S-boxes, in particular, S-box (13) is not inferior in its cryptographic quality to well-known S-box constructions, such as the Nyberg construction, and can be recommended for practical application in the tasks of improving the effectiveness of existing cryptographic algorithms, as well as the development of new promising ciphers.

Scientific novelty of the obtained research results – the methodology for synthesizing S-boxes based on Galois field constructions was further developed, as a result of which an effective method for synthesizing large sets of high-quality S-boxes based on Galois fields transform matrices was presented.

Practical significance of the research results – the practical value of the results obtained lies in the possibility of applying of the developed S-boxes to improve existing cryptographic algorithms or develop new ones. At the same time, the level of cryptographic quality of the proposed S-boxes is the same as for well-known Nyberg construction, while the cardinality of their set exceeds the cardinality of the Nyberg construction by ~23 times.

Conclusions / Висновок

We note the main results of the research performed:

1. It is shown that Galois field transform matrices can become the raw material for constructing cryptographically high-quality S-boxes. An efficient method for constructing cryptographically high-quality S-boxes of practically valuable lengths based on Galois field transform matrices has been proposed.

2. For the most applied in practice value of the S-boxes length $N = 256$, based on the proposed method for synthesizing S-boxes on the basis of Galois field transform matrices, a class of S-boxes was synthesized, the cryptographic quality indicators for which are not inferior to the well-known Nyberg construction, however, the cardinality of the presented class is in ~23 times greater when compared with the cardinality of the Nyberg construction S-boxes class.

3. In view of the high level of cryptographic quality of the proposed S-boxes, they can be recommended for practical use in order to improve existing cryptographic algorithms (block and stream symmetric ciphers, hash functions, generators of pseudo-random key sequences), as well as to develop promising ciphers.

As possible directions for further research, we can highlight the possibility of researching the cryptographic properties of S-boxes when they are represented using ANF constructed with the help of Galois field transform for values of $q = N$, i.e. using a single many-valued logic function, which could be the basis for the development of new effective methods for the synthesis of large classes of cryptographically high-quality S-boxes.

References

[1] Shannon, C. E. (1949). Communication theory of secrecy systems. *The Bell system technical journal,* 28(4), 656–715. https://doi.org/10.1002/j.1538-7305.1949.tb00928.x

[2] Mazurkov, M. I., & Sokolov, A. V. (2013). Nonlinear transformations based on complete classes of isomorphic and automorphic representations of field GF (256). *Radioelectronics and Communications Systems,* 56(11), 513–521. https://doi.org/10.3103/s0735272713110022

[3] Sokolov, A. V., & Djiofack, T. V. N. (2019). Nonlinear Properties of Rijndael S-boxes Represented by the Many-Valued Logic Functions. Proceedings of the International Workshop on Cyber Hygiene, Kyiv, Ukraine, 96–106.

[4] Rostovcev, A. G. (2002). Cryptography and Data Protection, SPb.: Mir i Sem'ja.

[5] Logachev, O. A., Sal'nikov, A. A., & Jashhenko, V. V. (2012). Boolean functions in coding theory and cryptology, USA: American Mathematical Society.

[6] Mazurkov, M. I., & Sokolov, A. V. (2013). Constructive method for synthesis of complete classes of multilevel de Bruijn sequences. Radioelectronics and Communications Systems, 56(1), 36–41. https://doi.org/10.3103/s0735272713010044

[7] Wang, J., Zhu, Y., Zhou, C., & Qi, Z. (2020). Construction Method and Performance Analysis of Chaotic S-Box Based on a Memorable Simulated Annealing Algorithm. *Symmetry,* 12, 2115. https://doi.org/10.3390/sym12122115

[8] Lambić, D. (2018). S-box design method based on improved one-dimensional discrete chaotic map. *Journal of Information and Telecommunication,* 2(2), 181–191. https://doi.org/10.1080/24751839.2018.1434723

[9] Lu, Q., Zhu, C., & Wang, G. (2019). A Novel S-Box Design Algorithm Based on a New Compound Chaotic System. *Entropy,* 21(10), 1004. https://doi.org/10.3390/e21101004

[10] Lai, Q., Akgul, A., Li, C., Xu, G., Çavuşoğlu, U. (2018). A New Chaotic System with Multiple Attractors: Dynamic Analysis, Circuit Realization and S-Box Design, *Entropy,* 20(1), 12. https://doi.org/10.3390/e20010012

[11] Hussain, I., Anees, A., Al-Maadeed, T., & Mustafa M. (2019). Construction of S-Box Based on Chaotic Map and Algebraic Structures. *Symmetry,* 11(3), 351. https://doi.org/10.3390/sym11030351

[12] FIPS 197 (2001) Advanced encryption standard. Retrieved from: http://csrc.nist.gov/publications/

[13] Waheed, A., Subhan, F., Suud, M.M., Alam, M., & Ahmad, S. (2023). An analytical review of current S-box design methodologies, performance evaluation criteria, and major challenges. *Multimedia Tools and Applications,* 82(19), 1–24. https://doi.org/10.1007/s11042-023-14910-3

[14] Stankovic, R. S., Astola, J. T., & Moraga, C. (2012). Representations of Multiple-Valued Logic Functions. Morgan and Claypool Publishers, 2012.

[15] Sokolov, A.V., & Overchuk, Yu.S. (2018). On the possibility of synthesizing an algebraic normal form of quaternary functions over the field GF (4). Proceedings of the first international scientific and practical conference "Problems of cyber security of information and telecommunication systems", 384–388.

[16] Grošek, O., & Fabšič, T. (2018). Computing multiplicative inverses in finite fields by long division, *Journal of Electrical Engineering*, 69(5), 400–402. https://doi.org/10.2478/jee-2018-0059

[17] Berlekamp, E. R. (2015) Algebraic coding theory: Revised Edition. World Scientific. https://doi.org/10.1142/9407

О. В. Бакуніна[1], Н. М. Баландіна[1], А. В. Соколов[2]

[1] Національний університет "Одеська юридична академія", м. Одеса, Україна
[2] Національний університет "Одеська політехніка", м. Одеса, Україна

МЕТОД СИНТЕЗУ S-БЛОКІВ НА ОСНОВІ МАТРИЦЬ GF-ПЕРЕТВОРЕННЯ

Криптографічні методи сьогодні є найважливішим інструментом для побудови систем захисту інформації. Водночас для вирішення проблеми шифрування великих обсягів інформації перевагу зазвичай віддають блоковим або потоковим симетричним шифрам, зважаючи на їх ефективність і доведену криптографічну стійкість, зокрема проти атак перспективного квантового криптоаналізу. Ефективність сучасних симетричних шифрів значною мі-

рою залежить від застосованих у їх конструкції криптографічних S-блоків, якість яких багато в чому визначає ступінь реалізації концепцій дифузії та конфузії криптоалгоритмом, тоді як наявність великих наборів криптографічно високоякісних S-блоків також важлива, із погляду їх застосування як довгострокового ключа. Сьогодні добре відома конструкція Ніберг, яку широко застосовують у шифрах, серед яких поширений блоковий симетричний шифр AES. Ця конструкція дає змогу синтезувати високоякісні S-блоки, які гармонійно задовольняють основні критерії криптографічної якості, однак множини S-блоків, синтезовані за допомогою цієї конструкції, невеликі, що актуалізує завдання розроблення нових методів синтезу великих множин криптографічно високоякісних S-блоків. Водночас, як показують дослідження, конструкції розширених полів Галуа є перспективним вихідним матеріалом для вирішення цієї проблеми. У цій статті побудовано матриці GF-перетворення порядку N=256 для всіх ізоморфних представлень розширеного поля Галуа GF(256), які є аналогічними перетворенню Ріда – Маллера для випадку функцій багатозначної логіки. У межах дослідження ідентифіковано інваріантні до ізоморфізму номери рядків матриць GF-перетворення, що дають змогу отримати біективні S-блоки, зокрема такі, що відповідають основним критеріям криптографічної якості компонентних булевих функцій, таким як алгебраїчний степінь нелінійності, відстань нелінійності, критерій поширення помилки та критерій мінімізації кореляції векторів виходу та входу S-блока. Потужність набору синтезованих S-блоків у ~23 рази перевищує потужність набору S-блоків конструкції Ніберг, що дає змогу використовувати їх як довгостроковий ключ. Запропоновані S-блоки можуть стати основою для підвищення ефективності наявних симетричних криптографічних алгоритмів, а також для розроблення нових шифрів.

Ключові слова: криптографія; булева функція; функція багатозначної логіки; криптографічна якість.

Інформація про авторів:

Бакуніна Олена Валеріївна, канд. фіз.-мат. наук, доцент, кафедра кібербезпеки.
Email: elenabakunina72@gmail.com; https://orcid.org/0000-0002-5700-7321

Баландіна Наталія Миколаївна, ст. викладач, кафедра кібербезпеки.
Email: nataliabalandina2103@gmail.com; https://orcid.org/0000-0002-3121-4517

Соколов Артем Вікторович, д-р техн. наук, доцент, кафедра кібербезпеки та програмного забезпечення.
Email: radiosquid@gmail.com; https://orcid.org/0000-0003-0283-7229

Цитування за ДСТУ: Бакуніна О. В., Баландіна Н. М., Соколов А. В. Метод синтезу s-блоків на основі матриць gf-перетворення. *Український журнал інформаційних технологій.* 2023. Т. 5, № 2. С. 41–48.

Citation APA: Bakunina, O. V., Balandina, N. M., & Sokolov, A. V. (2023). Synthesis method for s-boxes based on galois field transform matrices. *Ukrainian Journal of Information Technology*, 5(2), 41–48. https://doi.org/10.23939/ujit2023.02.041