DE GRUYTER
OPEN

TATRA
MOUNTAINS
Mathematical Publications

DOI: 10.1515/tmmp-2017-0020
Tatra Mt. Math. Publ. **70** (2017), 93–105

OPTIMIZATION OF THE HIGH NONLINEAR S-BOXES GENERATION METHOD

Mariia Rodinko — Roman Oliynykov — Yurii Gorbenko

ABSTRACT. The known method of high nonlinear S-boxes generation based on the gradient descent [Kazymyrov, O. V.: *Methods and Techniques of Generation of Nonlinear Substitutions for Symmetric Encryption Algorithms*. 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)] requires consecutive applications of several criteria for each formed substitution. This paper presents an improvement of the considered method by the appropriate selection of the criteria application order which decreases the required computational 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.

1. Introduction

Block ciphers are among the most extensively employed cryptographic primitives. Such algorithms are used to provide data confidentiality and integrity, as well 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 function is implemented by means of a substitution table (S-box).

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

2010 Mathematics Subject Classification: 94A60, 68P25.
Keywords: S-box, nonlinearity, algebraic immunity, vectorial Boolean function.

S-boxes are called optimal if they satisfy 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 an improvement of the known high nonlinearity S-boxes generation method [7] allowing several times reduction of required computational power.

2. 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 cryptanalytic methods. Currently, the following characteristics are considered the main ones: differential [8], linear [9] and algebraic [10].

The second group includes criteria based on the evaluation of the S-box Boolean functions cryptographic properties [11]. These include nonlinearity, the autocorrelation maximum, distribution criterion and others. However, as shown in [6], many of this group's criteria are not essential or redundant.

Thus, the following criteria are considered to be essential [6].

2.1. The maximum value of difference distribution table

The value of this criterion is defined as

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

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

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

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

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

According to this definition, the optimal characteristics of resistance of the transformation F against differential attacks are associated with low values of δ-uniformity. Obviously, 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 high strength of cryptographic transformation it is necessary to obtain low values of δ-uniformity.

2.2. The maximum absolute value of linear approximation table

The value of this criterion is defined as

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

where

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

and $\mu[s]$ – bit s of value μ.

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

A large part of the known methods for the evaluation of block cipher's strength to differential and linear cryptanalysis is 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.

2.3. The minimum degree of S-box Boolean function

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

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

where g_j is a set of all linear combinations of f_i, $\deg(g_j)$ is the maximum degree of the ANF representation of the Boolean function.

2.4. Algebraic immunity

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

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

$$r = N_c - \mathrm{Rank}(A),$$

where

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

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

Dimensionality of such matrix is

$$|A| = 2^n \cdot N_c.$$

2.5. Absence of fixed points

According to this criterion, the substitution S shall not map some x to itself, i.e., $S(x) \neq x$ for all x.

In most ciphers, this criterion is used for the protection against statistical attacks.

2.6. Nonlinearity

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

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

where $NL(g_j)$ is the 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 by the maximum of linear approximation table [15] and for a substitution S of degree 2^n is equal to

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

3. Optimal S-boxes generation

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

Table 1 shows the properties of randomly generated substitutions of degree $n = 2^8$. The sample in the given experiment contained 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] random substitutions with nonlinearity 100 were obtained, but on the cluster of 4096 computers.

TABLE 1. Cryptographic properties of randomly generated S-boxes.

#	Criterion	Value	Percent of substitutions satisfying the criterion
1	The maximum value of the difference distribution table	8	0.004
2	The maximum of linear approximation table (nonlinearity)	32 (96)	11
3		30 (98)	0.15
4		28 (100)	0
5	The minimum degree of S-box Boolean function	7	30
6	Algebraic immunity	3	100

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

Among the algebraic methods of S-boxes generation the power operations in the finite field [16] are widely used. 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 an unwanted property: the value of their algebraic immunity is only two, which creates a 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:
   (a) generation of permutation S based on vector Boolean functions that implements power transformation in the finite field;
   (b) 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 heuristic methods of S-boxes generation and allows to obtain 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 to obtain 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 and performance of his method.

We note that the block cipher K a l y n a [20] and the hash function K u p y n a [21] presented in the corresponding new Ukrainian standards use S-boxes with (currently) best known cryptographic characteristics (given in the Table 2).

TABLE 2. Cryptographic characteristics of substitutions from the Kalyna and Kupyna.

#	Characteristic	Value
1	The maximum of difference distribution table	8
2	The maximum of linear approximation table	24
3	The minimum degree of S-box Boolean function	7
4	Nonlinearity	104
5	Algebraic immunity	3
6	Absence of fixed points	Yes

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 the usage on a single PC.

4. Optimization of S-boxes generation method

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

- a 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, it is proposed to use $F(x) = x^d$. The following formula [15] is used to obtain the possible values of degree d:

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

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

TABLE 3. List of the vectorial Boolean functions permitted for utilization.

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

The 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 the destruction of the cyclic structure:

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

The main portion of computational resources is spent at the second stage of the search for S-boxes—checking substitutions for compliance with 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 criteria application can substantially reduce the search time for an S-box. Let us consider the principle of finding the optimal order of criteria application.

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

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

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

where $\theta_i(\sigma) \in [0; k)$ is a function that sets the criterion for the ith position in combination F_σ.

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

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

The combination of the criteria F_σ corresponding to the value $t_{\min}$, is the optimal one.

Now let us define an analytic expression for finding the values of the function $T(F_\sigma)$. The following factors influence the time of a substitution check:

- p_i is the probability that the substitution satisfies the ith criterion;
- v_i is the time needed to check whether the substitution complies with ith criterion.

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

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

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

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

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 us to get the optimal criteria sequence application for the S-boxes generation.

5. Practical results

Practical results presented below were obtained on the PC with the following characteristics:

- Intel(R) Core(TM) i3 CPU 2.53 GHz;
- 4 GB RAM.

5.1. 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 difference distribution table $a = 8$;
- the maximum of linear approximation table $b = 26$;
- the minimum degree of S-box Boolean function $c = 7$;
- algebraic immunity $d = 3$.

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

Table 4 shows the experimentally obtained values of the factors p and v. To obtain the value p for each criterion 1,000,000 substitutions were generated, and the ratio of S-boxes satisfying criterion to the total number of substitutions was found. To obtain the value v for each criterion 1,000,000 substitutions were generated and the average time of S-box verification of compliance with the criterion was measured.

TABLE 4. The values of factors for four criteria.

#	Criterion	Factor p	Factor v, sec
1	a	0.66	0.0003
2	b	0.1	0.0017
3	c	0.3	0.0018
4	d	0.6	0.0067

According to the formula, the values of function $T(F_\sigma)$ for combinations of criteria $F_\sigma \in [0; 24)$ were calculated. These values are shown in the Table 5. The value $t_{\min} = 0.0016735$ is obtained for the combination of criteria $d \circ c \circ b \circ a$.

Values presented in Table 5 are the time needed to check a single substitution. Experiments have shown that to generate one S-box satisfying four criteria 102 substitutions must be checked on average (to obtain this value a sample of 10,000 S-boxes that satisfy all four criteria was generated). Thus, the time for the generation of the substitution can be calculated as $T_{\text{theor}}(F_\sigma) = T(F_\sigma) \cdot 102$.

Fig. 1 shows graphs of functions $T_{\text{theor}}(F_\sigma)$ (continuous curve) and $T_{\exp}(F_\sigma)$ (dotted curve).

S-box generation method presented in [7] does not take into account the order of the application of the criteria. Our optimization allows us to decrease S-box generation time almost up to 5 times (considering the ratio of the worst time to the best time) for S-boxes with 8-uniformity, nonlinearity 102, algebraic immunity 3 and minimal degree 7.

TABLE 5. 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

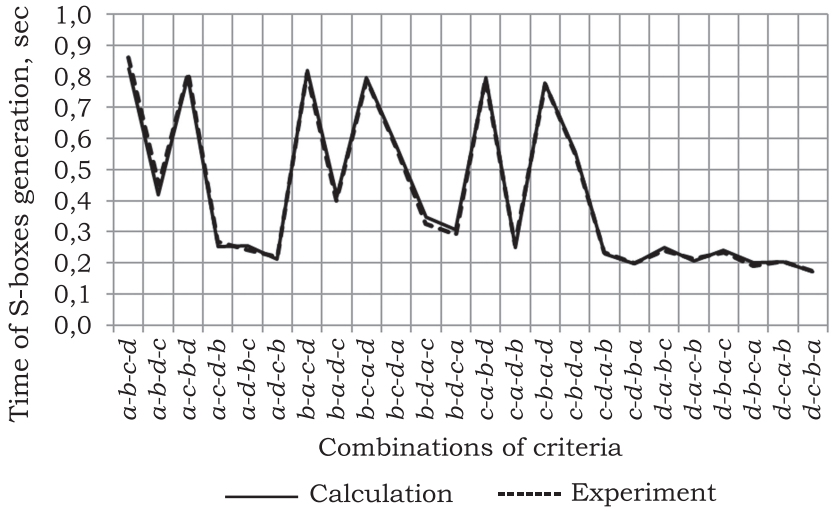

FIGURE 1. Graphs of functions $T_{\text{theor}}(F_\sigma)$ and $T_{\exp}(F_\sigma)$.

5.2. Generation of highly nonlinear S-boxes

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

- the maximum of difference distribution table $a = 8$;
- the maximum of linear approximation table $b = 24$ (compared with the previous case the nonlinearity was increased to 104);
- the minimum degree of S-box Boolean function $c = 7$;
- algebraic immunity $d = 3$;
- the absence of short cycles (cycle length ≤ 3).

Experiments have shown that the probability of the event when the substitution has a equal to nonlinearity 104 is 0.0000007.

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

The minimum value $t_{\min} = 0.001422$ is reached when the combinations of criteria are $d \circ c \circ b \circ a$ and $c \circ d \circ b \circ a$.

To generate an optimal S-box that also satisfies the criterion of fixed points absence, it is necessary to check 1,100,000 substitutions on average (based on the experiment where 50 optimal S-boxes were generated). Thus, the average generation time of one optimal S-box equals to $t_{\min} \cdot 1,100,000 = 0.0013275 \cdot 1,100,000 = 1564.2$ seconds ≈ 26 minutes (versus 2.5 hours in the worst criteria application sequence). The experimental results of the generation time of an optimal substitution confirms the analytically obtained value.

Examples of the obtained optimal S-boxes are presented in Appendix A.

6. Conclusions

Our paper proposes the optimization of the known method of S-box generation, based on minimizing the time needed to check the compliance of generated S-box with the set of criteria. The presented approach allows to determine the order of the application of the selection criteria in which the checking time is minimal.

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

REFERENCES

[1] MENEZES, A. J.—SCOTT, A. V.—VAN OORSCHOT, P. C.: *Handbook of Applied Cryptography*. CRC Press, Inc., Boca Raton, FL, USA, 1996.

[2] GORBENKO, I. D.: *Applied Cryptology. Theory. Practice. Application: Monograph*. Kharkiv National University of Radioelectronics, JSC Institute of Information Technologies, Kharkiv, 2012. (In Ukrainian)

[3] SHANNON, C. E.: *Communication Theory of Secrecy Systems*. Bell Syst. Tech. J. **28** (1949), 656–715.

[4] SOROKA, L. S.—KUZNETSOV, O. O.—MOSKOVCHENKO, I. V.—ISAYEV S. A.: *The research of differential properties of block symmetric,* Inform. Process. Syst. **6** (2010), 286–294. (In Russian)

[5] OLIYNYKOV, R.—KAZYMYROV, O.: *An impact of S-box Boolean function properties to strength of modern symmetric block ciphers,* Radio Engineering **166** (2011), 11–17.

[6] KAZYMYROV, O. V.: *Methods and Techniques of Generation of Nonlinear Substitutions for Symmetric Encryption Algorithms*. 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.—KAZYMYROVA, V.—OLIYNYKOV, R.: *A method for generation of high-nonlinear S-boxes based on gradient descent,* IACR Cryptology ePrint Archive, 2013, 578–578.

[8] BIHAM, E.—SHAMIR, A.: *Differential cryptanalysis of DES-like cryptosystem*, J. Cryptology **4** (1991), 3–72.

[9] MATSUI, M.: *Linear cryptoanalysis method for DES cipher*. In: Adv. in Cryptology––EUROCRYPT '93, (T. Helleseth, ed.), Lofthus, Norway, 1993, Lecture Notes in Comput. Sci., Vol. 765, Springer, Berlin, 1994, pp. 386–397.

[10] COURTOIS, N. T.—PIEPRZYK, J.: *Cryptanalysis of block ciphers with overdefined systems of equations*. In: Proc. of the 8th Internat. Conf. on the Theory and Appl. of Cryptology and Inform. Security—ASIACRYPT '02, Queenstown, New Zealand, 2002, Lecture Notes in Comput. Sci., Vol. 2501, Springer, Berlin, 2002, pp. 267–287.

[11] CRAMA, Y.—HAMMER, P. L.: *Boolean Models and Methods in Mathematics, Computer Science and Engineering*. In: Encyclopedia Math. Appl., Vol. 2, Cambridge University Press, 2010.

[12] NYBERG, K.: *Differentially uniform mapping for cryptography*. In: Adv. in Cryptology––EUROCRYPT '93, (T. Helleseth, ed.), Lofthus, Norway, 1993, Lecture Notes in Comput. Sci., Vol. 765, Springer, Berlin, 1994, pp. 55–64.

[13] NYBERG, K.: *Linear approximation of block ciphers*. In: Adv. in Cryptology–EUROCRYPT '94 (A. De Santis, ed.), Perugia, Italy, 1994, Lecture Notes in Comput. Sci., Vol. 950, Springer, Berlin, 1995, pp. 439–444.

[14] HONG, S.—LEE, S.—LIM, J.—SUNG, J.—CHEON, D.—CHO, I.: *Provable security against differential and linear cryptanalysis for SPN structure*. In: Proc. of the 7th Internat. Workshop—FSE '00 (B. Schneier, ed.), New York, NY, USA, 2000, Lecture Notes in Comput. Sci., Vol. 1978, Springer, Berlin, 2001, pp. 273–283.

[15] CARLET, C.: *Vectorial Boolean functions for cryptography*. In: Boolean Models and Methods in Mathematics, Computer Science, and Engineering (Y. Crama and P. Hammer, eds.), Cambridge University Press, Cambridge, 2010, pp. 39–469.

[16] NYBERG, K.: *Perfect nonlinear S-boxes*. In: Proc. of the Workshop on the Theory and Application of Cryptographic Techniques—EUROCRYPT '91, Brighton, UK, 1991, Lecture Notes in Comput. Sci., Vol. 547, Springer, Berlin, 1991, pp. 378–386.

[17] KAZYMYROV, O. V.—OLIYNYKOV, R. V.: *Vectorial Boolean functions application in substitutions generation for symmetric cryptographic transformation*, Inform. Process. Syst. **6** (2012), 97–102. (In Russian)

[18] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST): *Advanced Encryption Standard (AES)*. Federal Information Processing Standards (FIPS) Publication 197, Nov. 2001.

[19] TESAR, P.: *A new method for generating high non-linearity Sboxes*, Radioengineering **19** (2010), 23–26.

[20] OLIYNYKOV, R. ET ALL.: *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) Block cipher description is available in Englist at `http://eprint.iacr.org/2015/650.pdf`

[21] OLIYNYKOV, R. ET ALL.: *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 (hexadecimal notation)

The optimal S-box based on the vectorial Boolean function x^{254}.

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

The optimal S-box based on the vectorial Boolean function x^{191}.

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

Received July 30, 2015

Mariia Rodinko
V. N. Karazin Kharkiv National University
Kharkiv
UKRAÏNE
E-mail: m.rodinko@gmail.com

Roman Oliynykov
V. N. Karazin Kharkiv National University
Kharkiv
UKRAÏNE

JSC Institute of Information Technologies
Kharkiv
UKRAÏNE
E-mail: roliynykov@gmail.com

Yurii Gorbenko
JSC Institute of Information Technologies
Kharkiv
UKRAÏNE
E-mail: gorbenkou@iit.kharkov.ua