Generation of 8-bit S-Boxes having almost optimal cryptographic properties using smaller 4-bit S-Boxes and finite field multiplication

Reynier Antonio de la Cruz Jiménez

Institute of Cryptography, Havana University, Cuba
djr.antonio537@gmail.com

Abstract. Substitution boxes (S-Boxes) as the only component of nonlinearity in modern ciphers, play a crucial role in the protection against differential, linear and algebraic attacks. The construction of S-Boxes with cryptographic properties close to optimal is an open problem. In this article we propose a new construction for generating such 8-bit permutations with nonlinearity up to a value of 108.

Keywords: S-Box, permutations, vectorial Boolean functions, finite field multiplication.

1 Introduction and Motivation

Modern symmetric ciphers contain one or more cores of nonlinear operations. Often these cores are n to m Boolean mappings, called S-Boxes. Among the whole set of S-Boxes the bijective ones (also-called permutations) are particularly interesting. In the design of many block ciphers, S-Boxes are often chosen to bring confusion into ciphers. The security of these ciphers is then strongly dependent on the cryptographic properties of the S-Boxes, for this reason S-Boxes are carefully chosen and the criteria or algorithm used to build them are usually explained and justified by the designers of prospective algorithms.

The known methods for the construction of S-Boxes can be divided into three main classes: algebraic constructions, pseudo-random generation and heuristic techniques. Each approach has its advantages and disadvantages respectively [25]. The inversion in the finite field with 2^n elements is a good method for generating robust S-Boxes. With respect to cryptographic strength against differential and linear attacks, the inversion in the finite field, used in block ciphers like AES/Rijndael [35], Camellia [2], ARIA [30], HyRAL [23], Hierocrypt [37] has the best known values. Nevertheless, further analysis has shown that this approach leads to existence of a system of polynomial equations with low degree and "potential vulnerability" of the cipher to algebraic attacks [13]. It should be noted that the problem of solving generic systems of polynomials equations over finite fields is NP-hard [16] already for quadratic ones, but there are obviously instances where it is not the case. This discrepancy combined with the

fundamental complexity of rigourous analysis sometimes leads to certain controversy regarding the validity of the so-called algebraic attacks. However, from a designer's perspective, it is better to choose an S-Box (or several S-Boxes) that meets specific (see, Section 4) algebraic, linear and differential requirements. This kind of permutations has been used in the design of cryptographic algorithms like BelT [48], Kuznyechik [20] and Kalyna [38] and compared with the inversion function, which can be described by polynomial equations of degree 2, their main advantage (in terms of its cryptographic properties) is a description by a system of 441 polynomials equations of degree 3.

Motivated by specialist's work [8] of Luxembourg's university Alex Biryukov, Léo Perrin and Aleksei Udovenko on decomposition of the S-Box used in the block cipher Kuznyechik, hash function Streebog [21] and CAESAR first round candidate stribobr1 [45] we propose a new construction for generating cryptographically strong 8-bit S-Boxes using smaller ones and finite field multiplication.

In cryptography, it is not uncommon to build an S-Box from smaller ones, usually an 8-bit S-Box from several 4-bit S-Boxes. For example, S-Boxes used in CLEFIA [49], Iceberg [47], Khazad [4], Whirlpool [5] and Zorro [18] are permutations of 8 bits based on smaller S-Boxes. In many cases, such a structure is used not only to allow an efficient implementation of the S-Box in hardware or using a bit-sliced approach, but also to protect S-Boxes implemented in this way against side-channel attacks. In this work we do not investigate the implementation cost of our S-Boxes in hardware. We focus on some cryptographic properties of those S-Boxes obtained by our method.

This article is structured as follows: In Section 2 we give the basic definitions. In Section 3 we present a new method for constructing S-Boxes having almost optimal cryptographic properties. In Section 4 we present an algorithm for finding cryptographically strong 8-bit permutations. A summary of some available recent methods for the generation of permutations with strong cryptographic properties and some related problem with these methods are discussed in Section 5. New S-boxes with stronger properties, generated by our construction are given in Section 6. Our work is concluded in Section 7.

2 Definitions and Notations

Let V_n be the n-dimensional vector space over the field GF(2), by $S(V_n)$ we denote the symmetric group on set of 2^n elements. The finite field of size 2^n is denoted by GF(2^n), where GF(2^n)=GF(2)[ξ]/g(ξ), for some irreducible polynomial $g(\xi)$ of degree n. We use the notation $\mathbb{Z}/2^n$ for the ring of the integers modulo 2^n. There are bijective mappings between $\mathbb{Z}/2^n, V_n$ and GF(2^n) defined by the correspondences:

$$\left[a_{n-1} \cdot 2^{n-1} + \ldots + a_0\right] \leftrightarrow (a_{n-1}, \ldots, a_0) \leftrightarrow \left[a_{n-1} \cdot \xi^{n-1} + \ldots + a_0\right].$$

Using these mapping in what follows we make no difference between vectors of V_n and the corresponding elements in $\mathbb{Z}/2^n$ and GF(2^n).

Also in the rest of this article, we shall use the following operations and notations :

$a\|\|b$	- concatenation of the vectors a, b of V_l, i.e. a vector from V_{2l} ;
0	- the null vector of V_l ;
$\oplus$	- bitwise eXclusive-OR. Addition in GF(2^l);
$< a, b >$	- the scalar product of vectors $a = (a_{l-1}, \ldots, a_0), b = (b_{l-1}, \ldots, b_0)$ of V_l and is equal to $< a, b >= a_{l-1}b_{l-1} \oplus \ldots \oplus a_0 b_0$;
$w_H(a)$	- the Hamming weight of a binary vector $a \in V_l$, i.e. the number of its nonzero coordinates;
$\otimes$	- finite field multiplication ;
$F \circ G$	- a composition of mappings, where G is the first to operate;
F^{-1}	- the inverse transformation to some bijective mapping F.

Now, we give some basic definitions, which usually are used as cryptographic tools for evaluating the strength of S-Boxes with respect to linear, differential and algebraic attack. For this purpose, we consider an n-bit S-Box Φ as a vector of Boolean functions:

$$\Phi = (f_{n-1}, \ldots, f_0), f_i : V_n \to V_1, i = 0, 1, \ldots n-1. \tag{1}$$

For some fixed $i = 0, 1, \ldots n-1$, every Boolean function f_i can be written as a sum over V_1 of distinct t-order products of its arguments, $0 \leq t \leq n-1$; this is called the algebraic normal form of f_i. Functions f_i are called coordinate Boolean functions of the S-Box Φ and it is well known that most of the desirable cryptographic properties of Φ can be defined in terms of their linear combinations. S-Box coordinate Boolean functions of Φ and all their linear combinations are referred to as the S-Box component Boolean functions.

Definition 1. For each vector $a \in V_n$ the The Walsh-Hadamard transform $W_f(a)$ of the n-variable Boolean function f is defined as

$$W_f(a) = \sum_{x \in V_n} (-1)^{f(x) \oplus < a, x >}. \tag{2}$$

Definition 2. The nonlinearity N_f of the n-variable Boolean function f is defined as

$$N_f = \min_{g \in \mathcal{A}_n} w_H(f \oplus g), \tag{3}$$

where $\mathcal{A}_n$ is the set of all n-variable affine Boolean functions and $w_H(f \oplus g)$ is the Hamming weight of the n-variable Boolean function $f \oplus g$. The nonlinearity N_f can be expressed as follows:

$$N_f = 2^{n-1} - \frac{1}{2} \max_{a \in V_n \setminus \{0\}} |W_f(a)| \tag{4}$$

Definition 3. The autocorrelation transform, taken with respect to $a \in V_n$, of an n-variable Boolean function f is denoted by $\hat{r}_f(a)$ and defined as:

$$\hat{r}_f(a) = \sum_{x \in V_n} (-1)^{f(x) \oplus f(x \oplus a)}. \tag{5}$$

Definition 4. The absolute indicator of the n-variable Boolean function f, denoted by $AC(f)_{max}$ is defined as

$$AC(f)_{max} = \max_{a \in V_n \setminus \{0\}} |\hat{r}_f(a)|. \tag{6}$$

Definition 5. For $a, b \in V_n$ the Walsh transform $W_{\Phi}(a, b)$ of an n-bit S-Box Φ is defined as

$$W_{\Phi}(a, b) = \sum_{x \in V_n} (-1)^{<b, \Phi(x)> \oplus <a, x>}. \tag{7}$$

Definition 6. The nonlinearity of an n-bit S-Box Φ, denoted by N_{Φ}, is defined as

$$N_{\Phi} = \min_{a \in V_n \setminus \{0\}} \{N_{a_{n-1} f_{n-1} \oplus \ldots \oplus a_0 f_0}\}, \tag{8}$$

where $N_{b_{n-1} f_{n-1} \oplus \ldots \oplus b_0 f_0}$ is the nonlinearity of each of the component Boolean functions excluding the zero one.
The nonlinearity N_{Φ} of an arbitrary n-bit S-Box Φ can be calculated as follows

$$N_{\Phi} = 2^{n-1} - \frac{1}{2} \cdot \max_{a \neq 0, b \in V_n} |W_{\Phi}(a, b)|. \tag{9}$$

From a cryptographic point of view S-Boxes with small values of Walsh coefficients offer better resistance against linear attacks.

Definition 7. The differential uniformity of an n-bit S-Box Φ, denoted by δ_{Φ}, is defined as

$$\delta_{\Phi} = \max_{a \neq 0, b \in V_n} \delta(a, b), \tag{10}$$

where $\delta(a, b) = |\{x \in V_n | \Phi(x \oplus a) \oplus \Phi(x) = b\}|$.

The resistance offered by an S-Box against differential attacks is related by the highest value of δ, for this reason S-Boxes must have a small value of δ-uniformity for a sufficient level of protection against this type of attacks.

Definition 8. The maximal absolute indicator and the sum-of-squares indicator of an n-bit S-Box Φ, denoted by $AC(\Phi)_{max}$ and $\sigma(\Phi)$, respectively , are defined as

$$AC(\Phi)_{max} = \max_{a \in V_n \setminus \{0\}} |\hat{r}_f(a_{n-1} f_{n-1} \oplus \ldots \oplus a_0 f_0)|, \tag{11}$$

$$\sigma(\Phi) = \sum_{a \in V_n} \hat{r}_f^2(a). \tag{12}$$

Any n-bit S-box Φ should have low autocorrelation in order to improve the avalanche effect of the cipher [15], for this reason, the absolute indicators of the component Boolean functions of the S-box should be as small as possible. In other words, the parameter $AC(\Phi)_{max}$, should be as small as possible.

The algebraic degree of the Boolean functions $f : V_n \to V_1$, denoted by $\deg f$, is the maximum order of the terms appearing in its algebraic normal form.

Definition 9. The minimum degree of an S-Box Φ, denoted by $\deg(\Phi)$, is defined as

$$\deg(\Phi) = \min_{a \in V_n \setminus \{0\}} \{\deg(a_{n-1} f_{n-1} \oplus \ldots \oplus a_0 f_0)\}. \tag{13}$$

In order to resist low order approximation [19],[34] and higher order differential attacks [29] any n-bit S-Box Φ should have a minimum degree as high as possible.

Proposition 1 *For any 8-bit S-Box Φ we have,* $1 \leq \deg(\Phi) \leq 7$.

The annihilator of a Boolean function f with n variables is another Boolean function g with n variables such that $f \cdot g = 0$. For a given Boolean function f, the algebraic immunity $AI(f)$ is the minimum value d such that f or $f \oplus 1$ has a nonzero annihilator of degree d.

It is well known [10] that there are three kinds of definitions of the algebraic immunity for S-Boxes. At first, we present a concept of annihilating set [3]:

Definition 10. Let U be a subset of V_{2n}, then

$$\{p \in GF(2)[z_1, \ldots, z_{2n}] \Big| p(U) = 0\}$$

is the annihilating set of U.

Definition 11. The algebraic immunity of U is defined as

$$AI(U) = \min \Big\{ \deg p \;\Big|\; 0 \neq p \in GF(2)[z_1, \ldots, z_{2n}], p(U) = 0 \Big\}.$$

Definition 12. Let Φ be any n-bit S-Box, and define

$$AI(\Phi) = \min \Big\{ AI(\Phi^{-1}(a)) \Big| a \in V_n \Big\} \tag{14}$$

as the basic algebraic immunity of Φ,

$$AI_{gr}(\Phi) = \min \Big\{ \deg p \;\Big|\; 0 \neq p \in GF(2)[z_1, \ldots, z_{2n}], p(gr(\Phi)) = 0 \Big\} \tag{15}$$

as the graph algebraic immunity of Φ, where $gr(\Phi) = \{(x, \Phi(x)) | x \in V_n\} \subseteq V_{2n}$,

$$AI_{comp}(\Phi) = \min_{a \in V_n \setminus \{0\}} \Big\{ AI(a_{n-1} f_{n-1} \oplus \ldots \oplus a_0 f_0) \Big\} \tag{16}$$

as the component algebraic immunity of Φ.

For any n-bit permutation Φ the bounds of these three algebraic immunity definitions(explained in [3]) are the following , $AI(\Phi) \leq 1$(so there is no significance in analyzing the basic algebraic immunity of an S-Box), $AI_{gr}(\Phi) \leq d_{gr}$, where d_{gr} is the minimum positive integer which satisfies $\sum_{i=0}^{d_{gr}} \binom{2n}{i} > 2^n$ and $AI_{comp}(\Phi) \leq \lceil \frac{n}{2} \rceil$.

To the best of our knowledge, there is no literature that proposes any attack given the basic and component algebraic immunity rather than the graph algebraic immunity [7], [13]. Thus we focus on the graph algebraic immunity of

S-Box Φ – $AI_{gr}(\Phi)$ and also on the parameter $t_{\Phi}^{(AI_{gr}(\Phi))}$ referred to as the number of all the independent equations in input and output values of the S-Box Φ, i.e., equations of the form $p(x, \Phi(x)) = 0\ \forall x \in V_n$.

The level of protection provided by an S-Box Φ against algebraic attacks is measured by the parameters, $AI_{gr}(\Phi)$ and $t_{\Phi}^{(AI_{gr}(\Phi))}$, respectively.

Proposition 2 *([11]). For any 8-bit S-Box Φ we have $AI_{gr}(\Phi)) \leq 3$.*

Definition 13. An element $a \in V_n$ is called a fixed point of an n-bit S-Box Φ if $\Phi(a) = a$.

An n-bit substitution Φ must have no fixed point, i.e., $\Phi(a) \neq a, \forall a \in V_n$. Many ciphers have used the above mentioned notion for increasing resistance against statistical attacks.

Definition 14. Two n-bit S-Boxes Φ_1 and Φ_2 are affine/linear equivalent if there exist a pair of invertible affine/linear permutation $A_1(x)$ and $A_2(x)$, such that $\Phi_1(x) = A_2 \circ \Phi_2 \circ A_1(x)$.

The affine/linear equivalence can be used to prevent the appearance of fixed points during generation of some n-bit S-Box.

3 New Construction

Let $n = 2k$, where $k \geq 2$. Choosing the permutation polynomial (PP) $\tau_{2^k-2}(x) = x^{2^k-2}$ over GF(2^k) and arbitrary permutations $h_i \in S(V_k)$, $i = 1, 2$, we construct the following n-bit vectorial Boolean function $\pi : V_{2k} \to V_{2k}$ as follows

Construction of π

For the input value $(l\|r) \in V_{2k}$ we define the corresponding output value $\pi(l\|r) = (l_1\|r_1)$ where,

$$l_1 = \begin{cases} h_1(l), & \text{if } r = 0; \\ \tau_{2^k-2}(l \otimes r), & \text{if } r \neq 0; \end{cases}$$

$$r_1 = \begin{cases} h_2(r), & \text{if } l_1 = 0; \\ l_1 \otimes \tau_{2^k-2}(r), & \text{if } l_1 \neq 0. \end{cases}$$

Taking into account that block ciphers based on Substitution-Permutation Networks need the inverse substitution to π for the decryption process we also give the construction of π^{-1}.

Construction of π^{-1}

For the input value $(l_1\|r_1) \in V_{2k}$ we define the corresponding output value $\pi^{-1}(l_1\|r_1) = (l\|r)$ where,

$$r = \begin{cases} h_2^{-1}(r_1), & \text{if } l_1 = 0; \\ l_1 \otimes \tau_{2^k-2}(r_1), & \text{if } l_1 \neq 0. \end{cases}$$

$$l = \begin{cases} h_1^{-1}(l_1), & \text{if } r = 0; \\ \tau_{2^k-2}(l_1 \otimes r), & \text{if } r \neq 0. \end{cases}$$

It should be noted, that the proposed construction is different from decomposition obtained in [8] and S-Boxes generated by our construction can achieve better properties (see, Section 6).

4 Generating 8-bit permutations from smaller ones and finite field multiplication

In this work the substitution having almost optimal cryptographic properties refers to a permutation with

1. Absence of fixed points;
2. Maximum value of minimum degree;
3. Maximum algebraic immunity with the minimum number of equations;
4. Minimum value of δ-uniformity limited by parameter listed above;
5. Maximum value of nonlinearity limited by parameter listed above.

For example, for $n = 8$ an almost optimal permutation π without fixed points has:

- $\deg(\pi) = 7$;
- $AI_{gr}(\pi) = 3$ with $t_{\pi}^{(3)} = 441$;
- $\delta_{\pi} \leq 8$;
- $N_{\pi} \geq 100$.

For $n = 8$ in correspondence with the suggested construction of π we need to construct; the finite field $\mathrm{GF}(2^4)$, two 4-bit permutations $h_1, h_2 \in S(V_4)$ and the PP $\tau_{14}(x) = x^{14}$ over $\mathrm{GF}(2^4)$. It is well known [43] that there are only three irreducible polynomials of degree 4 over GF(2), $g_1(\xi) = \xi^4 + \xi + 1$, $g_2(\xi) = \xi^4 + \xi^3 + 1$ and $g_3(\xi) = \xi^4 + \xi^3 + \xi^2 + \xi + 1$. In what follows, for the sake of simplicity, we shall work in $\mathrm{GF}(2^4)$=GF(2)$[\xi]/g_1(\xi)$. Thus, π can be written as follows

$$\pi(l\|r) = (l_1\|r_1), \tag{17}$$

where,

$$l_1 = \begin{cases} h_1(l), & \text{if } r = 0; \\ (l \otimes r)^{14}, & \text{if } r \neq 0; \end{cases}$$

$$r_1 = \begin{cases} h_2(r), & \text{if } l_1 = 0; \\ l_1 \otimes r^{14}, & \text{if } l_1 \neq 0. \end{cases}$$

The main advantage of our construction is that it allows to perform a search based on random generation of 4-bit permutations for finding 8-bit S-Boxes having almost optimal cryptographic parameters. For this purpose we propose

the following generic algorithm. The basic steps of the algorithm for generating such permutations are described as follows:

Step 1. Generate randomly two 4-bit permutations $h_1, h_2 \in S(V_4)$;

Step 2. For already generated 4-bit permutations $h_1, h_2 \in S(V_4)$ construct the 8-bit permutation π according to (17);

Step 3. Test the permutation π for all criteria 1-5. If π satisfies all of them except criterion 1 then go to **Step 4**. Otherwise repeat **Step 1**.

Step 4. Apply affine/linear equivalence to π in order to achieve the required property 1.

Step 5. Output. A permutation π with the desired properties.

5 A discussion with respect to some recent methods

In [28] Kazymyrov *et al.* presented a method for generating cryptographically strong S-Boxes called Gradient descent method. The proposed method is based on the already known [27] method of gradient descent, but was adopted for the vectorial case. It allows to generate permutations for symmetric cryptography primitives providing a high level of resistance to differential, linear and algebraic attacks. The best result obtained in this work (in terms of its cryptographic properties) was a permutation without fixed points with the following properties

- minimum degree — 7;
- algebraic immunity — 3 (with 441 equations);
- 8 — uniform;
- nonlinearity — 104.

Moreover, in the same work was raised the following open question: *Does there exist an 8-bit permutation with algebraic immunity 3 and nonlinearity more than 104?*.

In [25] Ivanov *et al.* presented a method for generating S-Boxes with strong cryptographic properties based on Modified Immune Algorithm referred as the "*SpImmAlg*". The authors propose an S-Box generation technique using a special kind of artificial immune algorithm, namely the clonal selection algorithm, combined with a slightly modified hill climbing method for S-Boxes. The best result obtained in this work (in terms of its cryptographic properties) was a large set of permutations without fixed points with the following properties

- minimum degree — 7;
- algebraic immunity — 3 (with 441 equations);
- 6 — uniform;
- nonlinearity — 104.

In [31] Menyachikhin presented new methods for generating S-Boxes having almost optimal cryptographic properties called the Spectral-linear and spectral-difference methods [31]. The proposed methods are based on using linear and

differential spectrum for iteratively improving a given S-Box with respect to certain cryptographic properties. These methods multiply the given S-Box with some special permutations and the resulting S-Box is then stronger. The above mentioned methods can also be applied for generating involutive S-Boxes and orthomorphisms with strong cryptographic properties. The best results obtained by A. Menyachikhin using both methods (in terms of its cryptographic properties) were S-Boxes without fixed points with the following properties

- minimum degree — 7;
- algebraic immunity — 3 (with 441 equations);
- 6 — uniform;
- nonlinearity — 104.

All these results show us that finding cryptographically strong 8-bit S-Boxes with algebraic immunity 3 and nonlinearity more than 104 is a difficult task, moreover at the time of writing no counterexample was found in the public literature. In the next section we show that our construction produce 8-bit permutations with the best cryptographic properties reported for nonlinearity and algebraic immunity respectively.

6 Practical results

Based on an exhaustive search over all affine equivalence classes for 4-bit S-Boxes [6,14,42] was checked that for 8-bit permutations constructed according to (17) the following properties holds:

$$100 \leq N_\pi \leq 108, 6 \leq \delta_\pi \leq 18.$$

The algorithm described in the previous section was implemented in SAGE [44] but with the following slight modification, $h_1 = h_2 = h$. Furthermore, for the sake of simplicity 500 random generated 4-bit S-Boxes h were stored in a list. Then for each 4-bit substitution of this list we applied the rest of the steps specified in our algorithm. After several minutes 417 permutations having almost optimal cryptographic parameters were generated. A total of 56 generated permutations have algebraic immunity — 2. The remaining 27 have differential uniformity strictly greater than 8. In this search we did not find a 4-bit substitution h for which the resulting π has $N_\pi = 108$. Then, we decide generate 2^{20} random 4-bit substitution h and abort the algorithm as soon as a permutation π with almost optimal cryptographic properties reaching a nonlinearity of 108 has been found. After 7hr 17mins on 2.3GHz Intel Core i3-6100U processor with 4GB RAM, we found the next 4-bit S-Box h=(0,1,e,9,f,5,c,2,b,a,4,8,d,6,3,7) for which π has almost optimal cryptographic properties with $N_\pi = 108$. So instead of trying to find a random 4-bit substitution h for which the almost optimal permutation π generated by our algorithm has the maximal possible nonlinearity it was decided to solve the problem from the other side. We started to pick in our construction some 4-bit S-Boxes $h_i, i = 1, 2$ from the well-known class

$$\left\{ x^s \middle| gcd(s, 15) = 1, s \in \mathbb{N} \right\}$$

of Permutations Polynomials (also-called Power Functions) [43] over GF(2^4) until the expected result was achieved for $h_1 = x^{13}$ and $h_2 = x^{11}$.

Our experiments show that not any pair of 4-bit S-Boxes can generate 8-bit permutations having almost optimal cryptographic parameters. Moreover, the cryptographic quality of those 8-bit permutations not always depended on the cryptographic properties of smaller 4-bit S-Boxes, for example, if we choose $h_1 = h_2 = \tau_{14}(x) = x^{14} \in S(V_4)$ in our construction then the resulting 8-bit permutation do not possess a high value of algebraic immunity, even when x^{14} has optimal properties in $S(V_4)$, i.e $N_{x^{14}} = 4, \delta_{x^{14}} = 4, \deg(x^{14}) = 3, AI_{gr}(x^{14}) = 2, r^{(2)}_{x^{14}} = 21$. But if now, $h_1 = h_2 =$(b, c, 2, 3, d, a, 7, 1, 4, 0, f, e, 5, 6, 9, 8) $\in S(V_4)$ which have $N_h = 0, \delta_h = 10, \deg(h) = 1, AI_{gr}(h) = 1, r^{(1)}_h = 1$, then, the substitution π generated by our construction is almost optimal. We can thus discard the idea that the strength of π against differential, linear and algebraic attacks relies only on the quality of each of its 4-bit S-Boxes. How to select the 4-bit components h_1, h_2 in such a way that the obtained 8-bit substitution π will be almost optimal (with respect to the chosen criteria) is an open question.

However, our method has been applied to a large number of random 4-bit permutations. As a result we have obtained a lot of new affine nonequivalent 8-bit permutations without fixed points with the following cryptographic parameters

- minimum degree — 7;
- algebraic immunity — 3 (with 441 equations);
- 6 and 8 — uniform;
- nonlinearity in range of 100 up to a value of 108.

In Table 1 we show four 8-bit S-Boxes π_1, π_2, π_3 and π_4. As it can be seen, our S-Boxes provide high level of protection against differential, linear and algebraic attacks.

In Table 2 two other S-Boxes π_5 and π_6 with strong cryptographic properties are showed. As it can be seen from the table our permutations compared with π_1 and π_2 demonstrate better properties. The S-Box π_5 was produced by our algorithm and permutation π_6 was obtained choosing in construction (17) the next PPs $h_1 = x^{13}, h_2 = x^{11} \in S(V_4)$ followed by application of an affine transformation to avoid fixed points.

Finaly, in Table 3 we compare our results with the state-of-the-art in design of cryptographically strong S-Boxes obtained by different available methods. In this table we have added three parameters. The first two are transparency order[39] denoted by τ_π and defined as:

$$\tau_\pi = \max_{b \in V_n} \Big(|n - 2w_H(b)| - \frac{1}{2^{2n} - 2^n} \sum_{a \in V_n \setminus \{0\}} \Big| \sum_{c \in V_n, w_H(c)=1} (-1)^{<c,b>} W_{\pi(x) \oplus \pi(x \oplus a)}(0, c) \Big| \Big),$$

and the Signal-to-Noise Ratio $SNR(DPA)(\pi)$[22], defined as follows

$$SNR(\pi) = n 2^{2n} \Big(\sum_{a \in V_n} \Big(\sum_{i=0}^{n-1} W_{f_i}(a) \Big)^4 \Big)^{-\frac{1}{2}},$$

where $f_i, i = 0, \ldots, 7$ are the coordinate Boolean functions of the S-Box π. These parameters quantify the resistance of an n-bit S-Box π to Differential Power Anallysis (DPA). The last one is the well-known robustness *to differential cryptanalysis* (see, e.g.[46]).

Table 1: Some 8-bit S-Boxes generated by our construction

S-Box π_1															
$\mathbf{N_{\pi_1} = 100}$, $\mathbf{\delta_{\pi_1} = 8}$, $\mathbf{\deg(\pi_1) = 7}$, $\mathbf{AI_{gr}(\pi_1) = 3}$, $\mathbf{t^{(3)}_{\pi_1} = 441}$															
1b	d4	6b	e6	a6	e4	96	59	29	94	69	19	2b	d6	5b	a4
47	88	d7	57	62	06	f6	f7	ff	31	c0	1e	c1	6f	54	ae
d0	0f	db	7a	75	b9	12	18	83	5f	d1	39	ce	51	cf	aa
af	58	23	cc	f2	a8	93	1d	45	3c	9b	0b	42	bb	ef	08
ea	d5	6d	14	60	41	53	f8	2c	36	80	79	f5	27	b1	cd
c9	d2	35	a5	f1	bf	4b	3d	ec	9d	01	cb	16	1c	4a	d8
64	32	04	33	e0	97	05	26	63	c2	55	81	48	20	d3	49
38	e9	07	7f	34	c4	b5	df	e3	e8	8e	30	1f	7e	de	e5
f3	9a	eb	fd	73	fb	e1	dd	5a	3f	90	9e	b7	b4	c8	4c
02	6c	72	ac	24	87	e2	a7	7c	8a	0d	17	76	43	c6	ad
b6	2f	9f	0a	bd	dc	6a	a1	f0	da	8b	37	86	d9	4e	fe
7d	0e	b8	03	40	82	66	6e	15	78	13	ed	44	2d	2a	f4
95	09	67	a2	70	b3	91	71	61	ca	e7	4d	50	89	3a	a9
21	8d	c5	25	9c	5d	bc	28	10	2e	7b	b0	ba	0c	99	74
5e	92	84	a3	fc	11	65	00	f9	68	ab	c7	fa	c3	b2	52
8c	85	ee	3e	3b	1a	a0	46	be	98	77	8f	5c	4f	56	22

S-Box π_2															
$\mathbf{N_{\pi_2} = 102}$, $\mathbf{\delta_{\pi_2} = 8}$, $\mathbf{\deg(\pi_2) = 7}$, $\mathbf{AI_{gr}(\pi_2) = 3}$, $\mathbf{t^{(3)}_{\pi_2} = 441}$															
a7	40	bd	2c	25	fd	09	6c	d8	91	f4	98	d1	b4	49	65
a2	5d	f1	b7	84	9f	46	1b	ea	6e	d9	28	c2	75	33	ac
92	69	8d	6a	1e	90	e7	8e	03	1d	77	fa	f9	93	74	e4
54	26	bb	96	82	89	2d	0b	b0	32	a4	1f	af	39	14	9d
f6	c4	72	76	be	7e	04	c0	b2	0c	7a	08	ba	cc	c8	b6
f3	d6	b5	3d	a6	f8	88	5e	eb	4d	70	c5	2e	13	9b	63
c6	4f	36	fc	9c	19	ca	85	b3	2f	d3	e5	56	aa	60	79
61	12	c7	4b	18	86	8c	9e	59	41	0a	cd	94	df	53	d5
35	7b	4a	21	06	16	6b	10	5a	5c	7d	37	6d	4c	27	31
00	bf	38	57	b8	68	6f	d0	e8	50	07	3f	d7	80	ef	87
64	99	83	c1	3a	e1	42	db	58	62	a3	20	78	b9	fb	1a
51	f0	0e	ab	24	71	a5	55	5b	7f	d4	da	81	2a	8f	fe
97	8b	44	8a	22	67	ce	45	01	23	a9	ed	ec	66	a8	cf
30	ad	ff	1c	a0	ee	e3	4e	b1	11	0d	f2	43	5f	bc	52
05	e2	c9	e0	3c	f7	29	cb	02	3e	de	17	15	f5	dc	2b
c3	34	7c	dd	9a	0f	a1	95	e9	73	ae	d2	3b	e6	47	48

S-Box π_3															
$\mathbf{N_{\pi_3} = 104}$, $\mathbf{\delta_{\pi_3} = 8}$, $\mathbf{\deg(\pi_3) = 7}$, $\mathbf{AI_{gr}(\pi_3) = 3}$, $\mathbf{t^{(3)}_{\pi_3} = 441}$															
38	90	19	14	3d	9d	30	ad	b9	29	b4	84	0d	a0	24	00
c0	2d	26	b3	63	db	95	b8	9e	fd	4e	68	f6	45	d0	0b
f8	1b	47	98	1a	de	df	c4	83	99	01	46	c5	5d	82	5c
93	aa	35	ff	42	22	ca	60	55	17	e8	dd	88	77	bd	9f
f1	d7	a3	c6	97	25	65	b2	11	86	40	e3	f2	34	51	74
ab	4b	f7	12	ac	02	e5	ae	59	f5	e7	10	49	5b	be	bc
9a	b1	72	67	58	fc	15	a4	d6	8e	e9	9b	4d	2a	3f	c3
31	9c	54	d4	3b	27	80	1c	48	73	a7	f3	bb	6f	ef	c8
a2	87	13	4c	21	f9	5f	d8	cb	ea	a6	b5	7e	32	6d	94
62	50	b0	8a	b6	dc	3a	6a	da	6c	e6	56	8c	06	3c	e0
c9	fa	85	75	f4	fe	f0	0a	8f	7b	0e	8b	04	71	81	7f
53	e1	c2	ed	ee	20	2f	ce	0c	e2	0f	cd	c1	2c	03	23
6b	66	d1	a1	cf	d9	70	16	c7	08	a9	78	bf	1e	6e	b7
5a	cc	e4	5e	8d	fb	ba	76	92	1f	41	a5	37	69	d3	28
09	7d	96	39	d5	07	af	d2	44	91	a8	3e	7a	43	ec	eb
89	36	61	2b	79	05	4a	7c	1d	64	4f	2e	33	18	52	57

S-Box π_4															
$\mathbf{N_{\pi_4} = 104}$, $\mathbf{\delta_{\pi_4} = 6}$, $\mathbf{\deg(\pi_4) = 7}$, $\mathbf{AI_{gr}(\pi_4) = 3}$, $\mathbf{t^{(3)}_{\pi_4} = 441}$															
c9	9b	0f	2e	01	b4	0e	94	20	9a	bb	00	95	21	b5	2f
99	79	32	9f	0d	d9	ad	d4	e6	eb	74	46	a0	3f	92	4b
78	89	0c	82	e9	ee	8e	07	0b	e2	60	6c	67	e5	6b	85
dc	25	a3	d8	3b	65	7b	5e	fd	c6	1e	bd	40	98	e3	86
50	96	5d	34	9e	61	69	ff	a2	3c	08	55	f7	c3	aa	cb
6d	43	c0	f1	41	33	31	72	b2	f3	02	c2	70	81	b0	83
f4	ac	af	5a	d2	8b	f5	59	f6	24	7e	d1	27	7d	88	03
8c	d5	9d	c5	df	52	58	8d	10	cf	0a	97	87	42	1a	48
b1	5c	91	47	36	bc	d6	8a	1b	2d	6a	fb	e0	a7	71	cd
3d	ca	cc	73	a8	dd	bf	75	b9	11	62	ae	17	64	db	06
45	ef	6f	ab	93	b8	c4	2b	44	d7	7c	13	57	fc	38	80
ba	66	63	29	7a	56	4a	2c	4f	35	1c	7f	30	19	53	05
e1	3a	f2	6e	4c	ea	9c	a6	54	18	76	84	d0	be	22	c8
28	1f	51	b6	77	8f	e7	f8	a9	de	68	39	90	26	c1	4e
a4	b3	fe	ec	a5	04	12	a1	5f	fa	16	e8	b7	5b	49	4d
15	f0	3e	1d	e4	37	23	d3	ed	09	14	2a	c7	da	f9	ce

Table 2: The best S-Boxes produced by our construction

S-Box π_5															
$\mathbf{N_{\pi_5} = 106}$, $\mathbf{\delta_{\pi_5} = 6}$, $\mathbf{\deg(\pi_5) = 7}$, $\mathbf{AI_{gr}(\pi_5) = 3}$, $\mathbf{t^{(3)}_{\pi_5} = 441}$															
96	24	63	c0	ab	4f	a3	6b	2c	47	ec	c8	08	e4	8f	87
25	bc	20	d4	82	ca	f4	48	68	ea	3e	1e	76	a2	56	9c
12	c4	a6	18	e7	9d	be	7a	dc	3b	23	85	59	41	ff	62
98	14	5f	ee	f1	54	b1	a5	fa	0b	e5	ba	40	ae	1f	4b
2b	05	8c	7e	f0	07	f2	f7	7b	8b	f5	79	02	7c	8e	89
bd	69	55	5c	64	04	09	60	35	51	0d	58	6d	31	38	3c
1c	d0	f9	f6	16	c9	0f	df	26	30	c6	3f	19	ef	e0	29
0e	6c	d9	22	94	03	fb	97	4e	da	f8	21	6f	4d	b6	b5
8a	a8	7f	3a	73	9e	45	ed	92	e1	db	a4	36	0c	49	d7
af	ad	f3	44	83	99	b7	1a	e9	6a	2e	dd	34	70	c7	5e
b3	b9	ac	aa	72	cd	06	bf	13	61	cb	67	74	de	d8	15
a1	7d	0a	b2	95	50	b8	c5	cf	5a	e8	e2	2d	9f	27	77
37	d5	75	88	e6	ce	fd	28	5d	bb	33	46	1b	93	6e	a0
39	c1	2a	66	17	9a	4c	8d	a7	b0	d6	fc	5b	3d	71	eb
84	11	d3	90	01	53	43	52	81	80	10	c3	42	d2	91	c2
00	78	86	cc	65	57	4a	32	b4	d1	1d	9b	2f	e3	a9	fe

S-Box π_6															
$\mathbf{N_{\pi_6} = 108}$, $\mathbf{\delta_{\pi_6} = 6}$, $\mathbf{\deg(\pi_6) = 7}$, $\mathbf{AI_{gr}(\pi_6) = 3}$, $\mathbf{t^{(3)}_{\pi_6} = 441}$															
1b	58	81	db	94	8d	41	02	98	17	d7	4d	ce	0e	54	c2
9e	dd	ad	c3	7b	d3	75	b3	05	65	bd	0b	15	cd	a3	6b
e1	fb	38	b9	93	f2	9a	7a	59	d1	73	50	12	b0	31	d8
13	d6	a0	90	19	e4	2b	e6	5d	5f	d4	6f	29	a2	92	6d
4c	77	53	8f	80	30	c7	ab	e3	78	ec	a4	5c	c8	14	3f
3b	9c	7d	7e	6a	ee	18	9f	f9	88	ed	8b	69	0c	0f	fa
e9	36	83	32	91	0d	aa	87	1f	95	bc	24	20	09	b8	ae
6c	f0	35	ea	f1	c5	c4	2f	01	eb	1a	34	2e	df	00	de
96	10	16	48	79	2c	45	4e	43	21	72	7f	27	74	2a	1d
c1	7c	5e	dc	e2	07	99	fe	bb	42	85	c0	60	a7	25	39
e9	b1	e5	57	e0	f8	a9	03	fd	06	4a	b4	52	1e	ac	4f
33	51	c6	f5	68	11	28	62	bf	cc	22	ff	5b	b5	86	8c
be	5a	cb	a6	0a	26	76	37	e7	f6	4b	9b	67	da	b7	8a
b6	97	70	2d	08	d9	46	ca	a1	b2	84	ef	55	63	3e	fc
44	ba	e8	04	82	cf	f7	56	a5	3c	23	d0	6e	71	9d	49
64	3d	8e	61	f3	3a	f4	d2	47	af	d5	40	1c	66	89	a8

Table 3: A comparison between the cryptographic properties of 8-bit S-Boxes produced by different modern generation methods (NR means "not reported")

Methods/Cryptographic properties	N_π	δ_π	$\deg(\pi)$	$AI_{gr}(\pi)\left(t^{(AI_{gr}(\pi)}\right)$	$AC(\pi)_{max}\left(\sigma(\pi)\right)$	τ_π	$SNR(\pi)$	rdc
Finite Field Inversion [36](AES S-Box)	112	4	7	2(39)	32(133120)	7,860	9,600	0,984
Exponential method [1](BelT S-Box)	102	8	6	3(441)	88(232960)	7,833	8,318	0,969
4-uniform permutations method [40,41]	98	4	NR	NR	NR	NR	NR	NR
Gradient descent method [28]	104	8	7	3(441)	72(206464)	7,823	9,208	0,969
GA/HC [33]	100	NR	NR	NR	NR	NR	NR	NR
GaT [50]	104	NR	NR	NR	NR	NR	NR	NR
GA1 [26]	106	6	6	2(32)	56(151936)	7,850	9,458	0,977
	108	6	6	2(34)	48(148864)	7,849	9,768	0,977
GA2 [26]	110	6	7	2(36)	40(145024)	7,855	9,850	0,977
	112	6	7	2(38)	32(138112)	7,858	9,866	0,977
Hill Climbing [32]	100	NR	NR	NR	NR	NR	NR	NR
Hybrid Heuristic Methods [24]	102	6	4	3(441)	96(255872)	7, 833	8, 650	0, 977
	104	6	4	3(441)	96(242176)	7, 824	8, 467	0, 977
Simulated Annealing [12]	102	NR	NR	NR	80(NR)	NR	NR	NR
SpImmAlg [25]	104	6	7	3(441)	88(216448)	7,822	9,038	0,977
Spectral-linear and spectral-difference methods [31]	104	6	7	3(441)	NR	NR	NR	NR
Tweaking [17]	106	6	7	2(27)	56(171520)	7,854	9,481	0,977
New[S-Box π_1]	100	8	7	3(441)	72(186112)	7,839	8,220	0,969
New[S-Box π_2]	102	8	7	3(441)	80(227584)	7,783	8,751	0,969
New[S-Box π_3]	104	8	7	3(441)	72(193024)	7,806	8,169	0,969
New[S-Box π_4]	104	6	7	3(441)	80(192256)	7,818	8,745	0,977
New[S-Box π_5]	106	6	7	3(441)	72(191104)	7,816	9,013	0,977
New[S-Box π_6]	108	6	7	3(441)	64(185344)	7,838	9,335	0,977

This comparison shows that:

1. Our construction produces 8-bit permutations with the same properties reported in [1,12,17,24,25,28,31,32,33,50];

2. The GA1 and GA2 methods (with the exception of the AES S-Box) have the best values reported for nonlinearity, maximal absolute indicator and sum-of-squares indicators. But these S-Boxes do not possess a high value of algebraic immunity;

3. With respect to cryptographic strength against differential, linear and algebraic attacks S-Boxes π_5 and π_6 establish up to date a new record in the public available literature on generation of S-boxes with strong cryptographic properties;

4. The transparency order and SNR(DPA) for the proposed S-Boxes in this work $\pi_i, i = 1, \ldots, 6$ are lesser than that of AES S-Box and GA1,GA2 methods;

5. Finite Field Inversion and 4-uniform permutations methods have the smallest known values of differential uniformity but the other methods present good values for this parameter;

6. Finite Field Inversion method (AES S-Box) has the best value for robustness *to differential cryptanalysis* but the other methods exhibits acceptable values for this parameter.

The S-Boxes $\pi_i, i = 1, \ldots, 6$ generated by our method were selected in order to have good resistive properties both towards classical cryptanalysis as well as DPA attacks.

7 Conclusion and Future Work

In this article was presented a new method for constructing S-Boxes of dimension $n = 2k, k \geq 2$. In particular, we proposed a special algorithmic-algebraic scheme which

utilizes inversion in GF(2^4) and two arbitrary permutations from $S(V_4)$ for generating 8-bit S-boxes having almost optimal cryptographic properties. Our work solves the question about existence of permutations with algebraic immunity 3 and nonlinearity more than 104, providing new 8-bit S-Boxes which have better resistence to algebraic and DPA attacks in terms of algebraic immunity, transparency order and SNR(DPA) than AES' S-box while having comparable classical cryptographic properties. These substitutions can be appropriate in the design of stream cipher, block cipher and hash functions. It will be interesting to obtain theoretical results on cryptographic properties of the proposed construction for $n = 2k, k \geq 2$. Our work raised the following

Open Question: *Does there exist an 8-bit permutation with algebraic immunity 3 and nonlinearity more than 108?*

Acknowledgements. The author is very grateful to Orr Dunkelman and other anonymous reviewers for their useful comments and valuable observations, which helped to improve the final version of this article.

References

1. Agievich S., Afonenko A.: Exponential s-boxes. Cryptology ePrint Archive, Report 2004/024, 2004. http://eprint.iacr.org/2004/024.
2. Aoki K., Ichikawa T., Kanda M., Matsui M., Moriai S., Nakajima J., and Tokita T.: Camellia: A 128-Bit Block Cipher Suitable for Multiple Platforms - Design and Analysis. In Selected Areas in Cryptography, D. R. Stinson and S. Tavares,Eds., vol. 2012 of of LNCS.Springer Berlin Heidelberg, 2001, pp. 39-56.
3. Armknecht, F., Krause, M.: Constructing single and multioutput Boolean functions with maximal algebraic immunity. In: Bugliesi, M., Preneel, B., Sassone, V.,Wegener, I. (eds.) ICALP 2006, Part II. of LNCS, vol. 4052, pp. 180-191. Springer,Heidelberg (2006).
4. Barreto, P., Rijmen, V.: The Khazad legacy-level block cipher. Primitive submitted to NESSIE (2000).
5. Barreto, P., Rijmen, V.: The Whirlpool hashing function. In: First open NESSIE Workshop, Leuven, Belgium. Volume 13. (2000)
6. Bilgin B., Nikova S., Nikov V., Rijmen V. and Stutz G.: Threshold Implementations of all 3× 3 and 4 × 4 S-Boxes, http://eprint.iacr.org/2012/300/,2012.
7. Biryukov, A., De Cannière, C.: Block ciphers and systems of quadratic equations.In: Johansson, T. (ed.) FSE. 2003. of LNCS, vol. 2887, pp. 274-289. Springer, Heidelberg (2003)
8. Alex Biryukov, Léo Perrin, and Aleksei Udovenko.: Reverse engineering the S-Box of streebog, kuznyechik and STRIBOBr1. In Marc Fischlin and Jean-Sébastien Coron, editors, Advances in Cryptology - EUROCRYPT 2016, Part I, volume 9665 of LNCS, pages 372-402. Springer, Heidelberg, May 2016.
9. Canteaut, A., Duval, S., Leurent, G.: Construction of Lightweight S-Boxes using Feistel and MISTY structures. In Dunkelman, O., Keliher, L., eds.: Selected Areas in Cryptography 2015. of LNCS. Springer International Publishing (2015).
10. Carlet, C.: Vectorial Boolean functions for cryptography. Boolean Models and Methods in Mathematics, Computer Science, and Engineering. Cambridge University Press, 2010.
11. Carlet, C.: On the algebraic Immunities and Higher Order Nonlinearities of Vectorial Boolean Functions. Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes. Amsterdam: IOS Press, 2009, pp. 104-116.

12. Clark J.A., Jacob J.L., and Stepney S.: The design of s-boxes by simulated annealing. New Generation Computing Archive, 23(3), September 2005.
13. Courtois, N. T., and Pieprzyk, J.: Cryptanalysis of Block Ciphers with Overdefined Systems of Equations, http://eprint.iacr.org/2002/044/,2002.
14. De Cannière, C.: Analysis and Design of Symmetric Encryption Algorithms, Ph.D. thesis, 2007.
15. H. Feistel.: Cryptography and computer privacy. Scientific American, 228(5):15-23, 1973.
16. Garey M.R., Johnson D.S. . Computers and Intractability - A Guide to the Theory of NP-Completeness. W.H. Freeman and Company, 1979.
17. Fuller J. and Millan W.: Linear redundancy in s-boxes. In FSE'03, volume 2887 of of LNCS, pages 74-86.Springer, 2003.
18. Gérard, B., Grosso, V., Naya-Plasencia, M., Standaert, F.X.: Block ciphers that are easier to mask: how far can we go? In: Cryptographic Hardware and Embedded Systems-CHES 2013. Springer (2013) 38-399
19. Golić J. Dj.: Fast low order approximation of cryptographic functions. In Advances in Cryptology EUROCRYPT'96, volume 1070 of of LNCS, p.p 268-282. Springer Verlag, 1996.
20. GOST R 34.12-2015 Information technology. Cryptographic protection of information. Block ciphers. Moscow, Standartinform, 2015.
21. GOST R 34.11-2012 Information technology. Cryptographic protection of information. Hash function. Moscow, Standartinform, 2012.
22. Guilley S., Hoogvorst P. and Pacalet R.: Differential power analysis modeland some results. In CARDIS, pages 127-142, 2004.
23. Hirata K:. The 128-bit Block Cipher HyRAL (Hybrid Randomization Algorithm): Common KeyBlock Cipher. In International Symposium on Intelligence Information Processing and TrustedComputing (October 2010), pp. 9-14.
24. Isa H., Jamil N., and Z'aba M. (2016).: Hybrid Heuristic Methods in Constructing Cryptographically Strong S-boxes. International Journal of Cryptology Research 6(1): (2016)
25. Ivanov G., Nikolov N., and Nikova S.: Cryptographically Strong S-Boxes Generated by Modified Immune Algorithm. Cryptography and Information Security in the Balkans Volume 9540 of the series of LNCS pp 31-42.
26. Ivanov G, Nikolov N., and Nikova S.: Reversed genetic algorithms for generation of bijective S-Boxes with good cryptographic properties. IACR Cryptology ePrint Archive (2014), Report 2014/801,http://eprint.iacr.org/2014/801.pdf.
27. Izbenko Y., Kovtun V., Kuznetsov A.: The Design of Boolean Functions by Modified Hill Climbing Method.http://eprint.iacr.org/2008/111.pdf.
28. Kazymyrov O.V., Kazymyrova V.N., Oliynykov R.V.: A method for generation of high-nonlinear S-Boxes based on gradient descent, Mat. Vopr. Kriptogr., 2014, Volume 5, Issue 2, pp. 71-78.
29. Knudsen, L. R.: Truncated and Higher Order Differentials. In FSE, B. Preneel,Ed., vol. 1008 of of LNCS. Springer Berlin Heidelberg, 1995, pp. 196-211.
30. Kwon, D., Kim, J., Park, S., Sung, S., Sohn, Y.,Song, J., Yeom, Y., Yoon, E.-J., Lee, S., Lee, J.,Chee, S., Han, D., and Hong, J.: New Block Cipher: ARIA. In Information Security and Cryptology - ICISC 2003, J.-I. Lim and D.-H. Lee,Eds., vol. 2971 of of LNCS. Springer Berlin Heidelberg, 2004, pp. 432-445.
31. Menyachikhin A.: Spectral-linear and spectral-difference methods for generating cryptographically strong S-Boxes. In: Pre-proceedings of CTCrypt'16-Yaroslavl, Russia, 2016. p.232-252.

32. Millan W.: How to improve the nonlinearity of bijective s-boxes. In Australian Conference on Information Security and Privacy 1998, volume 1438, pages 181-192. Springer Verlag, 1998.
33. Millan W., L. Burnett, G. Carter, A. Clark, and E. Dawson.: Evolutionary heuristics for finding cryptographically strong s-boxes. In ICICS'99, volume 1726 of of LNCS, pages 263-274. Springer, 1999.
34. Millan W. L.: Low order approximation of cipher functions. In Cryptography: Policy and Algorithms Conference, Proceedings, volume 1029 of of LNCS, pp. 144-155. Springer Verlag, 1996.
35. NIST. Advanced Encryption Standard. Federal Information Processing Standard (FIPS) 197,November 2001.
36. Nyberg K.: Differentially uniform mappings for cryptography. In Helleseth, T. (ed.), Advances in Cryptology - EUROCRYPT'93, vol.765 of of LNCS, pp. 55-64. Springer Berlin Heidelberg, 1994.
37. Ohkuma K., Muratani H., Sano F., and Kawamura S.: The Block Cipher Hierocrypt. In Selected Areas in Cryptography, D. R. Stinson and S. Tavares, Eds., vol. 2012 of of LNCS. Springer Berlin Heidelberg, 2001, pp. 72-88.
38. Oliynykov R., Gorbenko I., Kazymyrov O., Ruzhentsev V., Kuznetsov O., Gorbenko Y., Dyrda O., Dolgov V., Pushkaryov A., Mordvinov R. and Kaidalov D.: DSTU 7624:2014. national standard of ukraine. information technologies. cryptographic data security. symmetric block transformation algorithm.Ministry of Economical Development and Trade of Ukraine, 2015.
39. Prouff E.: DPA Attacks and S-boxes. In FSE, pages 424-441, 2005.
40. Qu L.,Tan Y.,Li C., and Gong G.: More constructions of differentially 4-uniform permutations on $\mathbb{F}_{2^{2k}}$. In arxiv.org/pdf/1309.7423, 2013.
41. Qu L.,Tan Y., Tan C. and Li C.: Constructing differentially 4-uniform permutations over $\mathbb{F}_{2^{2k}}$ via the switching method. IEEE Transactions on Inform. Theory, 59(7):4675-4686, 2013.
42. Leander G., Poschmann A.: On the classification of 4 bit S-Boxes. of LNCS, 2007, vol. 4547, pp. 159-176.
43. Lidl, R., and Niederreiter, H.: Finite Fields,vol. 20 of Encyclopedia of Mathematics and its Applications. Cambridge University Press, 1997.
44. Sage Mathematics Software (Version 7.2). (2016) http://www.sagemath.org.
45. Saarinen, M.J.O. STRIBOB: Authenticated encryption from GOST R 34.11-2012 LPS permutation. In:Mathematical Aspects of Cryptography. Volume 6, No. 2. Steklov Mathematical Institute of Russian Academy of Sciences (2015) pp.67-78.
46. Seberry J, Zhang X.M and Zheng Y.: Systematic generation of cryptographically robust S-boxes,Proceedings of the First ACM Conference on Computer and Communications Security, The Association for Computing Machinery, Fairfax, VA, (1993), 171-182.
47. Standaert, F.X., Piret, G., Rouvroy, G., Quisquater, J.J., Legat, J.D. ICEBERG : An Involutional Cipher Efficient for Block Encryption in Reconfigurable Hardware. In Roy B., Meier W., eds. FSE. Volume 3017 of Lecture Notes in Computer Science. Springer Berlin Heidelberg (2004) 279-298
48. STB 34.101.31-2011 Information technologies. Information security. Cryptographic algorithms of enciphering and continuity test. Minsk, Gosstandart, 2011.
49. Shirai, T., Shibutani, K., Akishita, T., Moriai, S., Iwata, T.: The 128-bit blockcipher CLEFIA. In FSE, Springer (2007) 181-195
50. Tesař P.: A New Method for Generating High Non-linearity S-Boxes. Radioengineering - 2010. V. 19, NO. 1. - p. 23-26.