# 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 spectraldifferential 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 $G F(2)$. Suppose that $V_{n}^{\times}=V_{n} \backslash\{0\}$. Let $S\left(V_{n}\right)$ 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

$$
p_{g}=\max _{\alpha, \beta \in V_{n}^{\times}} p_{\alpha, \beta}^{g}
$$

where

$$
p_{\alpha, \beta}^{g}=2^{-n} \cdot\left|\left\{x \in V_{n} \mid g(x \oplus \alpha) \oplus g(x)=\beta\right\}\right| .
$$

The nonlinear order of $f$, denoted by $\operatorname{deg}(f)$, 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 $l_{\alpha}: V_{n} \rightarrow V_{1}$ the linear Boolean function equal to the sum of bits of argument selected by bits of $\alpha$ :

$$
l_{\alpha}(x)={\underset{i=0}{n-1} \alpha_{i} \cdot x_{i} . . . . . . .}
$$

The correlation $c\left(f_{1}, f_{2}\right)$ between two Boolean function $f_{1}$ and $f_{2}$ is defined as

$$
c\left(f_{1}, f_{2}\right)=2^{1-n} \cdot\left|\left\{x \mid f_{1}(x)=f_{2}(x)\right\}\right|-1 .
$$

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 $\delta_{g}$-parameter of an S-box $g$ is defined as the absolute value of the bias:

$$
\delta_{g}=\max _{\alpha, \beta \in V_{n}^{\times}} \delta_{\alpha, \beta}^{g},
$$

where

$$
\delta_{\alpha, \beta}^{g}=\left|c\left(l_{\alpha}, l_{\beta} \circ g\right)\right| .
$$

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

$$
\lambda_{g}=\min _{\alpha \in V_{n}^{\times}}\left\{\operatorname{deg}\left(l_{\alpha} \circ g(x)\right)\right\} .
$$

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

$$
r_{g}^{(i)}=\operatorname{dim} H_{g}^{(i)}
$$

where

$$
H_{g}^{(i)}=\left\{\begin{array}{l|c}
h \in G F(2)\left[z_{1}, \ldots, z_{2 n}\right] & \forall x \in V_{n}, h(x, g(x))=0 \\
0<\operatorname{deg} h \leq i
\end{array}\right\}
$$

Definition 5. The $r_{g}$-parameter of an S-box $g$ is defined as

$$
r_{g}=\min \left\{i \mid r_{g}^{(i)}>0\right\}
$$

Remark 1. For substitution $g \in S\left(V_{8}\right)$ 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

$$
T_{1}[\alpha, \beta]=\left|\left\{x \in V_{n} \mid g(x \oplus \alpha) \oplus g(x)=\beta\right\}\right|
$$

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

$$
T_{2}[\alpha, \beta]=\left|\left\{x \in V_{n} \mid \alpha \circ x=\beta \circ g(x)\right\}\right|-2^{n-1}
$$

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

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

we define the sets

$$
\begin{aligned}
D(g, p) & =\left\{(\alpha, \beta) \in V_{n}^{\times} \times V_{n} \mid p_{\alpha, \beta}^{g}=p\right\} \\
L(g, \delta) & =\left\{(\alpha, \beta) \in V_{n} \times V_{n}^{\times} \mid \delta_{\alpha, \beta}^{g}=\delta\right\}
\end{aligned}
$$

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

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

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

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

## 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 $\left(n=10^{10}\right)$ All pseudo-random involutory substitutions generated don't have quadratic equation.

## 4 New methods

New proposed methods are based on using linear $L\left(g_{i}\right)$ and differential $D\left(g_{i}\right)$ 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:

$$
(a, b, c, d, e) \in S\left(V_{n}\right) \times \mathbb{Q} \times \mathbb{Z} \times \mathbb{Q} \times V_{n}^{k}
$$

On the set of these objects we have an order relation

$$
\left(a^{\prime}, b^{\prime}, c^{\prime}, d^{\prime}, e^{\prime}\right) \leq(a, b, c, d, e), \text { if }\left\{\begin{array}{l}
b^{\prime}<b, d^{\prime} \leq d \text { or }  \tag{1}\\
b^{\prime}=b, c^{\prime} \leq c, d^{\prime} \leq d
\end{array}\right.
$$

### 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 $g_{0} \in S\left(V_{n}\right)$, parameter $w_{1} \in \mathbb{N}$.
Step 1. For substitution $g_{0}$ calculate values

$$
p_{g_{0}}, D\left(g_{0}\right), \delta_{g_{0}}, X_{g_{0}}
$$

where $X_{g_{0}}=\left\{x \in V_{n} \mid g_{0}(x+\alpha)+g_{0}(x)=\beta, \exists(\alpha, \beta) \in D\left(g_{0}, p_{g_{0}}\right)\right\}$.
Initialize list $I$ :

$$
I=\left\{\left(g_{0}, p_{g_{0}},\left|D\left(g_{0}, p_{g_{0}}\right)\right|, \delta_{g_{0}}, X_{g_{0}}\right)\right\}, \quad|I|=1
$$

Step 2. Using the list

$$
I=\left\{\left(g_{i}, p_{g_{i}},\left|D\left(g_{i}, p_{g_{i}}\right)\right|, \delta_{g_{i}}, X_{g_{i}}\right), i=0, \ldots,|I|-1\right\}
$$

construct the new list

$$
\begin{gathered}
I^{\prime}=\left\{\left(g_{i, j}^{\prime}, p_{g_{i, j}^{\prime}},\left|D\left(g_{i, j}^{\prime}, p_{g_{i, j}^{\prime}}\right)\right|, \delta_{g_{i, j}^{\prime}}, X_{g_{i, j}^{\prime}}\right)\right\} \\
\left|I^{\prime}\right| \leq \sum_{i=0}^{|I|-1} \frac{\left|X_{g_{i}}\right| \cdot\left(\left|X_{g_{i}}\right|-1\right)}{2}
\end{gathered}
$$

Substitutions $g_{i, j}^{\prime}$ are elements of list $I^{\prime}$, and $g_{i, j}^{\prime}$ is equal to substitution $g_{i}$ multiplied by transpositions from the set $X_{g_{i}}$ with special properties:

$$
g_{i, j}^{\prime}=\left(x, x^{\prime}\right) \cdot g_{i}
$$

where $x, x^{\prime} \in X_{g_{i}}, x \leq x^{\prime}, i=0, \ldots,|I|-1, j=j\left(x, x^{\prime}\right)$ is an injective mapping,

$$
p_{g_{i, j}^{\prime}} \leq p_{g_{i}}, \quad \delta_{g_{i, j}^{\prime}} \leq \delta_{g_{i}}
$$

and $\left|D\left(g_{i, j}^{\prime}, p_{g_{i, j}^{\prime}}\right)\right|<\left|D\left(g_{i}, p_{g_{i}}\right)\right|$ if $p_{g_{i, j}^{\prime}}=p_{g_{i}}$.
Step 3.
3.1. Remove repetitions from the list $I^{\prime}$.
3.2. Calculate the size $\left|I^{\prime}\right|$ of list $I^{\prime}$.
3.3. Sort the elements of list $I^{\prime}$ in the ascending order according to the order relation (1).
3.4. Numerate the sorted list elements by indexes $i=0, \ldots,\left|I^{\prime}\right|-1$.
3.5. Calculate values

$$
m_{1}=\min \left\{|I|-1,\left|I^{\prime}\right|-1\right\} \text { and } m_{2}=\min \left\{w_{1}-1,\left|I^{\prime}\right|-1\right\}
$$

Step 4. Compare the first elements of list $I^{\prime}$ and list $I$ :

- If $\sum_{i=0}^{m_{1}} p_{g_{i}^{\prime}}<\sum_{i=0}^{m_{1}} p_{g_{i}}$
or
$\sum_{i=0}^{m_{1}} p_{g_{i}^{\prime}}=\sum_{i=0}^{m_{1}} p_{g_{i}}$ and $\sum_{i=0}^{m_{1}}\left|D\left(g_{i}^{\prime}, p_{g_{i}^{\prime}}\right)\right|<\sum_{i=0}^{m_{1}}\left|D\left(g_{i}, p_{g_{i}}\right)\right|$,
then
4.1 Clean list $I$.
4.2 Copy elements from list $I^{\prime}$ with indexes $i=0, \ldots, m_{2}$ to list $I$.
4.3 Assign $|I|=m_{2}+1$.
4.4 Go to Step 2.
- Otherwise, the algorithm stops.

Output: the list

$$
I^{\prime}=\left\{\left(g_{i}, p_{g_{i}},\left|D\left(g_{i}, p_{g_{i}}\right)\right|, \delta_{g_{i}}, X_{g_{i}}\right), i=0, \ldots,\left|I^{\prime}\right|-1\right\},\left|I^{\prime}\right| \leq w_{1}
$$

Let us denote by $t_{1}$ the computational complexity of algorithm 1.
Proposition 1. For $n \rightarrow \infty$ we have

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

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 $g \in S\left(V_{n}\right)$. For elements of a differential spectrum $D(g)$ we have

$$
|D(g, p)| \leq\left(2^{n}-1\right) \cdot \frac{1}{p}, \quad p \in P_{n-1} \backslash\{0\}
$$

Thus, we obtain the following expressions:

$$
\begin{gathered}
\sum_{p \in P_{n-1} \backslash\{0\}}\left(2^{n}-1\right) \cdot \frac{1}{p}=\left(2^{n}-1\right) \cdot \sum_{p \in P_{n-1} \backslash\{0\}} \frac{1}{p}= \\
=\left(2^{n}-1\right) \cdot \sum_{i=1}^{2^{n-1}} \frac{2^{n-1}}{i}=\left(2^{n}-1\right) \cdot 2^{n-1} \cdot \sum_{i=1}^{2^{n-1}} \frac{1}{i} \leq \\
\leq\left(2^{n}-1\right) \cdot 2^{n-1} \cdot\left(\ln 2^{n-1}+1\right) \leq\left(2^{n}-1\right) \cdot 2^{n-1} \cdot\left(\log _{2} 2^{n-1}+1\right)= \\
=n \cdot 2^{n-1} \cdot\left(2^{n}-1\right)
\end{gathered}
$$

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 $X_{g_{i}}$

$$
C_{\left|X_{g_{i}}\right|}^{2} \leq C_{\left|V_{n}\right|}^{2}=\frac{2^{n} \cdot\left(2^{n}-1\right)}{2}
$$

(c) the complexity of computing $\delta_{g_{i}}$-parameter, which is equal to

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

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

$$
w_{1} \cdot 2 \cdot \frac{2^{n} \cdot\left(2^{n}-1\right)}{2} \cdot c \cdot 2^{2 n} \cdot n
$$

Finally, for the total complexity of the algorithm we have

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

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

$$
\delta_{g_{0}}, L\left(g_{0}\right), p_{g_{0}}, Y_{g_{0}}
$$

where $Y_{g_{0}}=\left\{y \in V_{n} \mid y \circ \alpha=g_{0}(y) \circ \beta ; \exists(\alpha, \beta) \in L\left(g_{0}, \delta_{g_{0}}\right)\right\}$.
Initialize list $I$ :

$$
I=\left\{\left(g_{0}, \delta_{g_{0}},\left|L\left(g_{0}, \delta_{g_{0}}\right)\right|, p_{g_{0}}, Y_{g_{0}}\right)\right\},|I|=1
$$

Step 2. Using the list

$$
I=\left\{\left(g_{i}, \delta_{g_{i}},\left|L\left(g_{i}, \delta_{g_{i}}\right)\right|, p_{g_{i}}, Y_{g_{i}}\right), i=0, \ldots,|I|-1\right\}
$$

construct the new list

$$
\begin{gathered}
I^{\prime}=\left\{\left(g_{i, j}^{\prime}, \delta_{g_{i, j}^{\prime}},\left|L\left(g_{i, j}^{\prime}, \delta_{g_{i, j}^{\prime}}\right)\right|, p_{g_{i, j}^{\prime}}, Y_{g_{i, j}^{\prime}}\right)\right\} \\
\left|I^{\prime}\right| \leq \sum_{i=0}^{|I|-1} \frac{\left|Y_{g_{i}}\right|\left(\left|Y_{g_{i}}\right|-1\right)}{2}
\end{gathered}
$$

Substitutions $g_{i, j}^{\prime}$ are elements of list $I^{\prime}$, and $g_{i, j}^{\prime}$ is equal to substitution $g_{i}$ multiplied by transpositions from the set $Y_{g_{i}}$ with special properties:

$$
g_{i, j}^{\prime}=\left(y, y^{\prime}\right) \cdot g_{i}
$$

where $y, y^{\prime} \in Y_{g_{i}}, y \leq y^{\prime}, i=0, \ldots,|I|-1, j=j\left(y, y^{\prime}\right)$ is injective mapping,

$$
\delta_{g_{i, j}^{\prime}} \leq \delta_{g_{i}}, \quad p_{g_{i, j}^{\prime}} \leq p_{g_{i}}
$$

and $\left|L\left(g_{i, j}^{\prime}, p_{g_{i, j}^{\prime}}\right)\right|<\left|L\left(g_{i}, p_{g_{i}}\right)\right|$ if $\delta_{g_{i, j}^{\prime}}=\delta_{g_{i}}$.
Step 3.
3.1. Remove repetitions from the list $I^{\prime}$.
3.2. Calculate the size $\left|I^{\prime}\right|$ of list $I^{\prime}$.
3.3. Sort the elements of list $I^{\prime}$ in the ascending order according to the order relation (1).
3.4. Numerate the sorted list elements by indexes $i=0, \ldots,\left|I^{\prime}\right|-1$.
3.5. Calculate values

$$
m_{1}=\min \left\{|I|-1,\left|I^{\prime}\right|-1\right\} \text { and } m_{2}=\min \left\{w_{2}-1,\left|I^{\prime}\right|-1\right\} .
$$

Step 4. Compare the first elements of list $I^{\prime}$ and list $I$ :

- If $\sum_{i=0}^{m_{1}} \delta_{g_{i}^{\prime}}<\sum_{i=0}^{m_{1}} \delta_{g_{i}}$
or
$\sum_{i=0}^{m_{1}} \delta_{g_{i}^{\prime}}=\sum_{i=0}^{m_{1}} \delta_{g_{i}}$ and $\sum_{i=0}^{m_{1}}\left|L\left(g_{i}^{\prime}, \delta_{g_{i}^{\prime}}\right)\right|<\sum_{i=0}^{m_{1}}\left|L\left(g_{i}, \delta_{g_{i}}\right)\right|$,
then
4.1. Clean list $I$.
4.2. Copy elements from list $I^{\prime}$ with indexes $i=0, \ldots, m_{2}$ to list $I$.
4.3. Assign $|I|=m_{2}+1$.
4.4. Go to Step 2.
- Otherwise, the algorithm stops.

Output: the list

$$
I^{\prime}=\left\{\left(g_{i}, \delta_{g_{i}},\left|L\left(g_{i}, \delta_{g_{i}}\right)\right|, p_{g_{i}}, Y_{g_{i}}\right), i=0, \ldots,\left|I^{\prime}\right|-1\right\}
$$

Let us denote by $t_{2}$ the computational complexity of algorithm 2 .
Proposition 2. For $n \rightarrow \infty$ we have

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

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 $g \in S\left(V_{n}\right)$. For elements of a linear spectrum $L(g)$ we have

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

Thus, we obtain the following expressions:

$$
\begin{gathered}
\sum_{\delta \in P_{n-2} \backslash\{0\}}\left(2^{n}-1\right) \cdot \frac{1}{\delta^{2}}=\left(2^{n}-1\right) \cdot \sum_{\delta \in P_{n-2} \backslash\{0\}} \frac{1}{\delta^{2}}= \\
=\left(2^{n}-1\right) \cdot \sum_{i=1}^{2^{n-2}} \frac{2^{2 n-4}}{i^{2}}=\left(2^{n}-1\right) \cdot 2^{2 n-4} \cdot \sum_{i=1}^{2^{n-2}} \frac{1}{i^{2}} \leq\left(2^{n}-1\right) \cdot 2^{2 n-4} \cdot \frac{\pi^{2}}{6} .
\end{gathered}
$$

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 $Y_{g_{i}}$

$$
C_{\left|Y_{g_{i}}\right|}^{2} \leq C_{\left|V_{n}\right|}^{2}=\frac{2^{n} \cdot\left(2^{n}-1\right)}{2}
$$

(c) the complexity of computing $\delta_{g_{i}}$-parameter, which is equal to

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

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

$$
w_{2} \cdot 2 \cdot \frac{2^{n} \cdot\left(2^{n}-1\right)}{2} \cdot c \cdot 2^{2 n} \cdot n
$$

Finally, for the total complexity of the algorithm we have

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

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 $Y_{g_{i}}, i=1, \ldots,|I|$, may be defined as $Y_{g_{i}}=V_{n} \backslash X_{g_{i}}$, where

$$
X_{g_{i}}=\left\{x \in V_{n} \mid g_{i}(x+\alpha)+g_{i}(x)=\beta ; \exists(\alpha, \beta) \in D\left(g_{i}, p_{g_{i}}\right)\right\}
$$

## 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 $\left(x, x^{\prime}\right) \cdot\left(g(x), g\left(x^{\prime}\right)\right)$.

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 $g \in S\left(V_{8}\right)$. As a result we have a lot of new affine nonequivalent substitutions $g^{\prime} \in S\left(V_{8}\right)$ with the following cryptographic parameters

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

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 $g \in S\left(V_{8}\right)$ 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 $g^{\prime} \in S\left(V_{8}\right)$, having the parameters

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

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), 2934.
[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, AddisonWesley, 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 highnonlinear 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 $\delta_{g}$
for large number $\left(n=10^{10}\right)$ of random substitutions

| $\delta_{g}$ | $\frac{8}{256}$ | $\frac{10}{256}$ | $\frac{12}{256}$ | $\frac{14}{256}$ | $\frac{16}{256}$ | $\frac{18}{256}$ | $\frac{20}{256}$ | $\frac{22}{256}$ | $\frac{24}{256}$ | $\frac{26}{256}$ |
| :--- | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: |
| $28 / 128$ | 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 $\left(n=10^{10}\right)$ of random substitutions

| $\overline{\lambda_{g}}$ | 5 | 6 | 7 |
| :---: | :---: | :---: | :---: |
|  | 43 | 7100716301 | 2899283656 |

Table 3. The joint distribution of parameters $p_{g}$ and $\delta_{g}$ for large number $\left(n=10^{10}\right)$ of random involutive substitutions $g \in S\left(V_{8}\right)$ without fixed points

| $\delta_{g} p_{g}$ | $\frac{8}{256}$ | $\frac{10}{256}$ | $\frac{12}{256}$ | $\frac{14}{256}$ | $\frac{16}{256}$ | $\frac{18}{256}$ | $\frac{20}{256}$ | $\frac{22}{256}$ | $\frac{24}{256}$ | $\frac{26}{256}$ | $\frac{28}{256}$ | $\frac{30}{256}$ | $\frac{32}{256}$ | $\frac{34}{256}$ | $\frac{36}{256}$ | $\frac{38}{256}$ | $\frac{40}{256}$ |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| 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 |
| 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 $\left(n=10^{10}\right)$ of random involutive substitutions $g \in S\left(V_{8}\right)$ 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 $\delta_{g}$

| The values of $\delta_{g^{\prime}}$ and $p_{g}$ parameters | $n$ |
| :---: | :---: |
| $\delta_{g^{\prime}}=26 / 128, p_{g^{\prime}}=6 / 256$ | $>10000$ |
| $\delta_{g^{\prime}}=24 / 128, p_{g^{\prime}}=8 / 256$ | $>1000$ |
| $\delta_{g^{\prime}}=24 / 128, p_{g^{\prime}}=6 / 256$ | $>10$ |

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 $g^{\prime}$ that we have constructed using our algorithms |
| :---: | :---: |
| $\begin{gathered} \delta_{g}=28 / 128, p_{g}=8 / 256, \overline{\lambda_{g}}=7, \\ r_{g}=3, r_{g}^{(3)}=441 \end{gathered}$ | $\begin{gathered} \delta_{g^{\prime}}=24 / 128, p_{g^{\prime}}=6 / 256, \overline{\lambda_{g^{\prime}}}=7, \\ r_{g^{\prime}}=3, r_{g^{\prime}}^{(3)}=441 \end{gathered}$ |
| fc ee dd $11 \mathrm{cf} 6 \mathrm{e} 3116 \mathrm{fb} \mathrm{c4} \mathrm{fa} \mathrm{da} 23 \mathrm{c5} 44 \mathrm{~d}$ |  |
| e9 77 fo db 93 2e 99 ba $1736 \mathrm{f1}$ bb 14 cd 5 f c1 | e9 77 fo 69 ac 2 e bd ba 173668 bb 14 cd 5 fc |
| f9 18655 a e2 5 c ef $2181 \mathrm{lc} 3 \mathrm{c} 42 \mathrm{8b} 18 \mathrm{se} 4 \mathrm{f}$ | f9 18655 a e2 5 c ef 21 aa $1 \mathrm{c} 3 \mathrm{c} 42 \mathrm{8b} 7 \mathrm{c} 8 \mathrm{e} 4 \mathrm{f}$ |
| 5842 ae e3 $6 \mathrm{a} 8 \mathrm{ffa0} 6 \mathrm{~b}$ ed 987 ff d4 d3 1f | 24842 ae e3 6a 8 f 7998 b ed 67 ff d4 7a 1f |
| eb 342 cc 51 ea c8 48 ab f2 2a 68 a 2 fd 3 ace cc | d0 342 LC 51 ea 5848 ab f2 $30 \mathrm{f1}$ a2 fd 3a ce cc |
|  | 9167 e $5688 \mathrm{c} 7612 \mathrm{bf} 721347 \mathrm{b3}$ 6e 5 d 87 |
| 15 al 9629107 b 9a c7 f3 9178 6f 9d 9e b2 b1 | 15 al 96 b4 10 7b 9a c7 f3 c5 78 6f 9d 9e d9 b1 |
| 327519 3d ff $358 \mathrm{8a} 7 \mathrm{e} 6 \mathrm{~d} 54 \mathrm{c} 680 \mathrm{c3}$ bd d 57 | 3275 a 3d ff $198 \mathrm{8a} 7 \mathrm{7e} 55$ e6 c6 80 c3 0 d 57 |
|  | df 9f 63 a9 3e a8 f7 c9 d7 a3 d6 f6 1022 b 9 |
| e0 f ec de 7a 94 b0 bc dc e8 28504 e 33 a 4a | e0 f ec de d3 f5 bo bc dc e8 2850 4e 33354 a |
| a7 976073 le 062441 la b8 3882649 fl 2641 | a7 976073 1e 646244 la bs 388299942641 |
|  | ad $45469227506 d 2 f 8 \mathrm{c}$ a0 a5 7d db d5 95 3b |
| 758 b3 4086 ac 1d f7 30376 b e4 88 d9 e7 89 | 7 cs 9 c 4086931 d 43 co 37 6b e4 88 b2 e7 89 |
| el 1 lb 83494 c 3 f f8 fe $8 \mathrm{~d} 53 \mathrm{aa} 90 \mathrm{ca} \mathrm{d8} 8561$ | el lb $83494 \mathrm{c} 3 \mathrm{ff8} \mathrm{fe} 8 \mathrm{~d} \mathrm{fb} 8190 \mathrm{ca}$ d8 8561 |
|  | $207170 \mathrm{a4} 6 \mathrm{cc}$ da $95 \mathrm{5b} \mathrm{cb} 9 \mathrm{bb} 25 \mathrm{c} 2$ be e5 2 dd 52 |
| 59 a 674 d 2 e6 f4 b4 c0 d1 $66 \mathrm{af} \mathrm{c2} 39 \mathrm{lb} 63 \mathrm{~b} 6$ |  |
| Substitutions $g$ and $g^{\prime}$ differ in 63 values (differing positions are in bold). |  |
| Sequence of 36 transpositions is converting S-box $g$ to $g^{\prime}$ :$\begin{aligned} & (6 e, b 7),(f b, 53),(d a, 2 b),(c 5, b 5),(d b, 69),(93, a c),(99, b d),(f 1,68),(81, a b),(1,7 c),(5,24),(a 0,79), \\ & (6,98),(d 3,7 a),((b b, d 0),(c 8,58),(2 a, 30),(b 5,91),(70,67),(9 c, b 3),(29, b 4),(b 2, d 9),(19, a),(35, a), \\ & (6 d, 55),(54, e 6),(b d, 0),(f 5,9 f),(24,63),(43, f 7),(79, a 3),(94,9 f),(0,64),(30, c 0),(2 d, 6 c),(d 0, c 2) . \end{aligned}$ |  |

Table 7.

| Original s-box $g$ of state standard of the Republic of Belarus «BelT) | One of the new S-boxes $g^{\prime}$ that we have constructed using our algorithms |
| :---: | :---: |
| $\begin{gathered} \delta_{g}=26 / 128, p_{g}=8 / 256, \overline{\lambda_{g}}=6, \\ r_{g}=3, r_{g}^{(3)}=441 \end{gathered}$ | $\begin{gathered} \delta_{g^{\prime}}=24 / 128, p_{g^{\prime}}=6 / 256, \overline{\lambda_{g^{\prime}}}=7, \\ r_{g^{\prime}}=3, r_{g^{\prime}}^{(3)}=441 \end{gathered}$ |
| b1 94 ba c8 a 8 f5 3b 366 d ( 08 e 58 4a 5d e4 | b1 17 0 c8 a 8 f5 3b 36 6d ba 8 e 58 4a 5d e4 |
| 854 fa 9d 1b b6 c7 ac 25 2e 72 c2 2 fd ce d | 854 fa 9d 1b 3f c7 ac 25 2e 72 c2 be fd ce d |
| 5 b e3 d6 $1217 \mathrm{b9} 6181$ fe 6786 ad 716 bb 89 b | 5 b e3 d6 12 2 b9 6181 fe 6786 ad 71 6b 89 |
| 5 c b0 c0 ff $33 \mathrm{c} 356 \mathrm{~b} 835 \mathrm{c} 4 \mathrm{~S}^{\text {ae d8 e0 }} 7 \mathrm{ff} 99$ | 5 c b0 c0 ff 33 c3 56 b8 $35 \mathrm{c} 4 \mathrm{~S}^{5} \mathrm{ae}$ d8 e0 7f 99 |
| e1 2b dc 1a e2 8257 ec 703 fcc f0 95 ee 8d f1 | e1 2 b dc 1a e2 b6 57 ec 701 ecc f0 95 ee 23 fl |
| c1 ab 7638 9f e6 78 ca f7 c6 f8 60 d5 bb 9c 4 f | c1 ab 7638 bf e6 78 ca f7 c6 f8 60 d5 bb 9c 4 f |
| f3 3c 657 b 637 c 306 a dd 4 e a7 799 e b2 3 d 31 | f3 3c $657 \mathrm{7b} 637 \mathrm{c} 30 \mathrm{6a}$ dd 4 e a7 79 9e b2 3d 2 d |
| $3 \mathrm{e} 98 \mathrm{b5} 6 \mathrm{e} 27 \mathrm{~d} 3 \mathrm{bc}$ cf 59 1e 18 if $4 \mathrm{c} 5 \mathrm{5a}$ b7 93 | $3 \mathrm{e} 98 \mathrm{b5} 6 \mathrm{e} 27 \mathrm{~d} 3$ bc cf 598218 if $4 \mathrm{c} 5 \mathrm{5a}$ b7 93 |
| e9 de e7 2c 8f c fa6 2 ld db $49 \mathrm{f4} 6 \mathrm{ff} 739647$ | e9 de e7 2c 8f c fl 731 db 49 f 46 ff 73961 ld |
|  | $6 \mathrm{a6} 5316$ ed 247 al 3739 cb a3 83 3 a9 8b f6 |
| 92 bd 9 l 1 c e5 d1 $41115445 \mathrm{fb} \mathrm{c} 95 \mathrm{5e} 4 \mathrm{~d}$ e f2 |  |
| 682080 aa $227 \mathrm{7d} 642 \mathrm{fl} 2687 \mathrm{f9} 3490405511$ | 682080 aa 227 d 64 da 2647 f9 3490405511 |
| be 32971343 fc 9 a 48 aO 2 a 88 ff 19 4b 9 al | $9432971343 \mathrm{fc} 9 \mathrm{a} 48 \mathrm{a0} 2 \mathrm{a} 885 \mathrm{ff} 19 \mathrm{4b} 9 \mathrm{al}$ |
| 7 e cd a4 d0 1544 af 8 c a5 8450 bf 66 d2 e8 8a | 7 ecd a 4 d0 1544 af 8 c a5 84509 f 66 d 2 e8 8a |
| a2 d7 465242 as df b3 6974 c5 51 eb 232921 | a2 d7 465242 a 8 df b3 6974 c 551 eb 8 d 2921 |
|  | d4 ef d9 b4 3a 622875911410 ea 776 cc 2 f 87 |
| Substitutions $g$ and $g^{\prime}$ differ in 23 values (differing positions are in bold). |  |
| ```Sequence of }14\mathrm{ transpositions is converting S-box g}\mathrm{ to }\mp@subsup{g}{}{\prime}\mathrm{ : (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 $g^{\prime}$ that we have constructed using our algorithms |
| :---: | :---: |
| $\begin{gathered} \delta_{g}=28 / 128, p_{g}=12 / 256, \overline{\lambda_{g}}=6, \\ r_{g}=3, r_{g}^{(3)}=441 \end{gathered}$ | $\begin{gathered} \delta_{g^{\prime}}=24 / 128, p_{g^{\prime}}=6 / 256, \overline{\lambda_{g^{\prime}}}=7, \\ r_{g^{\prime}}=3, r_{g^{\prime}}^{(3)}=441 \end{gathered}$ |
| a3 d7 $983 \mathrm{f8} 48 \mathrm{f6}$ f4 b3 21157899 b1 af f9 | a3 7f db 83804853 da b3 de 159 ab 5 d b1 ee f9 |
| e7 2d 4d 8a ce 4c ca 2e 5295 d9 1e 4 e 384428 | c4 2d 4d 5f ce 99 ca 977195 d 1e 4e 497028 |
| a df 2 a0 17 f1 606812 b7 7a c3 e9 fa 3d 53 | 89342 a0 17 f1 f0 6812 b7 22 4c e9 fa 98 e6 |
| 9684 6b ba f2 63 9a 197 c ae e5 f5 f7 16 6a a2 | 9684 e ba f2 6360197 c ae 2f f5 f7 8f 6a a2 |
| 39 b 67 b f c1 9381 lb ee b4 1a ea d0 912 f b8 | 6 e b6 36 f c1 9381 lb af b4 1a ea d0 91 e 5 b 8 |
| 55 b9 da 853 f 41 bf e0 5a 58805 f 66 b d8 90 | 55 b 9 d 7853 f 41 bf d4 5a $5892 \mathrm{8a} 66$ b d8 90 |
|  | 4f d5 f6 7e 3366656945009456 6d 3d 9b 76 |
| $97 \mathrm{fc} \mathrm{b2} \mathrm{c2} \mathrm{b0} \mathrm{fe} \mathrm{db} 20$ e1 eb d6 e4 dd 47 4a 1d | e2 fc b2 c2 29 fe 8b 20 e1 eb bb e4 7747 4a 3 |
| 42 ed $9 \mathrm{e} 6 \mathrm{e} 49 \mathrm{3c}$ cd 4327 d 278 d 4 de c7 6718 | 42 ed 9e 3938 c3 cd 4327 d2 744421 c7 6718 |
| 89 cb 301 f 8 d c6 8f aa c8 74 dc c9 5d 5c 31 a4 | 9f 6b 30 1f 72 c6 16 f3 6474 dc c9 3c 5c 31 a4 |
|  |  |
| $34 \mathrm{4b} 1 \mathrm{c} 73 \mathrm{~d} 1 \mathrm{c} 4 \mathrm{fd} 3 \mathrm{~b}$ cc fb 7f ab e6 3e 5b a5 | e7 4b 1c $73 \mathrm{~d} 1 \mathrm{f4} \mathrm{fd} 3 \mathrm{~b}$ cc fb df ab a 3e 5 b a5 |
| ad 4239 c 145122 f0 2979717 la ff 8c e e2 | ad 423 9c 14512 lb 78 b0 79 cb a7 ff 8c 52 2e |
| c ef bc 72756 f 37 al ec d3 8e $628 \mathrm{8b} 8610$ e 8 | c ef bc 8d 756 f 37 a1 ec d3 7a 629 aa 13 e8 |
| 87711 be 924 ff 24 c 53236 9d cf f3 a6 bb ac | 8 dd 11 be f8 3524 c5 32 7b 9d cf 86 a6 d6 7d |
| 5 e 6 c a9 135725 b5 e3 bd a8 3a 13559 2a 46 | 5 e 6 c a9 105725 b5 e3 bd a8 3a 10559 2a 46 |

Substitutions $g$ and $g^{\prime}$ differ in 89 values (differing positions are in bold).
Sequence of 58 transpositions is converting S-box $g$ to $g^{\prime}$ :
$(d 7,7 f),(9, d b),(f 8,80),(f 6,53),(f 4, d a),(21, d e),(78,9 a),(99,5 d),(a f, e e),(e 7, c 4),(8 a, 5 f),(4 c, 5 d)$, $(2 e, 97),(52,71),(d 9, d),(38,49),(44,70),(a, 89),(d f, 34),(60, f 0),(7 a, 22),(c 3,5 d),(3 d, 98),(53, e 6)$, $(6 b, e),(9 a, f 0),(e 5,2 f),(16,8 f),(39,6 e),(7 b, 36),(d a, 7 f),(e 0, d 4),(80,92),(35,4 f),(c 0, e 6),(a 7,7 e)$, $(97, e 2),(b 0,29),(d b, 8 b),(d 6, b b),(d d, 77),(1 d, 3),(3 c, 5 d),(d 4,70),(89,9 f),(c b, e),(8 d, 72),(a a, f 3)$, (c8,64), (9f,e6), (2b,8e), (7d, ac), ( $34, c 4$ ), (c4,7f), $(22,8 e),(71, e),(86, f 3),(10,13)$.

Table 9.

| Original involutive S-box $g$ of block cipher «Khazad-0» | One of the new involutive S-boxes $g^{\prime}$ that we have constructed using our algorithms |
| :---: | :---: |
| $\begin{gathered} \delta_{g}=34 / 128, p_{g}=8 / 256, \overline{\lambda_{g}}=7, \\ r_{g}=3, r_{g}^{(3)}=441 \end{gathered}$ | $\begin{gathered} \delta_{g^{\prime}}=24 / 128, p_{g^{\prime}}=6 / 256, \overline{\lambda_{g^{\prime}}}=7, \\ r_{g^{\prime}}=3, r_{g^{\prime}}^{(3)}=441 \end{gathered}$ |
| a7 d3 e6 71 d0 ac 4d 79 3a c9 91 fc 1e 4754 bd | e2 98 2d d4 8b ac 7f 79 3a dc 75 fc 1e 4754 |
| 87 c a5 7 a fb 63 b 8 dd d 4 e5 b3 c5 be a9 88 c c 22 | 8 c a7 $7 \mathrm{a} \mathrm{fb} 63 \mathrm{~b} 8 \mathrm{b9}$ bf e5 b3 c5 be 85 d 0 c c a 2 |
| 39 df 29 da 2 b a8 cb 4c 4b 22 aa $244170 \mathrm{a6}$ f9 | cb a5 29 da 2b 91 f2 4c ba 22 b2 2441 |
|  |  |
| 675 c 5548 e 52 ea 42 5b 5d 305851593 c 4 e | 675 c 5548 e 52 ea 42 df 5 d ab 6c 51593 c 4 e |
| 388 l 7214 e7 c6 de $508 \mathrm{8e} 92 \mathrm{~d} 7793459 \mathrm{la}$ ce | 388 al 7214 e7 c6 de $508 \mathrm{el} 92 \mathrm{~d} 1775 \mathrm{5b} 459 \mathrm{al} 32$ |
|  |  |
| db cf ec cc c1 a1 c0 d6 1d f4 61 3b 10 d8 68 ao | db cf ec cc c1 1c c0 d6 3b f4 61 |
|  |  |
| 3290 af 19 a3 f7 739 d 1574 ee ca 9 f ¢ 1 lb 75 |  |
| $86849 \mathrm{c} 4 \mathrm{a} 971 \mathrm{la} 65 \mathrm{f6}$ ed 9 bb 2683 eb 6 f 81 | $86849 \mathrm{cl} 4 \mathrm{al} 1 \mathrm{la} 65 \mathrm{f6}$ ed d7 bb 2083 eb b0 81 |
|  |  |
|  |  |
| Substitutions $g$ and $g^{\prime}$ differ in 88 values (differing positions are in bold). |  |
|  |  |
| Sequence of 30 pairs transpositions is converting S-box $g$ to $g^{\prime}$ : |  |
|  |  |
|  |  |
|  |  |

Table 10.


