Spectral-linear and spectral-differential methods for generating S-boxes having almost optimal cryptographic parameters

A.V. Menyachikhin

TVP Laboratories, Moscow
email: and88@list.ru

Abstract. S-boxes are important parts of modern ciphers. To construct S-boxes having cryptographic parameters close to optimal is an unsolved problem at present time. In this paper some new methods for generating such S-boxes are introduced.

Keywords: S-box, substitution, involutory substitution, spectral-linear method, spectral-differential method, Kuznechik, BelT, Skipjack, Khazad-0, Khazad, Anubis

1 Introduction

All modern block and stream ciphers have one or more nonlinear elements. S-box is one of the most used nonlinear cornerstones of modern ciphers.

The problems of S-boxes design with strong properties were considered in many papers (for example [1-6, 8, 9, 11-19, 22, 26-28, 30-42, 45-48]).

Cryptographic properties deal with the application of attacks on ciphers. The basic cryptographic properties are: linear and differential properties, nonlinearity degree, the minimum degree of polynomial relations between components of input and output vectors.

In this paper we introduce new methods for generating S-boxes. These methods involve a process of iterative improvements of given pseudo-random S-boxes. We also introduce two algorithms implementing these methods. By means of these algorithms we construct many new substitutions with stronger properties than was known previously.

This paper is organized as follows. In Section 2 we give necessary definitions. In Section 3 we describe the known methods of constructing S-boxes and empirical distribution of cryptographic properties of random substitutions. We present spectral-linear and spectral-differential methods in Section 4. Section 5 contains new substitutions with stronger properties. We summarize the results in Section 6.

2 Our definitions

Let $V_n(2) = V_n$ be n-dimensional vector space over the field $GF(2)$. Suppose that $V_n^{\times} = V_n \setminus \{0\}$. Let $S(V_n)$ be the symmetric group on set of 2^n elements. The cardinality of a set A is usually denoted $|A|$.

Definition 1. The p_g-parameter of an S-box g is defined as

$$p_g = \max_{\alpha,\beta \in V_n^{\times}} p^g_{\alpha,\beta},$$

where

$$p^g_{\alpha,\beta} = 2^{-n} \cdot |\{x \in V_n \,|g(x \oplus \alpha) \oplus g(x) = \beta\}|.$$

The *nonlinear order* of f, denoted by $\deg(f)$, is the maximum order of terms appeared in its algebraic normal form. A linear Boolean function is a Boolean function of nonlinear order 1, i.e. its algebraic normal form involves only isolated arguments. Given $\alpha \in V_n$, we denote by $l_\alpha : V_n \to V_1$ the linear Boolean function equal to the sum of bits of argument selected by bits of α:

$$l_\alpha(x) = \bigoplus_{i=0}^{n-1} \alpha_i \cdot x_i.$$

The *correlation* $c(f_1, f_2)$ between two Boolean function f_1 and f_2 is defined as

$$c(f_1, f_2) = 2^{1-n} \cdot |\{x \,|f_1(x) = f_2(x)\}| - 1.$$

The extreme value of the correlation between linear functions of input bits and linear functions of output bits of g is called the *bias* of g.

Definition 2. The δ_g-parameter of an S-box g is defined as the absolute value of the bias:

$$\delta_g = \max_{\alpha,\beta \in V_n^{\times}} \delta^g_{\alpha,\beta},$$

where

$$\delta^g_{\alpha,\beta} = |c(l_\alpha, l_\beta \circ g)|.$$

Definition 3. The nonlinear order of an S-box g, denoted by λ_g, is the minimum nonlinear order over all linear combinations of the components of g:

$$\lambda_g = \min_{\alpha \in V_n^{\times}} \{\deg(l_\alpha \circ g(x))\}.$$

The *generalized nonlinear order* of S-boxes g and g^{-1}, denoted by $\overline{\lambda_g}$, is the minimum of the nonlinear orders of g and g^{-1}:

$$\overline{\lambda_g} = \min\left\{\lambda_g, \lambda_{g^{-1}}\right\}.$$

Some S-boxes may be described by the system of polynomial equations.

Definition 4. For $i > 0$ the $r_g^{(i)}$-parameter of an S-box g is defined as

$$r_g^{(i)} = \dim H_g^{(i)},$$

where

$$H_g^{(i)} = \left\{ h \in GF(2)[z_1, ..., z_{2n}] \;\middle|\; \begin{array}{c} \forall x \in V_n, h(x, g(x)) = 0, \\ 0 < \deg h \leq i \end{array} \right\}.$$

Definition 5. The r_g-parameter of an S-box g is defined as

$$r_g = \min \left\{ i \,\middle|\, r_g^{(i)} > 0 \right\}$$

Remark 1. For substitution $g \in S(V_8)$ we have $r_g \leq 3$.

The *Difference Distribution Table* (DDT) of an S-box g is a $2^n \times 2^n$ matrix T_1, where

$$T_1[\alpha, \beta] = |\{x \in V_n \,|g(x \oplus \alpha) \oplus g(x) = \beta\}|.$$

The *Linear Approximation Table* (LAT) of an S-box g is a $2^n \times 2^n$ matrix T_2, where

$$T_2[\alpha, \beta] = |\{x \in V_n \,|\alpha \circ x = \beta \circ g(x)\}| - 2^{n-1}.$$

The distribution of the coefficients in both the DDT and the LAT is the most important parameter of our methods. According to [26] we define the linear and the differential spectra of permutation g.

For $g \in S(V_n)$ and for elements $p \in P_{n-1}$ and $\delta \in P_{n-2}$,

$$P_j = \left\{ \frac{i}{2^j} \,\middle|\, i = 0, 1, ..., 2^j \right\}, \quad |P_j| = 2^j + 1, j \in \{n-2, n-1\}$$

we define the sets

$$D(g, p) = \left\{ (\alpha, \beta) \in V_n^{\times} \times V_n \,\middle|\, p_{\alpha,\beta}^g = p \right\};$$
$$L(g, \delta) = \left\{ (\alpha, \beta) \in V_n \times V_n^{\times} \,\middle|\, \delta_{\alpha,\beta}^g = \delta \right\}.$$

Definition 6. The *differential spectrum* of an S-box g is defined as

$$D(g) = \{(p, \; |D(g, p)|) \,|p \in P_{n-1}\}, \quad |D(g)| = 2^{n-1} + 1.$$

Definition 7. The *linear spectrum* of an S-box g is defined as

$$L(g) = \{(\delta, |L(g, \delta)|) \,|\delta \in P_{n-2}\}, \quad |L(g)| = 2^{n-2} + 1.$$

3 Basic approaches to the construction of S-boxes and distribution of cryptographic parameters of random substitutions

3.1 Known approaches to the construction of S-boxes

The available techniques for S-box generation may be divided into three main classes: explicit algebraic constructions, pseudo-random generation and heuristic techniques.

The first approach is based on some known algebraic constructions (for example, exponential [1, 23, 37], logarithmic [42], piecewise linear [8, 47] or polynomial [48] substitution boxes) and their affine transformation. This is the most popular approach, because S-boxes from the known classes are often optimized for all the desired criteria.

The second approach uses heuristic techniques involving the hill climbing method, the simulated annealing method, the genetic algorithm or a combination of these [19, 22, 24, 30].

The third approach uses some pseudo-random generation [25] to construct the entries in the S-box and then test whether the S-box is good or not. This approach takes a great effort to find a good S-box because of the small number of good S-boxes among all in the whole space.

There are also some other approaches for the construction of S-box [2, 34].

3.2 Empirical distribution of cryptographic properties of random substitutions

Empirical distribution is considered in many papers (see for example, [3, 4, 9, 13]). This subsection includes empirical results of cryptographic properties. We have generated pseudo-random substitutions using "Mersenne twister" [29] and "Present-80" algorithm of block cipher [10].

Table 1 and Table 2 (see Appendix) present joint empirical distribution of basic cryptographic properties constructed by means of large number of pseudo-random substitutions ($n = 10^{10}$). All pseudo-random substitutions generated don't have quadratic equation.

Table 3 and Table 4 (see Appendix) present joint empirical distribution of basic cryptographic properties constructed by means of large number of pseudo-random involutory substitutions without fixed points ($n = 10^{10}$) All pseudo-random involutory substitutions generated don't have quadratic equation.

4 New methods

New proposed methods are based on using linear $L(g_i)$ and differential $D(g_i)$ spectra to improve iteratively given S-box with respect to all properties. We multiply given S-box on some special permutations.

Algorithms implementing these methods operate with the following objects:

$$(a, b, c, d, e) \in S(V_n) \times \mathbb{Q} \times \mathbb{Z} \times \mathbb{Q} \times V_n^k.$$

On the set of these objects we have an order relation

$$(a', b', c', d', e') \leq (a, b, c, d, e), \text{ if} \begin{cases} b' < b,\ d' \leq d \text{ or} \\ b' = b,\ c' \leq c,\ d' \leq d \end{cases} \tag{1}$$

4.1 The algorithm implementing a spectral-differential method of S-boxes generation

Let $w_1 \in \mathbb{N}$ be the size of list I.

Algorithm 1.

Input: substitution $g_0 \in S(V_n)$, parameter $w_1 \in \mathbb{N}$.

Step 1. For substitution g_0 calculate values

$$p_{g_0}, D(g_0), \delta_{g_0}, X_{g_0},$$

where $X_{g_0} = \{x \in V_n \,|g_0(x+\alpha) + g_0(x) = \beta,\ \exists\,(\alpha, \beta) \in D(g_0, p_{g_0})\}$.

Initialize list I:

$$I = \{(g_0, p_{g_0}, |D(g_0, p_{g_0})|, \delta_{g_0}, X_{g_0})\}, \quad |I| = 1.$$

Step 2. Using the list

$$I = \{(g_i, p_{g_i}, |D(g_i, p_{g_i})|, \delta_{g_i}, X_{g_i}),\ i = 0, ..., |I| - 1\}$$

construct the new list

$$I' = \left\{\left(g'_{i,j}, p_{g'_{i,j}}, \left|D\left(g'_{i,j}, p_{g'_{i,j}}\right)\right|, \delta_{g'_{i,j}}, X_{g'_{i,j}}\right)\right\},$$

$$|I'| \leq \sum_{i=0}^{|I|-1} \frac{|X_{g_i}| \cdot (|X_{g_i}| - 1)}{2}.$$

Substitutions $g'_{i,j}$ are elements of list I', and $g'_{i,j}$ is equal to substitution g_i multiplied by transpositions from the set X_{g_i} with special properties:

$$g'_{i,j} = (x, x') \cdot g_i,$$

where $x, x' \in X_{g_i}$, $x \le x'$, $i = 0, ..., |I| - 1$, $j = j(x, x')$ is an injective mapping,

$$p_{g'_{i,j}} \le p_{g_i}, \quad \delta_{g'_{i,j}} \le \delta_{g_i},$$

and $\left|D\left(g'_{i,j}, p_{g'_{i,j}}\right)\right| < \left|D\left(g_i, p_{g_i}\right)\right|$ if $p_{g'_{i,j}} = p_{g_i}$.

Step 3.

3.1. Remove repetitions from the list I'.

3.2. Calculate the size $|I'|$ of list I'.

3.3. Sort the elements of list I' in the ascending order according to the order relation (1).

3.4. Numerate the sorted list elements by indexes $i = 0, \ldots, |I'| - 1$.

3.5. Calculate values

$$m_1 = \min\{|I|-1, |I'|-1\} \text{ and } m_2 = \min\{w_1 - 1, |I'|-1\}.$$

Step 4. Compare the first elements of list I' and list I:

– If $\sum_{i=0}^{m_1} p_{g'_i} < \sum_{i=0}^{m_1} p_{g_i}$

or

$\sum_{i=0}^{m_1} p_{g'_i} = \sum_{i=0}^{m_1} p_{g_i}$ and $\sum_{i=0}^{m_1} \left|D\left(g'_i, p_{g'_i}\right)\right| < \sum_{i=0}^{m_1} |D\left(g_i, p_{g_i}\right)|$,

then

4.1 Clean list I.

4.2 Copy elements from list I' with indexes $i = 0, ..., m_2$ to list I.

4.3 Assign $|I| = m_2 + 1$.

4.4 Go to Step 2.

– Otherwise, the algorithm stops.

Output: the list

$$I' = \left\{\left(g_i, p_{g_i}, |D\left(g_i, p_{g_i}\right)|, \delta_{g_i}, X_{g_i}\right),\ i = 0, ..., |I'| - 1\right\}, |I'| \le w_1.$$

Let us denote by t_1 the computational complexity of algorithm 1.

Proposition 1. *For $n \to \infty$ we have*

$$t_1 = O\left(n^2 \cdot 2^{6n-1}\right).$$

Proof. We divide the proof in two stages. In the first stage we compute the maximum number of iterations of step 2 of the algorithm. In the second stage we find the complexity of step 2.

1. Let $g \in S(V_n)$. For elements of a differential spectrum $D(g)$ we have

$$|D(g, p)| \le (2^n - 1) \cdot \frac{1}{p}, \quad p \in P_{n-1} \setminus \{0\}.$$

Thus, we obtain the following expressions:

$$\sum_{p\in P_{n-1}\setminus\{0\}}(2^n-1)\cdot\frac{1}{p}=(2^n-1)\cdot\sum_{p\in P_{n-1}\setminus\{0\}}\frac{1}{p}=$$

$$=(2^n-1)\cdot\sum_{i=1}^{2^{n-1}}\frac{2^{n-1}}{i}=(2^n-1)\cdot 2^{n-1}\cdot\sum_{i=1}^{2^{n-1}}\frac{1}{i}\leq$$

$$\leq(2^n-1)\cdot 2^{n-1}\cdot\left(\ln 2^{n-1}+1\right)\leq(2^n-1)\cdot 2^{n-1}\cdot\left(\log_2 2^{n-1}+1\right)=$$

$$=n\cdot 2^{n-1}\cdot(2^n-1).$$

2. The estimate of the complexity of step 2 is the product of the following values:

   (a) the parameter w_1,

   (b) the estimate of the number of all transpositions from the set X_{g_i}

   $$C^2_{|X_{g_i}|}\leq C^2_{|V_n|}=\frac{2^n\cdot(2^n-1)}{2},$$

   (c) the complexity of computing δ_{g_i}-parameter, which is equal to

   $$c\cdot 2^{2n}\cdot n, where\ c=const.$$

The computation of other parameters is not so difficult as just described. Thus, the complexity of step 2 is smaller than

$$w_1\cdot 2\cdot\frac{2^n\cdot(2^n-1)}{2}\cdot c\cdot 2^{2n}\cdot n.$$

Finally, for the total complexity of the algorithm we have

$$t_1\leq w_1\cdot c\cdot n^2\cdot\left(2^{6n-1}-2^{5n}+2^{4n-1}\right)\leq w_1\cdot c\cdot n^2\cdot 2^{6n-1}.$$

The proposition is proved. □

4.2 The algorithm implementing a spectral-linear method of S-boxes construction

Let $w_2\in\mathbb{N}$ be the size of list I.

Algorithm 2.

Input: substitution g_0, parameter w_2.

Step 1. For substitution g_0 calculate values

$$\delta_{g_0}, L(g_0), p_{g_0}, Y_{g_0},$$

where $Y_{g_0} = \{y \in V_n \,|y \circ \alpha = g_0\,(y) \circ \beta;\ \exists\,(\alpha,\beta) \in L\,(g_0, \delta_{g_0})\,\}$.

Initialize list I:

$$I = \{(g_0, \delta_{g_0}, |L\,(g_0, \delta_{g_0})|\,, p_{g_0}, Y_{g_0})\}\,, |I| = 1.$$

Step 2. Using the list

$$I = \{(g_i, \delta_{g_i}, |L\,(g_i, \delta_{g_i})|\,, p_{g_i}, Y_{g_i})\,,\ i = 0, ..., |I| - 1\}$$

construct the new list

$$I' = \left\{\left(g'_{i,j}, \delta_{g'_{i,j}}, \left|L\left(g'_{i,j}, \delta_{g'_{i,j}}\right)\right|, p_{g'_{i,j}}, Y_{g'_{i,j}}\right)\right\},$$

$$|I'| \leq \sum_{i=0}^{|I|-1} \frac{|Y_{g_i}|\,(|Y_{g_i}| - 1)}{2}.$$

Substitutions $g'_{i,j}$ are elements of list I', and $g'_{i,j}$ is equal to substitution g_i multiplied by transpositions from the set Y_{g_i} with special properties:

$$g'_{i,j} = (y, y') \cdot g_i,$$

where $y, y' \in Y_{g_i}$, $y \leq y'$, $i = 0, ..., |I| - 1$, $j = j\,(y, y')$ is injective mapping,

$$\delta_{g'_{i,j}} \leq \delta_{g_i}, \quad p_{g'_{i,j}} \leq p_{g_i},$$

and $\left|L\big(g'_{i,j}, p_{g'_{i,j}}\big)\right| < \left|L\big(g_i, p_{g_i}\big)\right|$ if $\delta_{g'_{i,j}} = \delta_{g_i}$.

Step 3.

3.1. Remove repetitions from the list I'.

3.2. Calculate the size $|I'|$ of list I'.

3.3. Sort the elements of list I' in the ascending order according to the order relation (1).

3.4. Numerate the sorted list elements by indexes $i = 0, \ldots, |I'| - 1$.

3.5. Calculate values

$$m_1 = \min\{|I| - 1, |I'| - 1\} \text{ and } m_2 = \min\{w_2 - 1, |I'| - 1\}.$$

Step 4. Compare the first elements of list I' and list I:

– If $\sum_{i=0}^{m_1} \delta_{g'_i} < \sum_{i=0}^{m_1} \delta_{g_i}$

or

$\sum_{i=0}^{m_1} \delta_{g'_i} = \sum_{i=0}^{m_1} \delta_{g_i}$ and $\sum_{i=0}^{m_1} \left|L\left(g'_i, \delta_{g'_i}\right)\right| < \sum_{i=0}^{m_1} |L\,(g_i, \delta_{g_i})|$,

then

4.1. Clean list I.

4.2. Copy elements from list I' with indexes $i = 0, ..., m_2$ to list I.

4.3. Assign $|I| = m_2 + 1$.

4.4. Go to Step 2.

– Otherwise, the algorithm stops.

Output: the list

$$I' = \{(g_i, \delta_{g_i}, |L(g_i, \delta_{g_i})|, p_{g_i}, Y_{g_i}),\ i = 0, ..., |I'| - 1\}.$$

Let us denote by t_2 the computational complexity of algorithm 2.

Proposition 2. *For $n \to \infty$ we have*

$$t_2 = O\left(n \cdot 2^{7n-4}\right).$$

Proof. We divide the proof in two stages. In the first stage we compute the maximum number of iterations of step 2 of the algorithm. On the second stage we find the complexity of step 2 .

1. Let $g \in S(V_n)$. For elements of a linear spectrum $L(g)$ we have

$$|L(g, \delta)| \leq (2^n - 1) \cdot \frac{1}{\delta^2}, \quad \delta \in P_{n-2} \setminus \{0\}.$$

Thus, we obtain the following expressions:

$$\sum_{\delta \in P_{n-2} \setminus \{0\}} (2^n - 1) \cdot \frac{1}{\delta^2} = (2^n - 1) \cdot \sum_{\delta \in P_{n-2} \setminus \{0\}} \frac{1}{\delta^2} =$$

$$= (2^n - 1) \cdot \sum_{i=1}^{2^{n-2}} \frac{2^{2n-4}}{i^2} = (2^n - 1) \cdot 2^{2n-4} \cdot \sum_{i=1}^{2^{n-2}} \frac{1}{i^2} \leq (2^n - 1) \cdot 2^{2n-4} \cdot \frac{\pi^2}{6}.$$

2. The complexity of step 2 is the product of the following values:

   (a) the parameter w_2,

   (b) the estimate of the number of all transpositions from the set Y_{g_i}

$$C^2_{|Y_{g_i}|} \leq C^2_{|V_n|} = \frac{2^n \cdot (2^n - 1)}{2},$$

   (c) the complexity of computing δ_{g_i}-parameter, which is equal to

$$c \cdot 2^{2n} \cdot n, where\ c = const.$$

The computation of other parameters is not so difficult as just described. Thus, the complexity of step 2 is smaller than

$$w_2 \cdot 2 \cdot \frac{2^n \cdot (2^n - 1)}{2} \cdot c \cdot 2^{2n} \cdot n.$$

Finally, for the total complexity of the algorithm we have

$$t_2 \leq w_2 \cdot c \cdot \frac{\pi^2}{6} \cdot n \cdot \left(2^{7n-4} - 2^{6n-3} + 2^{5n-4}\right) \leq w_2 \cdot c \cdot \frac{\pi^2}{6} \cdot n \cdot 2^{7n-4}.$$

This completes the proof of Proposition 2. □

Remark 2. The parameters $w_1, w_2 \in \mathbb{N}$ should be chosen according to available computing resources (the number of processor cores).

Remark 3. The best results we have obtained by means of both our algorithms.

Remark 4. The set $Y_{g_i},\ i = 1, ..., |I|$, may be defined as $Y_{g_i} = V_n \backslash X_{g_i}$, where

$$X_{g_i} = \{x \in V_n \,|g_i\,(x + \alpha) + g_i\,(x) = \beta;\ \exists\,(\alpha, \beta) \in D\,(g_i, p_{g_i})\}\,.$$

5 Experimental results

Algorithms 1 and 2 have been applied to S-boxes, used in modern block ciphers. Some of the results are presented in this Section.

Table 6 (see Appendix) includes the original S-box of the national standards of the Russian Federation GOST R 34.11-2015 [20] and GOST R 34.12-2012 [21] and one of the new S-boxes that we have constructed starting from the original S-box using our algorithms. It is obvious that the new S-box is stronger.

Table 7 (see Appendix) includes the original S-box of the State standard of the Republic of Belarus «BelT» [2, 44] and one of the new S-boxes that we have constructed from the original S-box using our algorithms. This table shows that the new S-box has better properties.

Table 8 (see Appendix) includes the original S-box of block cipher «Skipjack» [7, 43] developed by the NSA of US and one of the new S-boxes that we have constructed from the original S-box using our algorithms. As it may be seen from the table our S-box again demonstrates better properties.

Construction of modern ciphers deals with software-hardware implementation. This is one of the reasons why involutions are used in cryptography. In fact they are the most popular constructions. We apply the new spectral-linear and spectral-differential

methods to generate involutive and efficiently-implemented S-boxes without fixed points using pairs of transposition $(x, x') \cdot (g(x), g(x'))$.

Table 9 (see Appendix) presents the original S-box of block cipher "Khazad-0" and one of the new involutive S-boxes that we have constructed from the original S-box using our algorithms.

Table 10 (see Appendix) presents the original S-box of block ciphers "Khazad" and "Anubis" [5, 6] and one of the new efficiently-implemented S-boxes that we have constructed from the original S-box using our algorithms.

Our methods have been applied to a large number of random substitutions $g \in S(V_8)$. As a result we have a lot of new affine nonequivalent substitutions $g' \in S(V_8)$ with the following cryptographic parameters

$$\delta_{g'} = {}^{24}\!/_{128},\ p_{g'} = {}^{6}\!/_{256},\ \overline{\lambda_{g'}} = 7,\ r_{g'} = 3,\ r_{g'}^{(3)} = 441.$$

Table 5 (see Appendix) presents the numbers of constructed substitutions with given values of parameters.

6 Conclusions

The results allow us to come to the following conclusions.

1. In this paper we present two universal methods. Nowadays these methods are the most efficient for generating S-boxes. Each substitution $g \in S(V_8)$ used in modern block ciphers, except $g(x) = x^{2^n-2}$ and affine equivalent to it [14], may be optimized by our methods.

2. Our methods allow to construct a lot of new affine nonequivalent S-boxes with strong cryptographic properties.

3. Algorithms 1 and 2 have acceptable complexity.

4. Algorithms 1 and 2 presented in this paper are deterministic.

5. A large number of substitutions $g' \in S(V_8)$, having the parameters

$$\delta_{g'} = {}^{24}\!/_{128},\ p_{g'} = {}^{6}\!/_{256},\ \overline{\lambda_{g'}} = 7,\ r_{g'} = 3,\ r_{g'}^{(3)} = 441$$

are the reality of nowadays.

Remark 5. The methods may be used for generate non-bijective substitutions.

The author is very thankful to B. A. Pogorelov and A. E. Trishin for helpful discussions on the subject and for useful comments.

Our methods are patented and protected by RU Patent №2633132. For licensing inquiries please email us at and88@list.ru.

References

[1] Agievich S.V., Afonenko A.A., "On the properties of exponential substitutions", *Vesti NAN Belarusi*, **1** (2005), 106–112 (in Russian).

[2] Agievich S.V., Galinsky B. A., Mikulich N.D., Kharin U.S., "Algorithm of block encryption BelT" (in Russian), http://apmi.bsu.by/assets/files/agievich/BelT.pdf.

[3] Alekseychuk A., Kovalchuk L., Pal'chenko S., "Cryptographic parameters of s-boxes that characterize the security of GOST-like block ciphers against linear and differential cryptanalysis", *Zakhist Inform.*, **2** (2007), 12–23 (in Ukrainian).

[4] Alekseychuk A., Kovalchuk L., "Upper bounds of maximum values of average differential and linear characteristic probabilities of Feistel cipher with adder modulo 2^m", *Theory of Stochastic Processes*, **12 (28)**:1–2 (2006), 20-32.

[5] Barreto P., Rijmen V., "The ANUBIS block cipher", NESSIE submission, 2000.

[6] Barreto P., Rijmen V., "The KHAZAD block cipher", NESSIE submission, 2000.

[7] Biham E., Biryukov A., Shamir A,, "Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials,", EUROCRYPT'99, Lect. Notes Comput. Sci., **1592**, 1999, 12–23.

[8] Bugrov A.D., "Piecewise affine substitution of finite fields", *Prikl. Diskr. Matem.*, **4(30)** (2015), 5–23 (in Russian).

[9] Blondeau C., Gerard B., "Links between theoretical and effective differential probabilities: experiments on PRESENT", In: ECRYPT II Workshop on Tools for Cryptanalysis, 2010, https://eprint.iacr.org/2010/261.pdf.

[10] Bogdanov A., Knudsen L.R., Leander G., Paar C., Poschmann A., Robshaw M.J.B., Seurin Y., and Vikkelsoe C., "PRESENT: An ultra-lightweight block cipher", CHES 2007, Lect. Notes Comput. Sci., **4727**, 2007, 450–466.

[11] Carlet C., Ding C., "Nonlinearities of S-boxes", *Finite Fields Appl.*, **13** (2007), 121-135.

[12] Chabaud F., Vaudenay S., "Links between differential and linear cryptanalysis", EUROCRYPT, Lect. Notes Comput. Sci., **950**, 1994, 356–365.

[13] Daemen J., Rijmen V., "Probability distributions of correlations and differentials in block ciphers", *J. Math. Crypt.*, **1** (2007), 221–242.

[14] Daemen J., Rijmen V., *The Design of Rinjdael: AES – The Advanced Encryption Standard*, Springer, 2002.

[15] Dygin D.M., Lavrikov I.V., Marshalko G.B., Rudsky V.I., Trifonov D.I., Shishkin V.A., "On a new Russian Encryption Standard", *Mathematical aspects of cryptography*, **6**:2 (2015), 29–34.

[16] Evans A., *Orthomorphism Graphs of Groups*, Lect. Notes Math., **1535**, Springer-Verlag, Berlin, 1992, 116 pp.

[17] Gluhov M.M., "On the matrices of transitions of differences when using some modular groups", *Mathematical aspects of cryptography*, **4**:4 (2013), 27–47 (in Russian).

[18] Gluhov M.M., "On a method of construction of orthogonal quasigroups systems by means of groups", *Mathematical aspects of cryptography*, **2**:4 (2011), 5–24 (in Russian).

[19] Goldberg D., *Genetic Algorithms in Search, Optimization and Machine Learning*, Addison-Wesley, Reading, 1985, 432 pp.

[20] *GOST R 34.12-2015. Information technology. Cryptographic protection of information. Block ciphers*, Standartinform, Moscow, 2015 (in Russian).

[21] *GOST R 34.11-2012. Information technology. Cryptographic protection of information. Hash function*, Standartinform, Moscow, 2012 (in Russian).

[22] Izbenko Y., Kovtun V., Kuznetsov A., "The design of Boolean functions by modified hill climbing method", TNG'09: Proc. Sixth Int. Conf. on Inf. Technol.: New Generations, *IEEE Computer Soc.*, 2009, 356–361.

[23] Jacobson Jr. M., Huber K., *The MAGENTA Block Cipher Algorithm*, NIST AES Proposal, 1998, http://edipermadi.files.wordpress.com/2008/09/magenta-spec.pdf.

[24] Kazymyrov O.V., Kazymyrova V.N., Oliynykov R.V., "A method for generation of high-nonlinear S-boxes based on gradient descent", *Mathematical aspects of cryptography*, **5**:2 (2014), 71–78.

[25] Knuth D., *Art of Computer Programming, Volume 2: Seminumerical Algorithms*, 3rd ed., Addison-Wesley Professional, 1997.

[26] Leander G., Poschmann A., "On the classification of 4-bit s-boxes", Lect. Notes Comput. Sci., **4547**, 2007, 159–176.

[27] Malyshev F.M., "Doubly transitive XSL-families of permutations", *Mathematical aspects of cryptography*, **1**:2 (2010), 93–103 (in Russian).

[28] Malyshev F.M., "The duality of difference and linear methods in cryptography", *Mathematical aspects of cryptography*, **5**:3 (2014), 35–47 (in Russian).

[29] Matsumoto M., Nishimura T., "Mersenne Twister: a 623-dimensionally equidistributed uniform pseudo-random generator", *ACM Trans. Modeling and Computer Simul. (TOMACS)*, **8**:1 (1998), 3–30.

[30] Millan W., Clark A., Dawson E., "Smart hill climbing finds better Boolean functions", Lect. Notes Comput. Sci., **1334**, 1997, 149–158.

[31] Millan W., "How to improve the nonlinearity of bijective S-boxes", Lect. Notes Comput. Sci., **1438**, 1998, 181–192.

[32] Nyberg K., "On the construction of highly nonlinear permutations", EUROCRYPT'92, Lect. Notes Comput. Sci., 1992, 92-98.

[33] Nyberg K., "Perfect nonlinear S-boxes", EUROCRYPT'91, Lect. Notes Comput. Sci., 1991, 378-386.

[34] Nyberg K., Knudsen L., "Provable security against differential cryptanalysis", *J. Cryptology*, **8**:1 (1992), 27-37.

[35] Pichkur A.B., "Description of the set of permutations represented as a product of two permutations with fixed number of mobile points", *Mathematical aspects of cryptography*, **3**:2, (2012), 79-95 (in Russian).

[36] Pichkur A.B., "Description of the set of permutations represented as a product of two permutations with fixed number of mobile points. II", *Mathematical aspects of cryptography*, **4**:1 (2013), 87-109 (in Russian).

[37] Pieprzyk J., "Non-linearity of exponent permutations", EUROCRYPT'89, Lect. Notes Comput. Sci., **434**, 1990, 81-92.

[38] Pogorelov B.A., "Substitution groups. Part 1 (the review over 1981-95)", Trudy po Diskretnoi Matematike, **2**, 1998, 237-281 (in Russian).

[39] Pogorelov B.A., Pudovkina M.A., "On the distance from permutations to the union of all imprimitive groups with identical parameters of imprimitivity systems", *Discrete Math. Appl.*, **24**:3 (2014), 163–173.

[40] Sachkov V.N., "Combinatorial properties of differentially 2-uniform substitutions", *Mathematical aspects of cryptography*, **6**:1 (2015), 159–179 (in Russian).

[41] Sachkov V.N., "Random mapping with fixed elements", *Mathematical aspects of cryptography*, **2**:2 (2011), 95-118 (in Russian).

[42] Shemyakina O.V., "On the estimation of the characteristics of partitions of various algebraic structures", Inf. security of Russian regions (ISRR-2011) (St-Pb.: SPOISU), 2011, 137 (in Russian).

[43] *Skipjack and KEA Algorithm Specifications, Version 2.0.*, 1998, http://csrc.nist.gov/encryption/skipjack-kea/htm.

[44] *STB 34.101.31-2011. Information technologies. Information security. Cryptographic algorithms of enciphering and continuity test*, Gosstandart, Minsk, 2011 (in Russian).

[45] Tokareva N.N., "Quadratic approximations of the special type for the 4-bit permutations in S-boxes", *Prikl. Diskr. Matem.*, **1** (2008), 50–54 (in Russian).

[46] Tokareva N.N., "On quadratic approximations in block ciphers", *Probl. Inf. Transmiss.*, **44**:3 (2008), 266–286.

[47] Trishin A.E., "The nonlinearity index for a piecewise-linear substitution of the additive group of the field", *Prikl. Diskr. Matem.*, **4(30)** (2015), 32–42 (in Russian).

[48] Trishin A.E., "The method of constructing orthogonal Latin squares on the basis of substitution binomials of finite fields", *Obozr. prikl. i prom. matem.*, **15**:4 (2008), 764–765 (in Russian).

Appendix

Table 1. The joint distribution of parameters p_g and δ_g
for large number ($n = 10^{10}$) of random substitutions

δ_g \ p_g	$\frac{8}{256}$	$\frac{10}{256}$	$\frac{12}{256}$	$\frac{14}{256}$	$\frac{16}{256}$	$\frac{18}{256}$	$\frac{20}{256}$	$\frac{22}{256}$	$\frac{24}{256}$	$\frac{26}{256}$
28/128	0	87	71	5	0	0	0	0	0	0
30/128	1540	7493651	7280003	664650	37389	1796	76	1	0	0
32/128	51188	477406097	560256566	57285935	3499466	182943	8460	357	16	0
34/128	112385	1562941349	2052055232	224393364	14348696	787832	39093	1780	67	2
36/128	66444	1215660385	1718774425	196521916	12947800	733502	36999	1612	79	2
38/128	22649	493419401	732222169	86210160	5784645	334687	17574	842	36	1
40/128	6099	151993952	234104868	28171461	1915341	112199	5977	279	14	1
42/128	1408	40873385	65184317	8004338	550334	32381	1671	84	4	1
44/128	303	10030340	16604441	2079231	144388	8597	450	30	1	0
46/128	64	2275760	3925207	504185	35402	2204	121	7	0	0
48/128	9	477750	862912	113575	8193	515	36	1	0	0
50/128	2	92970	177265	23889	1716	116	5	0	0	0
52/128	0	16563	33479	4797	361	20	1	0	0	0
54/128	0	2816	6005	889	62	4	0	0	0	0
56/128	0	447	932	131	12	0	0	0	0	0
58/128	0	54	145	18	1	0	0	0	0	0
60/128	0	7	23	5	0	0	0	0	0	0
62/128	0	2	1	0	0	0	0	0	0	0
64/128	0	0	1	0	0	0	0	0	0	0

Table 2. Empirical distribution of parameter $\overline{\lambda_g}$
for large number ($n = 10^{10}$) of random substitutions

$\overline{\lambda_g}$	5	6	7
	43	7100716301	2899283656

Table 3. The joint distribution of parameters p_g and δ_g
for large number ($n = 10^{10}$) of random involutive substitutions $g \in S(V_8)$
without fixed points

δ_g \ p_g	$\frac{8}{256}$	$\frac{10}{256}$	$\frac{12}{256}$	$\frac{14}{256}$	$\frac{16}{256}$	$\frac{18}{256}$	$\frac{20}{256}$	$\frac{22}{256}$	$\frac{24}{256}$	$\frac{26}{256}$	$\frac{28}{256}$	$\frac{30}{256}$	$\frac{32}{256}$	$\frac{34}{256}$	$\frac{36}{256}$	$\frac{38}{256}$	$\frac{40}{256}$
28/128	590	93771	105093	30290	7050	1394	286	57	8	2	0	0	0	0	0	0	0
30/128	65367	21024974	29009900	9145391	2258699	504435	106672	20630	3730	681	115	18	0	0	0	0	0
32/128	771867	460010027	869598317	333799705	94915565	23130073	5400964	1158703	240057	46669	8922	1600	277	39	7	3	0
34/128	568358	458997063	952330024	381587915	111542137	28057245	6786544	1510151	326130	66237	13049	2524	467	75	7	3	0
36/128	693472	734760284	1830988788	833334303	266469424	69848483	17747649	4078302	921352	194279	40022	7839	1554	261	40	8	2
38/128	86282	109066477	274763483	124020816	39372527	10486470	2704962	637255	147741	32214	6802	1378	269	44	11	0	0
40/128	154681	222611061	658551126	334408938	115336765	31398366	8340727	1975204	464297	100752	21581	4240	843	166	30	3	2
42/128	5204	8917426	25306761	12228324	4059524	1119393	299530	72758	17532	3917	804	175	46	10	1	0	1
44/128	28123	50822684	169219875	92052089	33240521	9237481	2516284	604695	145376	32022	7021	1456	290	52	7	2	1
46/128	178	473276	1508786	773256	266177	75805	20885	5216	1285	327	66	17	4	3	0	0	0
48/128	4299	10198208	37707025	21648720	8083892	2278262	633869	153367	37692	8430	1861	363	64	20	3	0	0
50/128	6	17733	65065	35861	12789	3660	1046	276	63	17	5	0	0	0	0	0	0
52/128	506	1766921	7304586	4419700	1703348	486257	137390	33956	8435	1909	433	86	14	4	0	0	0
54/128	0	454	2024	1270	473	136	41	11	3	1	0	0	0	0	0	0	0
56/128	64	259891	1220926	778605	310524	90326	26069	6441	1583	365	94	15	7	1	0	0	0
58/128	0	9	59	26	18	1	2	0	1	0	0	0	0	0	0	0	0
60/128	6	32404	174294	118602	48475	14342	4314	1142	285	60	17	7	0	0	0	0	0
62/128	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
64/128	0	3294	21032	15153	6452	1882	628	148	38	11	3	0	0	0	0	0	0
66/128	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
68/128	0	272	2175	1664	791	239	74	19	4	1	0	0	0	0	0	0	0
70/128	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
72/128	0	17	166	157	62	26	10	1	0	0	0	0	0	0	0	0	0
74/128	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
76/128	0	1	18	8	5	1	0	0	0	0	0	0	0	0	0	0	0

Table 4. Empirical distribution of parameter $\overline{\lambda_g}$
for large number ($n = 10^{10}$) of random involutive substitutions $g \in S(V_8)$
without fixed points

$\overline{\lambda_g}$	5	6	7
	83	5794820756	4205179161

Table 5. The number n of constructed substitutions with parameters p_g and δ_g

The values of $\delta_{g'}$ and p_g parameters	n
$\delta_{g'} = 26/128,\ p_{g'} = 6/256$	>10000
$\delta_{g'} = 24/128,\ p_{g'} = 8/256$	>1000
$\delta_{g'} = 24/128,\ p_{g'} = 6/256$	>10

Table 6.

Original S-box g of the national standards of the Russian Federation GOST R 34.11-2015 and GOST R 34.12-2012	One of the new S-boxes g' that we have constructed using our algorithms
$\delta_g = 28/128, p_g = 8/256, \overline{\lambda_g} = 7,$ $r_g = 3, r_g^{(3)} = 441$	$\delta_{g'} = 24/128, p_{g'} = 6/256, \overline{\lambda_{g'}} = 7,$ $r_{g'} = 3, r_{g'}^{(3)} = 441$
fc ee dd 11 cf **6e** 31 16 **fb** c4 fa **da** 23 **c5** 4 4d e9 77 f0 **db** **93** 2e **99** ba 17 36 **f1** bb 14 cd 5f c1 f9 18 65 5a e2 5c ef 21 **81** 1c 3c 42 8b **1** 8e 4f **5** 84 2 ae e3 6a 8f **a0** **6** b ed **98** 7f d4 **d3** 1f **eb** 34 2c 51 ea **c8** 48 ab f2 **2a** **68** a2 fd 3a ce cc **b5** **70** e 56 8 c 76 12 bf 72 13 47 **9c** **b7** 5d 87 15 a1 96 **29** 10 7b 9a c7 f3 **91** 78 6f 9d 9e **b2** b1 32 75 **19** 3d ff **35** 8a 7e **6d** **54** c6 80 c3 **bd** d 57 df **f5** **24** a9 3e a8 **43** c9 d7 **79** d6 f6 **7c** 22 b9 3 e0 f ec de **7a** **94** b0 bc dc e8 28 50 4e 33 **a** 4a a7 97 60 73 1e **0** 62 44 1a b8 38 82 **64** **9f** 26 41 ad 45 46 92 27 5e **55** 2f 8c **a3** a5 7d **69** d5 95 3b 7 **58** **b3** 40 86 **ac** 1d **f7** **30** 37 6b e4 88 **d9** e7 89 e1 1b 83 49 4c 3f f8 fe 8d **53** **aa** 90 ca d8 85 61 20 71 **67** a4 **2d** **2b** 9 5b cb 9b 25 **d0** be e5 **6c** 52 59 a6 74 d2 **e6** f4 **b4** **c0** d1 66 af **c2** 39 4b **63** b6	fc ee dd 11 cf **b7** 31 16 **53** c4 fa **2b** 23 **b5** 4 4d e9 77 f0 **69** **ac** 2e **bd** ba 17 36 **68** bb 14 cd 5f c1 f9 18 65 5a e2 5c ef 21 **aa** 1c 3c 42 8b **7c** 8e 4f **24** 84 2 ae e3 6a 8f **79** **98** b ed **6** 7f d4 **7a** 1f **d0** 34 2c 51 ea **58** 48 ab f2 **30** **f1** a2 fd 3a ce cc **91** **67** e 56 8 c 76 12 bf 72 13 47 **b3** **6e** 5d 87 15 a1 96 **b4** 10 7b 9a c7 f3 **c5** 78 6f 9d 9e **d9** b1 32 75 **a** 3d ff **19** 8a 7e **55** **e6** c6 80 c3 **0** d 57 df **9f** **63** a9 3e a8 **f7** c9 d7 **a3** d6 f6 **1** 22 b9 3 e0 f ec de **d3** **f5** b0 bc dc e8 28 50 4e 33 **35** 4a a7 97 60 73 1e **64** 62 44 1a b8 38 82 **99** **94** 26 41 ad 45 46 92 27 5e **6d** 2f 8c **a0** a5 7d **db** d5 95 3b 7 **c8** **9c** 40 86 **93** 1d **43** **c0** 37 6b e4 88 **b2** e7 89 e1 1b 83 49 4c 3f f8 fe 8d **fb** **81** 90 ca d8 85 61 20 71 **70** a4 **6c** **da** 9 5b cb 9b 25 **c2** be e5 **2d** 52 59 a6 74 d2 **54** f4 **29** **2a** d1 66 af **eb** 39 4b **5** b6
Substitutions g and g' differ in 63 values (differing positions are in bold).	
Sequence of 36 transpositions is converting S-box g to g': (6e,b7),(fb,53),(da,2b),(c5,b5),(db,69),(93,ac),(99,bd),(f1,68),(81,aa),(1,7c),(5,24),(a0,79), (6,98),(d3,7a),(eb,d0),(c8,58),(2a,30),(b5,91),(70,67),(9c,b3),(29,b4),(b2,d9),(19,a),(35,a), (6d,55),(54,e6),(bd,0),(f5,9f),(24,63),(43,f7),(79,a3),(94,9f),(0,64),(30,c0),(2d,6c),(d0,c2).	

Table 7.

Original S-box g of state standard of the Republic of Belarus «BelT»	One of the new S-boxes g' that we have constructed using our algorithms
$\delta_g = 26/128, p_g = 8/256, \overline{\lambda_g} = 6,$ $r_g = 3, r_g^{(3)} = 441$	$\delta_{g'} = 24/128, p_{g'} = 6/256, \overline{\lambda_{g'}} = 7,$ $r_{g'} = 3, r_{g'}^{(3)} = 441$
b1 **94** **ba** c8 a 8 f5 3b 36 6d **0** 8e 58 4a 5d e4 85 4 fa 9d 1b **b6** c7 ac 25 2e 72 c2 **2** fd ce d 5b e3 d6 12 **17** b9 61 81 fe 67 86 ad 71 6b 89 b 5c b0 c0 ff 33 c3 56 b8 35 c4 5 ae d8 e0 7f 99 e1 2b dc 1a e2 **82** 57 ec 70 **3f** cc f0 95 ee **8d** f1 c1 ab 76 38 **9f** e6 78 ca f7 c6 f8 60 d5 bb 9c 4f f3 3c 65 7b 63 7c 30 6a dd 4e a7 79 9e b2 3d **31** 3e 98 b5 6e 27 d3 bc cf 59 **1e** 18 1f 4c 5a b7 93 e9 de e7 2c 8f c f **a6** **2d** db 49 f4 6f 73 96 **47** 6 **7** 53 16 ed 24 7a 37 39 cb a3 83 3 a9 8b f6 92 bd 9b 1c e5 d1 41 1 54 45 fb c9 5e 4d e f2 68 20 80 aa 22 7d 64 **2f** 26 **87** f9 34 90 40 55 11 **be** 32 97 13 43 fc 9a 48 a0 2a 88 5f 19 4b 9 a1 7e cd a4 d0 15 44 af 8c a5 84 50 **bf** 66 d2 e8 8a a2 d7 46 52 42 a8 df b3 69 74 c5 51 eb **23** 29 21 d4 ef d9 b4 3a 62 28 75 91 14 10 ea 77 6c **da** **1d**	b1 **17** **0** c8 a 8 f5 3b 36 6d **ba** 8e 58 4a 5d e4 85 4 fa 9d 1b **3f** c7 ac 25 2e 72 c2 **be** fd ce d 5b e3 d6 12 2 b9 61 81 fe 67 86 ad 71 6b 89 b 5c b0 c0 ff 33 c3 56 b8 35 c4 5 ae d8 e0 7f 99 e1 2b dc 1a e2 **b6** 57 ec 70 **1e** cc f0 95 ee **23** f1 c1 ab 76 38 **bf** e6 78 ca f7 c6 f8 60 d5 bb 9c 4f f3 3c 65 7b 63 7c 30 6a dd 4e a7 79 9e b2 3d **2d** 3e 98 b5 6e 27 d3 bc cf 59 **82** 18 1f 4c 5a b7 93 e9 de e7 2c 8f c f **7** **31** db 49 f4 6f 73 96 **1d** 6 **a6** 53 16 ed 24 7a 37 39 cb a3 83 3 a9 8b f6 92 bd 9b 1c e5 d1 41 1 54 45 fb c9 5e 4d e f2 68 20 80 aa 22 7d 64 **da** 26 **47** f9 34 90 40 55 11 **94** 32 97 13 43 fc 9a 48 a0 2a 88 5f 19 4b 9 a1 7e cd a4 d0 15 44 af 8c a5 84 50 **9f** 66 d2 e8 8a a2 d7 46 52 42 a8 df b3 69 74 c5 51 eb **8d** 29 21 d4 ef d9 b4 3a 62 28 75 91 14 10 ea 77 6c **2f** **87**
Substitutions g and g' differ in 23 values (differing positions are in bold).	
Sequence of 14 transpositions is converting S-box g to g': (94,17),(ba,0),(b6,3f),(2,be),(17,be),(82,3f),(3f,1e),(8d,23),(9f,bf),(31,2d),(a6,7),(47,1d), (2f,da),(87,1d).	

Table 8.

Original S-box of block cipher «Skipjack» developed by the US NSA	One of the new S-boxes g' that we have constructed using our algorithms
$\delta_g = 28/128,\ p_g = 12/256,\ \overline{\lambda_g} = 6,$ $r_g = 3,\ r_g^{(3)} = 441$	$\delta_{g'} = 24/128,\ p_{g'} = 6/256,\ \overline{\lambda_{g'}} = 7,$ $r_{g'} = 3,\ r_{g'}^{(3)} = 441$
a3 **d7** **9** 83 **f8** 48 **f6** **f4** b3 **21** 15 **78** **99** b1 **af** f9 **e7** 2d 4d **8a** ce **4c** ca **2e** **52** 95 **d9** 1e 4e **38** **44** 28 **a** **df** 2 a0 17 f1 **60** 68 12 b7 **7a** **c3** e9 fa **3d** **53** 96 84 **6b** ba f2 63 **9a** 19 7c ae **e5** f5 f7 **16** 6a a2 **39** b6 **7b** **f** c1 93 81 1b **ee** b4 1a ea d0 91 **2f** b8 55 b9 **da** 85 3f 41 bf **e0** 5a 58 **80** **5f** 66 **b** d8 90 **35** d5 **c0** **a7** 33 **6** 65 69 45 **0** 94 56 6d **98** 9b 76 **97** fc b2 c2 **b0** fe **db** 20 e1 eb **d6** e4 **dd** 47 4a **1d** 42 ed 9e **6e** **49** **3c** cd 43 27 d2 **7** **d4** **de** c7 67 18 **89** **cb** 30 1f **8d** c6 **8f** **aa** **c8** 74 dc c9 **5d** 5c 31 a4 **70** 88 61 2c **9f** **d** **2b** 87 50 82 54 **64** 26 **7d** **3** 40 **34** 4b 1c 73 d1 **c4** fd 3b cc fb **7f** ab **e6** 3e 5b a5 ad **4** 23 9c 14 51 **22** **f0** **29** 79 **71** **7e** ff 8c **e** **e2** **c** ef bc **72** 75 6f 37 a1 ec d3 **8e** 62 **8b** **86** **10** e8 **8** **77** 11 be **92** **4f** 24 c5 32 **36** 9d cf **f3** a6 **bb** **ac** 5e 6c a9 **13** 57 25 b5 e3 bd a8 3a **1** **5** 59 2a 46	a3 **7f** **db** 83 **80** 48 **53** **da** b3 **de** 15 **9a** **5d** b1 **ee** f9 **c4** 2d 4d **5f** ce **99** ca **97** **71** 95 **d** 1e 4e **49** **70** 28 **89** **34** **2** a0 17 f1 **f0** 68 12 b7 **22** **4c** e9 fa **98** **e6** 96 84 **e** ba f2 63 **60** 19 7c ae **2f** f5 f7 **8f** 6a a2 **6e** b6 **36** **f** c1 93 81 1b **af** b4 1a ea d0 91 **e5** b8 55 b9 **d7** 85 3f 41 bf **d4** 5a 58 **92** **8a** 66 **b** d8 90 **4f** d5 **f6** **7e** 33 **6** 65 69 45 **0** 94 56 6d **3d** 9b 76 **e2** fc b2 c2 **29** fe **8b** 20 e1 eb **bb** e4 **77** 47 4a **3** 42 ed 9e **39** **38** **c3** cd 43 27 d2 **7** **44** **21** c7 67 18 **9f** **6b** 30 1f **72** c6 **16** **f3** **64** 74 dc c9 **3c** 5c 31 a4 **e0** 88 61 2c **c0** **d9** **8e** 87 50 82 54 **c8** 26 **ac** **1d** 40 **e7** 4b 1c 73 d1 **f4** fd 3b cc fb **df** ab **a** 3e 5b a5 ad **4** 23 9c 14 51 **2b** **78** **b0** 79 **cb** **a7** ff 8c **52** **2e** **c** ef bc **8d** 75 6f 37 a1 ec d3 **7a** 62 **9** **aa** **13** e8 **8** **dd** 11 be **f8** **35** 24 c5 32 **7b** 9d cf **86** a6 **d6** **7d** 5e 6c a9 **10** 57 25 b5 e3 bd a8 3a **1** **5** 59 2a 46
Substitutions g and g' differ in 89 values (differing positions are in bold).	
Sequence of 58 transpositions is converting S-box g to g': (d7,7f),(9,db),(f8,80),(f6,53),(f4,da),(21,de),(78,9a),(99,5d),(af,ee),(e7,c4),(8a,5f),(4c,5d), (2e,97),(52,71),(d9,d),(38,49),(44,70),(a,89),(df,34),(60,f0),(7a,22),(c3,5d),(3d,98),(53,e6), (6b,e),(9a,f0),(e5,2f),(16,8f),(39,6e),(7b,36),(da,7f),(e0,d4),(80,92),(35,4f),(c0,e6),(a7,7e), (97,e2),(b0,29),(db,8b),(d6,bb),(dd,77),(1d,3),(3c,5d),(d4,70),(89,9f),(cb,e),(8d,72),(aa,f3), (c8,64),(9f,e6),(2b,8e),(7d,ac),(34,c4),(c4,7f),(22,8e),(71,e),(86,f3),(10,13).	

Table 9.

Original involutive S-box g of block cipher «Khazad-0»	One of the new involutive S-boxes g' that we have constructed using our algorithms
$\delta_g = 34/128,\ p_g = 8/256,\ \overline{\lambda_g} = 7,$ $r_g = 3,\ r_g^{(3)} = 441$	$\delta_{g'} = 24/128,\ p_{g'} = 6/256,\ \overline{\lambda_{g'}} = 7,$ $r_{g'} = 3,\ r_{g'}^{(3)} = 441$
a7 **d3** **e6** **71** **d0** ac **4d** 79 3a **c9** **91** fc 1e 47 54 bd 8c **a5** 7a fb 63 b8 **dd** **d4** e5 b3 c5 be **a9** **88** c a2 **39** **df** 29 da 2b **a8** **cb** 4c **4b** 22 **aa** 24 41 **70** a6 **f9** **5a** **e2** **b0** **36** 7d e4 **33** ff 60 **20** 8 **8b** 5e **ab** **7f** 78 7c 2c 57 d2 **dc** 6d 7e d 53 94 c3 **28** 27 **6** 5f **ad** 67 5c 55 48 e 52 ea 42 **5b** 5d **30** **58** 51 59 3c 4e 38 8a 72 14 e7 c6 de 50 8e 92 d1 77 **93** 45 9a **ce** **2d** **3** 62 **b6** **b9** **bf** 96 6b 3f 7 12 ae 40 34 46 **3e** db cf ec cc c1 **a1** c0 d6 **1d** f4 61 **3b** 10 d8 68 a0 b1 **a** 69 **6c** 49 fa 76 c4 **9e** 9b 6e 99 c2 b7 **98** bc 8f **85** 1f b4 f8 **11** 2e **0** **25** **1c** **2a** **3d** 5 **4f** 7b **b2** **32** 90 **af** 19 a3 f7 **73** 9d 15 **74** **ee** ca 9f f 1b **75** 86 84 9c 4a 97 1a 65 f6 ed **9** bb **26** 83 eb **6f** 81 **4** 6a 43 **1** **17** e1 87 **f5** 8d **e3** 23 80 **44** **16** 66 **21** **fe** d5 **31** **d9** 35 18 **2** 64 **f2** f1 56 cd 82 c8 **ba** f0 ef e9 **e8** fd 89 **d7** c7 b5 a4 **2f** 95 13 b f3 **e0** 37	**e2** **98** **2d** **d4** **8b** ac **7f** 79 3a **dc** **75** fc 1e 47 54 bd 8c **a7** 7a fb 63 b8 **b9** **bf** e5 b3 c5 be **85** **d0** c a2 **cb** **a5** 29 da 2b **91** **f2** 4c **ba** 22 **b2** 24 41 **2** a6 **31** **3d** **2f** **6f** **fe** 7d e4 **e0** ff 60 **e8** 8 **88** 5e **30** **4d** 78 7c 2c 57 d2 **ad** 6d 7e d 53 94 c3 **ee** 27 **3e** 5f **f5** 67 5c 55 48 e 52 ea 42 **df** 5d **ab** **6c** 51 59 3c 4e 38 8a 72 14 e7 c6 de 50 8e 92 d1 77 **5b** 45 9a **32** **e3** **f9** 62 **d3** **dd** **a** 96 6b 3f 7 12 ae 40 34 46 **6** db cf ec cc c1 **1c** c0 d6 **3b** f4 61 **4** 10 d8 68 a0 b1 **25** 69 **a8** 49 fa 76 c4 **1** 9b 6e 99 c2 b7 **b6** bc 8f **a9** 1f b4 f8 **21** 2e **11** **93** **a1** **af** **5a** 5 **44** 7b **aa** **ce** 90 **2a** 19 a3 f7 **9e** 9d 15 **16** **28** ca 9f f 1b **17** 86 84 9c 4a 97 1a 65 f6 ed **d7** bb **20** 83 eb **b0** 81 **1d** 6a 43 **73** **3** e1 87 **c9** 8d **e6** 23 80 **9** **74** 66 **58** **36** d5 **0** **70** 35 18 **d9** 64 **39** f1 56 cd 82 c8 **4b** f0 ef e9 **26** fd 89 **4f** c7 b5 a4 **71** 95 13 b f3 **33** 37
Substitutions g and g' differ in 88 values (differing positions are in bold).	
Sequence of 30 pairs transpositions is converting S-box g to g': (a7,e2),(0,11);(d3,98),(1,73);(e6,2d),(2,d9);(71,d4),(3,f9);(d0,8b),(4,1d);(4d,7f),(6,3e);(c9,dc), (9,d7);(91,75),(a,25);(a5,e2),(11,21);(dd,b9),(16,74);(d4,bf),(17,f9);(a9,85),(1c,a1);(88,8b),(1d, 3b);(39,cb),(20,e8);(df,e2),(21,58);(a8,75),(25,93);(cb,f2),(26,e8);(4b,ba),(28,ee);(aa,b2),(2a,af);(70,d9),(2d,e3);(f9,31),(2f,bf);(5a,3d),(30,ab);(e2,bf),(31,58);(b0,6f),(32,ce);(36,fe),(33,e0); (dc,ad),(44,d7);(ad,f5),(4f,d7);(5b,bf),(58,6c);(93,bf),(6c,75);(b6,98),(73,9e).	

Table 10.

Original efficiently-implemented S-box g of block ciphers «Khazad» and «Anubis»	One of the new efficiently-implemented S-boxes g' that we have constructed using our algorithms
$\delta_g = 32/128,\ p_g = 8/256,\ \overline{\lambda_g} = 7,$ $r_g = 3,\ r_g^{(3)} = 441$	$\delta_{g'} = 30/128,\ p_{g'} = 8/256,\ \overline{\lambda_{g'}} = 7,$ $r_{g'} = 3,\ r_{g'}^{(3)} = 441$
ba 54 2f 74 53 d3 d2 4d 50 ac 8d bf 70 52 9a 4c ea d5 97 d1 33 51 5b a6 de 48 a8 99 db 32 b7 fc e3 9e 91 9b e2 bb 41 6e a5 cb 6b 95 a1 f3 b1 2 cc c4 1d 14 c3 63 da 5d 5f dc 7d cd 7f 5a 6c 5c f7 26 ff ed e8 9d 6f 8e 19 a0 f0 89 f 7 af fb 8 15 d 4 1 64 df 76 79 dd 3d 16 3f 37 6d 38 b9 73 e9 35 55 71 7b 8c 72 88 f6 2a 3e 5e 27 46 c 65 68 61 3 c1 57 d6 d9 58 d8 66 d7 3a c8 3c fa 96 a7 98 ec b8 c7 ae 69 4b ab a9 67 a 47 f2 b5 22 e5 ee be 2b 81 12 83 1b e 23 f5 45 21 ce 49 2c f9 e6 b6 28 17 82 1a 8b fe 8a 9 c9 87 4e e1 2e e4 e0 eb 90 a4 1e 85 60 0 25 f4 f1 94 b e7 75 ef 34 31 d4 d0 86 7e ad fd 29 30 3b 9f f8 c6 13 6 5 c5 11 77 7c 7a 78 36 1c 39 59 18 56 b3 b0 24 20 b2 92 a3 c0 44 62 10 b4 84 43 93 c2 4a bd 8f 2d bc 9c 6a 40 cf a2 80 4f 1f ca aa 42	cd ef 6d e4 6b 61 bd bb cc 62 e1 bc cf c7 ed b6 a5 fe 8e 40 f1 d0 da 43 35 4c a6 6a 4a 5a 22 53 37 d4 1e 8f ae 78 e0 30 29 28 2f 7a 67 89 a4 2a 27 b9 ca df 9a 18 70 20 94 a8 af ce 87 b4 99 9e 13 74 81 17 82 dc d3 d5 e3 d6 1c 63 19 e9 71 65 7c c9 b3 1f b5 dd 8c 86 c1 db 1d b1 77 c4 c3 b2 76 5 9 4b 93 4f f7 2c c2 ad 1b 4 f6 2 c5 91 36 4e de f8 41 88 60 5c 25 fd 2b 8a 50 fa a2 f3 e6 42 44 fb a1 ff 57 3c 75 2d 7b f9 56 f5 12 23 9f 6f e8 64 38 ee c8 98 97 3e 34 c0 bf b7 3f 90 a9 84 7e d7 2e 10 1a aa 39 a0 a7 ea d9 69 24 3a cb 5b 5f 52 3d 54 f 9d c6 31 e2 7 b 6 eb 9c 9b 58 68 5e 5d 6e b8 d 96 51 32 b0 8 0 3b c 15 f2 f4 46 21 47 49 a3 e5 ac 16 59 45 55 72 33 26 a ba 48 3 d8 80 fc 92 4d ab be f0 e 95 1 ec 14 d1 7f d2 8d 6c 66 73 8b 7d 83 e7 79 11 85
Substitutions g and g' differ in all values.	

P mini-box **3 f e 0** 5 4 **b c d** a 9 **6 7 8 2 1**	P' mini-box **6 d b 8** 5 4 **0 f 3** a 9 **2 e 1 c** 7
$\delta_P = 4,\ p_P = 4,\ \overline{\lambda_P} = 3$	$\delta_{P'} = 4,\ p_{P'} = 6,\ \overline{\lambda_{P'}} = 2$
Substitutions P and P' differ in 12 values (differing positions are in bold).	
Sequence of 5 pairs transpositions is converting mini-box P to P': (3,6),(0,8); (f,d),(1,7); (e,b),(2,c); (b,8),(6,c); (c,d),(7,8).	
Q mini-box 9 **e 5 6 a 2 3 c f** 0 **4 d 7 b 1 8**	Q' mini-box 9 **7 f 4 3 c d 1 a** 0 **8 e 5 6 b 2**
$\delta_Q = 4,\ p_Q = 4,\ \overline{\lambda_Q} = 3$	$\delta_{Q'} = 6,\ p_{Q'} = 6,\ \overline{\lambda_{Q'}} = 3$
Substitutions Q and Q' differ in 14 values (differing positions are in bold).	
Sequence of 6 pairs transpositions is converting mini-box Q to Q': (e,7),(1,b); (5,f),(2,c); (6,4),(3,d); (a,d),(4,8); (c,b),(7,f); (f,d),(8,b).	