UDC 681.3.06

IMPROVEMENT OF THE METHOD FOR OPTIMAL S-BOXES GENERATION

M.Yu. RODINKO, R.V. OLIYNYKOV, T.O. HRINENKO

The known method of high nonlinear S-boxes generation based on the gradient descent requires a consecutive application of several criteria for each formed substitution. This paper presents improvement of the considered method by the appropriate selection of the criteria application order which decreases the required computation power for S-box generation. The proposed modification allows generation of a byte substitution with nonlinearity 104, algebraic immunity 3 and 8-uniformity within approximately 30 minutes of a single PC running time.

Keywords: S-box, nonlinearity, algebraic immunity, vectorial Boolean function.

INTRODUCTION

Block ciphers are among the most spread cryptographic primitives. Such algorithms are used to provide data confidentiality and integrity, as well as they are used as a core element of other cryptographic transformations like pseudorandom sequences generators, hash functions, etc. [1, 2].

Each block cipher contains a nonlinear function in a quotient ring for providing nonlinear dependence between plaintext, key and ciphertext [3]. Often such a function is implemented using a substitution table (S-box).

S-box properties have serious impact to the cipher strength (and its margin) against various methods of cryptanalysis [4, 5]. Appropriate selection of S-boxes allows reducing the number of rounds of iterative symmetric transformation (increasing performance) keeping its cryptographic strength.

S-boxes are called optimal if they are satisfied a set of essential criteria reaching extreme values for differential, linear and algebraic characteristics [6].

Most known methods of S-box generation are insufficiently effective for obtaining substitutions with optimal cryptographic characteristics on a single PC.

This paper presents improvement of the known high nonlinearity S-boxes generation method [7] allowing several times decrease of required computation power.

1. THE S-BOXES SELECTION CRITERIA

Basic S-boxes selection criteria can be divided into two groups. The first one includes the criteria taking into account the transformation strength against cryptanalysis methods. Currently as the main characteristics are considered the following: differential [8], linear [9] and algebraic [10].

The second group includes criteria based on the S-box Boolean functions cryptographic properties evaluation [11]. These include nonlinearity, the autocorrelation maximum, distribution criterion and others. However, as shown in [6], many of this group criteria are unessential or redundant for applications in block transformations. Thus, the following criteria considered to be essential [6].

1. The maximum value of difference distribution table (DDT) is defined as

$$\delta = \max_{\alpha\in F_2^n,\alpha\neq 0,\beta\in F_2^n} \#\{x \mid S(x)\oplus S(x\oplus\alpha)=\beta\}.$$

This value influences the cipher strength against differential cryptanalysis, which is one of the most universal and effective attacks on block ciphers.

Equivalent to a maximum value of differential table is the notion of δ-uniformity [12].

Definition 1. *Let G_1 and G_2 be finite Abelian groups. A mapping F: $G_1 \to G_2$ is called differentially δ-uniform if for all $\alpha \in G_1$, $\alpha \neq 0$ and $\beta \in G_2$*

$$|\{z \in G_1 | F(z+\alpha) - F(z) = \beta\}| \le \delta.$$

According to this definition, the optimal characteristics of resistance of transformation F against differential attacks are associated with low values of δ-uniformity. Obviously that the requirement of low values of δ-uniformity is equivalent to the requirement of low values of the maximum value of non-trivial difference transformation. Therefore to achieve a high strength of cryptographic transformation it is necessary to obtain low values of δ-uniformity.

2. The maximum absolute value of linear approximation table (LAT) is defined as

$$\lambda = \max_{\alpha,\beta\neq 0}\left|LAT(\alpha,\beta)-2^{n-1}\right|,$$

where

$$LAT(\alpha,\beta) = \\ = \#\left\{x \,\middle|\, x\in Z_2^n, \bigoplus_{s=0}^{N}(x[s]\cdot\alpha[s]) = \bigoplus_{t=0}^{N}(S(x)[t]\cdot\beta[t])\right\},$$

and $\mu[s]$ – bit s of value μ.

The property influences the cipher strength against linear cryptanalysis. In [13] it was shown that the complete set of linear characteristics, called linear hull, should be taken into consideration for precise evaluation of the cipher strength against linear attacks.

A large part of the known methods of evaluating of block cipher strength to differential and linear cryptanalysis based on the differential and linear properties of S-boxes used in their construction. In [14] it was shown that the SPN structure with maximal diffusion layer provides a provable security against differential (linear) cryptanalysis: the probability of each differential (linear hull) is bounded by p^n (q^n), where p (q) is a maximal non-trivial differential (linear) probability of n active S-boxes.

3. The minimum degree of S-box Boolean function (BF). Each S-box can be represented as a set of Boolean functions. Let $S = (f_0, f_1, \ldots, f_{m-1})$ – substitution $n \times m$, where f_i – Boolean function from n variables. The minimum degree of S-box [15] is defined as

$$deg(S) = \min_{0<j<2^m} \left(deg\left(g_j\right) \right),$$

where g_j – a set of all linear combinations of f_i; $deg\left(g_j\right)$ – the maximum degree of Boolean function represented in ANF.

4. Algebraic immunity characterizes the cipher strength against algebraic attack, i.e., a minimum degree of an overdefined system of equations which can be used to describe the S-box. At such description of the S-box a lower terms degree can be received than when presenting in the form of a set of Boolean functions.

In general form for S-box $n \times m$ the required number of equations of system of degree d is [6]

$$r = N_c - Rank(A),$$

where

$$N_c = \sum_{i=0}^{d} C_{n+m}^{i},$$

where $Rank(A)$ – rank of the binary matrix A containing all possible multiplications of input and output bits of S-box.

Dimensionality of such matrix is

$$|A| = \left(2^n\right) \times N_c.$$

5. The absence of fixed points. According to this criterion substitution S must not have such transitions that $S(x) = x$. In most ciphers criterion is used for protection against statistical attacks.

The nonlinearity of S-box is also assumed to be a one of the main criterion. In terms of Boolean functions [15], the nonlinearity of substitution S is

$$NL(S) = \min_{0<j<2^n} \left(NL\left(g_j\right) \right),$$

where $NL\left(g_j\right)$ – minimal Hamming distance between the function g_j and all affine functions over the field $GF(2^n)$.

However, the value of nonlinearity is uniquely determined from the maximum of linear approximation table [15] and for substitution S of degree 2^n is

$$NL(S) = 2^{n-1} - \frac{1}{2} \max_{\alpha,\beta \in GF\left(2^n\right)} \left| LAT(\alpha,\beta) \right|.$$

2. OPTIMAL S-BOXES GENERATION

A large part of all existing methods of S-boxes generation can be divided into two types: algebraic [16, 17] or random. The latter are simpler for implementation, but with computational power for practical implementation limited to the single PC it is possible to obtain byte substitutions with nonlinearity up to 98.

Table 1 shows the properties research results of randomly generated substitutions of degree $n = 2^8$. The sample in the given experiment obtained for 10 million substitutions. During the experiment no substitution with nonlinearity 100 has been found. Herewith, all generated S-boxes satisfied the criterion of algebraic immunity. In [6] it was obtained random substitutions with nonlinearity 100, but on the cluster of 4096 computers.

Contrary to random generation methods, the algebraic ones suggest the S-boxes on the basis of balanced Boolean functions with nonlinearity 112.

Table 1

Cryptographic properties of randomly generated S-boxes

Criterion	Value	% of S-boxes satisfying criterion
The maximum of DDT	8	0,004
The maximum of LAT (nonlinearity)	32 (96)	11
	30 (98)	0,15
	28 (100)	0
The minimum degree of BF	7	30
Algebraic immunity	3	100

Among the algebraic methods of S-boxes generation it is widely used the power operations in the finite field [16]. Such substitutions were considered the most optimal for a long time, and Rijndael/AES [18] also uses this type of S-box. However, these byte substitutions have the unwanted property: the value of their algebraic immunity is only two that creates the potential cipher vulnerability to algebraic attacks.

The considered method of high nonlinear S-boxes generation providing both algebraic immunity and strength to the differential and linear cryptanalysis has the following steps [7].

1. Pseudorandom substitution generation:

1.1. generation permutation S based on vectorial Boolean function that implements power transformation in the finite field;

1.2. random swap of N value pairs of permutation S and forming permutation S'.

2. Compliance test of generated permutation S' to the S-box criteria set.

The given algorithm combines the advantages of algebraic and random methods of S-boxes generation and allows obtaining the substitution with an algebraic immunity 3 and nonlinearity up to 104. The problem of the existence of permutations with a higher nonlinearity while maintaining high values of algebraic immunity remains open.

Another method that allows obtaining the S-boxes with nonlinearity 104 has been proposed in [19]. The method combines the special genetic algorithm with total tree searching. However, the author does not give any information about the values of other indicators of obtained substitutions.

We note that the block symmetric cipher Kalyna [20] and the hash function Kupyna [21] presented in the corresponding new Ukrainian standards use S-boxes with the best currently known cryptographic characteristics (given in the Table 2).

Thus, the modified method of gradient descent is currently assumed to be the most effective method of the optimal S-boxes generation. However, the method can be further optimized in terms of performance for using on a single PC.

Table 2

Cryptographic characteristics of substitutions from the Kalyna and Kupyna

Characteristic	Value
The maximum of DDT	8
The maximum of LAT	24
The minimum degree of BF	7
Nonlinearity	104
Algebraic immunity	3
The absence of fixed points	Yes

3. OPTIMIZATION OF S-BOXES GENERATION METHOD

As input parameters the method of generating S-boxes accepts the following [7]:

– vectorial Boolean function $F(x)$ (with nonlinearity 112 and the maximum of difference distribution table equal to 4);

– the number of random pairs of values N to be swapped.

As a vectorial Boolean function is proposed to use $F(x) = x^d$. To obtain possible values of degree d it is used the following formula [16]:

$$d = (2^n - 1) - 2^i,\ i = 0,...,7.$$

Table 3 shows the vectorial Boolean functions permitted for use in the *S*-boxes generation algorithm with $n = 2^8$.

Table 3

List of the vectorial Boolean functions permitted for use

i	$F(x)$
0	x^{127}
1	x^{191}
2	x^{223}
3	x^{239}
4	x^{247}
5	x^{251}
6	x^{253}
7	x^{254}

A value of $N = 22$, at which all necessary properties of the S-box are reached, has been obtained in [6].

The following PEA-equivalent transformation is applied to the final substitution not only for removing fixed points, but also for destruction cyclic structure:

$$F(x) = M_1 \cdot G(M_2 \cdot x \oplus V_2) \oplus V_1 .$$

The main part of computational resources is spent on the second stage of the search S-boxes – checking substitutions for compliance to the selection criteria set. Optimization of this stage significantly decreases the *S*-boxes generation time.

Selection criteria of substitutions are partially interdependent. Changing the order of applying the criteria can substantially reduce the search time of S-box. Let's consider the principle of finding the most optimal order of applying the criteria.

Let there be given k selection criteria substitutions $\xi_0 ,..., \xi_{k-1}$. Then the number of possible combinations of k criteria specifying the order of their use is $k!$.

Let F_σ, where $\sigma \in [0; k!)$, is a combination of the criteria of the following form:

$$F_\sigma = \xi_{\theta_{k-1}(\sigma)} \circ \xi_{\theta_{k-2}(\sigma)} \circ \ldots \circ \xi_{\theta_i(\sigma)} \circ \ldots \circ \xi_{\theta_0(\sigma)} ,$$

where $\theta_i(\sigma) \in [0; k)$ – function that sets criterion for the i-th position in combination F_σ.

Let $T(F_\sigma)$ be a function returning time of checking a single substitution using a criteria sequence F_σ. Then the problem of minimizing time of checking substitution for compliance of k criteria is to find t_{min}:

$$t_{\min} = \min_{0 \le \sigma < k!} \left(T(F_\sigma) \right).$$

The combination of the criteria F_σ corresponding to the value t_{min} is the most optimal.

Now define an analytic expression for finding the values of the function $T(F_\sigma)$. It is introduced the following factors influencing time of substitution check: p_i – probability that the substitution satisfies the i-th criterion; v_i – time of checking of one substitution to compliance to the i-th criterion.

Here the index i denotes the ordinal number of criterion in the particular combination F_σ. Application of criteria is performed from right to left.

The values of the factors are found experimentally because there no analytical methods for their obtaining at the moment.

Using these factors, the following expression for $T(F_\sigma)$ was got:

$$T(F_\sigma) = \sum_{i=0}^{k-1} (\varphi_i \cdot v_i),$$

where $\varphi_0 = 1$, $\varphi_i = \varphi_{i-1} \cdot p_{i-1}$, $i = 1 \ldots k-1$.

Minimizing the function $T(F_\sigma)$ allows to get the optimal criteria sequence application for the S-boxes generation.

4. PRACTICAL RESULTS

4.1. Comparison of theoretical and empirical results

The proposed optimization was used for byte S-boxes generation with application of the following four criteria ($k = 4$):

– the maximum of DDT $a = 8$;

– the maximum of LAT $b = 26$;

– the minimum degree of BF $c = 7$;

– algebraic immunity $d = 3$.

Substitutions generation is performed on the basis of a vectorial Boolean function $F(x) = x^{254}$.

Table 5 shows the experimentally obtained values of the factors p and v.

According to the formula the values of function $T(F_\sigma)$ for combinations of criteria $F_\sigma \in [0; 24)$ were calculated. The calculated values are shown in Table 6.

Table 5

The values of factors for four criteria

Criterion	Factor p	Factor v, sec
a	0.66	0.0003
b	0.1	0.0017
c	0.3	0.0018
d	0.6	0.0067

According to the Table 6 $t_{\min} = 0.0016735$ value of the function is obtained for the combination of criteria $d \circ c \circ b \circ a$.

Values given in the Table 6 is time taken to check a single substitution. Experiments have shown that for one S-box generation satisfying four criteria 102 substitutions must be checked on the average. Thus, the time of S-box generation can be calculated as $T_{theor}(F_\sigma) = T(F_\sigma) \cdot 102$.

Experimental values of S-box generation time for all combinations of criteria were obtained. Fig. 1 shows graphs of functions $T_{theor}(F_\sigma)$ (continuous curve) and $T_{exp}(F_\sigma)$ (dotted curve).

4.2. High nonlinear S-boxes generation

The values of the function were calculated and it was chosen the best order of the criteria application for optimal S-boxes generation for the following set:

– the maximum of DDT $a = 8$;

– the maximum of LAT $b = 24$ (compared with the previous case the nonlinearity increased to 104);

– the minimum degree of BF $c = 7$;

– algebraic immunity $d = 3$;

– the absence of short cycles (up to 3).

Experiments have shown that the probability that the substitution has nonlinearity 104 is equal to 0,0000007.

The absence of short cycles is reached by applying PEA-equivalence to the given S-box, so it is not necessary to include this criterion to the list of criteria when the minimum of time is been calculating.

The minimum value $t_{\min} = 0{,}001422$ when combinations of criteria $d \circ c \circ b \circ a$ and $c \circ d \circ b \circ a$.

To generate an optimal S-box it is needed to check 1,100,000 substitutions on average. Thus, the average generation time of the one optimal S-box equals to $t_{\min} \cdot 1{,}100{,}000 = 0.001422 \cdot 1{,}100{,}000 = 1564.2$ sec. $\approx$ 26 minutes. The experimental results of optimal substitution generation time confirms analytically obtained value.

CONCLUSIONS

The paper presents the optimization of the known S-box generation method with high nonlinearity, based on the time minimization of S-box checking for compliance with the set of criteria. The presented approach allows the order determination of the selection criteria application in which the checking time of S-box will be minimal.

Table 6

The calculated values of function $T(F_\sigma)$

A number of criteria combination	The order of application of the criteria	The value of function $T(F_\sigma)$	A number of criteria combination	The order of application of the criteria	The value of function $T(F_\sigma)$
0	$a \circ b \circ c \circ d$	0.0080914	12	$c \circ a \circ b \circ d$	0.0078093
1	$a \circ b \circ d \circ c$	0.0041214	13	$c \circ a \circ d \circ b$	0.0024593
2	$a \circ c \circ b \circ d$	0.0078334	14	$c \circ b \circ a \circ d$	0.0076245
3	$a \circ c \circ d \circ b$	0.0024834	15	$c \circ b \circ d \circ a$	0.0054665
4	$a \circ d \circ b \circ c$	0.0025164	16	$c \circ d \circ a \circ b$	0.0022435
5	$a \circ d \circ c \circ b$	0.0020864	17	$c \circ d \circ b \circ a$	0.0019355
6	$b \circ a \circ c \circ d$	0.0080360	18	$d \circ a \circ b \circ c$	0.0024517
7	$b \circ a \circ d \circ c$	0.0040660	19	$d \circ a \circ c \circ b$	0.0020217
8	$b \circ c \circ a \circ d$	0.0077948	20	$d \circ b \circ a \circ c$	0.0023593
9	$b \circ c \circ d \circ a$	0.0056368	21	$d \circ b \circ c \circ a$	0.0019573
10	$b \circ d \circ a \circ c$	0.0034186	22	$d \circ c \circ a \circ b$	0.0019815
11	$b \circ d \circ c \circ a$	0.0030166	23	$d \circ c \circ b \circ a$	0.0016735

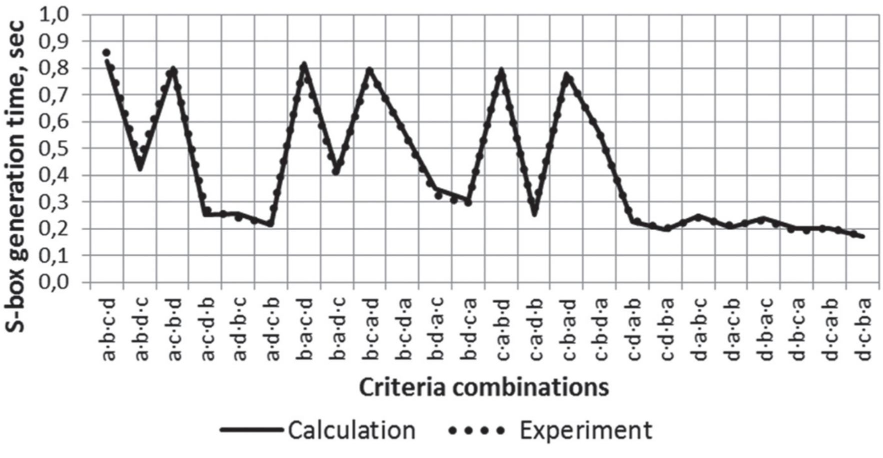

Fig. 1. Graphs of functions $T_{theor}(F_\sigma)$ and $T_{exp}(F_\sigma)$

Two variants of the optimal order of the criteria application on the S-boxes generation were proposed. Software implementation on a single PC allows to reach average 30 minutes generation time for a permutation of 2^8 degree with nonlinearity 104.

References

[1] *Menezes Alfred J.* Handbook of Applied Cryptography [Text] / Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone.

[2] *Gorbenko Ivan Dmytrovych.* Applied cryptology. Theory. Practice. Application [Text]: monograph / Gorbenko I.D., Gorbenko Yu.I.; Kharkiv National University of Radioelectronics, JSC “Institute of Information Technologies”. – Kharkiv: Fort, 2012. 868 pp. (in Ukrainian).

[3] *Shannon C.E.* Communication Theory of Secrecy Systems [Text] / C.E Shannon // Bell System Technical Journal. - 1949. - Vol. 28. – pp. 656-715.

[4] *Soroka L.S.* The research of differential properties of block symmetric / L.S. Soroka, O.O. Kuznetsov, I.V. Moskovchenko, S.A. Isayev // Information processing systems. – 2010. - № 6(87). – 286–294 pp. (in Russian).

[5] *Oliynykov R.* An Impact Of S-box Boolean Function Properties To Strength Of Modern Symmetric Block Ciphers / R. Oliynykov, O. Kazymyrov // Радиотехника. – 2011. – Вып. 166. – С. 11-17.

[6] *Kazymyrov O.V.* Methods and Techniques of Generation of Nonlinear Substitutions for Symmetric Encryption Algorithms / O.V. Kazymyrov // The thesis for the scholarly degree of candidate of technical sciences, speciality 05.13.21 – Information security systems. – Kharkiv National University of Radioelectronics, Kharkiv, 2014 (in Russian).

[7] *Kazymyrov O.* A Method For Generation Of High-Nonlinear S-boxes Based On Gradient Descent / O. Kazymyrov, V. Kazymyrova, R. Oliynykov // IACR Cryptology ePrint Archive, 2013. – p. 578.

[8] *Biham E.* Differential Cryptanalysis of DES-like Cryptosystem [Text] / E. Biham, A. Shamir // Journal of Cryptology. – 1991. – Vol. 4. – pp. 3-72.

[9] *Matsui, M.* Linear Cryptoanalysis Method for DES Cipher [Text] / M. Mitsuru // EUROCRYPT’93. - May 1993. – pp. W112–123.

[10] *Courtois N. T.* Cryptanalysis of block ciphers with overdefined systems of equations [Text] / N. T. Courtois, J. Pieprzyk // Advances in Cryptology – ASIACRYPT 2002 : proceedings of the 8th International Conference on the Theory and Application of Cryptology and Information Security, Queenstown, New Zealand, December 1–5, 2002. – Berlin ; Heidelberg : Springer, 2002. – P. 267–287. – (Lecture Notes in Computer Science; vol. 2501).

[11] *Y. Crama and P.L. Hammer.* Boolean Models and Methods in Mathematics, Computer Science and Engineering / Encyclopedia of Mathematics and its Applications. V. 2, Cambridge University Press, 2010.

[12] *K. Nyberg*, Differentially uniform mapping for cryptography, Copyright (c) 1998, Springer-Verlag.

[13] *K. Nyberg*, Linear approximation of block ciphers, Advances in Cryptology – Eurocrypt’94, Lecture Notes in Computer Science, vol. 950, Springer-Verlag, 1994.

[14] *S. Hong, S. Lee, J. Lim, J. Sung, D. Cheon and I. Cho*, Provable Security against Differential and Linear cryptanalysis for SPN Structure. B. Schneier (Ed.): FSE 2000, LNCS 1978, pp. 273-283, 2001.

[15] *Carlet C.* Vectorial Boolean Functions for Cryptography [Text] / C. Carlet // Boolean Models and Methods in Mathematics, Computer Science, and Engineering / ed. Y. Crama, P. Hammer. – Cambridge : Cambridge University Press, 2010. – P. 398–469.

[16] *Nyberg K.* Perfect nonlinear S-boxes [Text] / K. Nyberg // Advances in Cryptology – EUROCRYPT ‘91 : proceedings of the Workshop on the Theory and Application of of Cryptographic Techniques, Brighton, UK, April 8–11, 1991. Berlin ; Heidelberg : Springer, 1991. – P. 378–386. – (Lecture Notes in Computer Science; vol. 547).

[17] *Kazymyrov O.V.* Vectorial Boolean functions application in substitutions generation for symmetric cryptographic transformation [Text] / O.V. Kazymyrov, R.V. Oliynykov // Information processing systems. – 2012. – № 6 (104). – 97–102 pp. (in Russian).

[18] *Daemen J., Rijmen V.,* AES submission, Document on Rijndael, Version 2, September 1999, pp1-45.

[19] *TESAR P.* A New Method for Generating High Nonlinearity SBoxes [Text] / Petr TESAR // Radioengineering. – 2010. – Vol. 19, № 1. – P. 23–26.

[20] *Roman Oliynykov, Ivan Gorbenko, Oleksandr Kazymyrov, Victor Ruzhentsev, Oleksandr Kuznetsov, Yurii Gorbenko, Oleksandr Dyrda, Viktor Dolgov, Andrii Pushkaryov, Ruslan Mordvinov, Dmytro Kaidalov.* DSTU 7624:2014. National Standard of Ukraine. Information technologies. Cryptographic Data Security. Symmetric block transformation algorithm. Ministry of Economical Development and Trade of Ukraine, 2015 (in Ukrainian).

[21] *Roman Oliynykov, Ivan Gorbenko, Oleksandr Kazymyrov, Victor Ruzhentsev, Artem Boyko, Oleksandr Kuznetsov, Yurii Gorbenko, Viktor Dolgov, Oleksandr Dyrda, Andrii Pushkaryov.* DSTU 7564:2014. National Standard of Ukraine. Information technologies. Cryptographic Data Security. Hash function. Ministry of Economical Development and Trade of Ukraine, 2015 (in Ukrainian).

APPENDIX A

EXAMPLES OF THE OPTIMAL S-BOXES

An example of the optimal S-box based on the Vectorial Boolean function x^{191} (hexadecimal notation)

5c	06	e1	54	39	4c	9b	08	f4	32	c1	22	7a	0b	81	47
79	e2	a5	10	76	e4	86	c0	2a	75	1c	77	f0	1e	3d	a4
91	19	34	95	7d	85	b8	c7	a7	3b	e8	cd	4d	b4	fc	bb
7c	17	42	98	31	ec	bc	f5	5d	fb	02	4f	4e	78	e6	94
e7	30	2c	0d	e0	f3	bf	fa	db	ba	15	1d	40	18	ca	b1
f9	03	d0	d8	ad	44	3a	72	a2	73	df	66	01	fe	be	fd
ef	e3	a9	cb	28	b2	d5	2b	23	2e	99	5e	2d	5b	c8	48
6e	8f	f6	c5	d7	cc	82	65	14	67	c3	1f	26	e9	8c	97
a1	71	8d	ae	1b	ee	c6	68	84	b9	60	87	5f	9c	49	6b
b6	b0	6f	ff	d9	b7	38	cf	a0	eb	8b	4a	f7	3f	3e	da
80	b5	59	0c	6a	1a	96	d2	89	8e	9e	d4	24	25	16	ab
a6	9d	33	70	05	74	63	7b	5a	36	6d	4b	ea	dd	f8	ac
21	2f	69	53	51	f2	7f	92	9a	6c	43	00	d6	50	a3	46
c9	29	90	37	c2	41	7e	09	55	58	20	aa	27	e5	88	64
61	f1	d3	af	d1	11	9f	0a	0e	13	12	3c	dc	35	ed	45
93	b3	c4	bd	57	62	52	8a	a8	0f	04	ce	de	07	83	56

An example of the optimal S-box based on the Vectorial Boolean function x^{254} (hexadecimal notation)

1a	a8	96	a1	a6	97	80	26	c1	f2	32	7f	8b	c9	f0	c3
64	79	27	10	43	4c	6c	9b	c4	ac	d8	ea	b2	9e	d5	8e
7d	02	c7	0e	17	83	cb	07	61	e0	84	fa	3e	03	7a	24
be	8c	19	6f	1d	f7	b8	68	b3	e6	db	78	d1	cd	0a	a7
a3	b4	f1	fc	3f	5d	57	4f	42	8d	ca	71	5f	ab	66	d9
a0	72	16	ad	9c	2c	49	30	bb	99	31	ce	34	3c	fe	d3
18	d0	ef	cf	82	36	cc	6d	d6	b7	c6	5c	58	86	20	e4
75	7e	87	41	8a	53	1f	21	63	67	74	37	0c	2d	91	48
54	df	38	73	44	b1	ae	40	2a	62	fb	c5	f5	1c	4d	af
45	70	dc	95	04	ec	0f	bc	fd	6b	0d	a2	2e	93	3a	eb
59	aa	c0	55	06	ed	e1	50	4b	d7	5a	65	4a	e3	25	a9
c8	b5	5b	76	47	05	14	22	2f	81	9a	0b	c2	77	09	35
90	1e	e9	3d	7b	f4	51	92	29	33	b0	9d	23	d2	12	6a
89	2b	d4	28	dd	f6	f8	8f	08	69	39	00	a5	e5	e2	88
52	1b	f9	da	bf	b9	f3	60	13	ff	56	7c	de	6e	5e	85
3b	9f	e8	11	4e	bd	94	a4	46	ba	ee	15	98	01	b6	e7

Manuscript received October, 6, 2015

Rodinko Mariia Yuriivna, Master Student of Information Technologies Security Department at KNURE. Scientific interests: symmetric cryptography and cryptanalysis.

Oliynykov Roman Vasylovych, Doctor of Technical Sciences, Professor at Information Technologies Security Department at KNURE. Scientific interests: symmetric cryptography and cryptanalysis, network security.

Hrinenko Tetiiana Oleksiivna, Candidate of Technical Sciences (PhD), Associate Professor at Information Technologies Security Department at KNURE. Scientific interests: information technologies security.

УДК 681.3.06

Усовершенствование метода генерации оптимальных S-блоков / М.Ю. Родинко, Р.В. Олейников, Т.А. Гриненко // Прикладная радиоэлектроника: научн.-техн. журнал. – 2015. – Том 14. – № 4. – С. 315–320.

Известный метод генерации S-блоков с высокой нелинейностью, основанный на градиентном спуске, предполагает последовательное применение нескольких критериев к каждой сформированной подстановке. В данной работе представлено усовершенствование рассматриваемого метода путем выбора порядка применения критериев, для которого требуемая вычислительная мощность для генерации подстановок будет наименьшей. Предложенная модификация позволяет сгенерировать байтовую подстановку с нелинейностью 104, алгебраическим иммунитетом 3 и 8-равномерностью в пределах приблизительно 30 минут на персональном компьютере.

Ключевые слова: S-блок, нелинейность, алгебраический иммунитет, векторная булева функция.

Табл.: 6. Ил.: 1. Библиогр.: 21 наим.

УДК 681.3.06

Удосконалення методу генерації оптимальних S-блоків / М.Ю. Родінко, Р.В. Олійников, Т.О. Гріненко // Прикладна радіоелектроніка: наук.-техн. журнал. – 2015. – Том 14. – № 4. – С. 315–320.

Відомий метод генерації S-блоків з високою нелінійністю, заснований на градієнтному спуску, передбачає послідовне застосування декількох критеріїв до кожної сформованої підстановки. У даній роботі наведено удосконалення методу, що розглядається, шляхом вибору порядку застосування критеріїв, для якого потрібна обчислювальна потужність для генерації підстановок буде найменшою. Запропонована модифікація дозволяє згенерувати байтову підстановку з нелінійністю 104, алгебраїчним імунітетом 3 та 8-рівномірністю в межах приблизно 30 хвилин на персональному комп'ютері.

Ключові слова: S-блок, нелінійність, алгебраїчний імунітет, векторна булева функція.

Табл.: 6. Іл.: 1. Бібліогр.: 21 найм.