Computer Science Journal of Moldova, vol.**28**, no.3(84), 2020

Investigation of Some Cryptographic Properties of the 8x8 S-boxes Created by Quasigroups

Aleksandra Mileva, Aleksandra Stojanova,
Dušan Bikov, Yunqing Xu

Abstract

We investigate several cryptographic properties in 8-bit S-boxes obtained by quasigroups of order 4 and 16 with several different algebraic constructions. Additionally, we offer a new construction of N-bit S-boxes by using different number of two layers – the layer of bijectional quasigroup string transformations, and the layer of modular addition with N-bit constants. The best produced 8-bit S-boxes so far are regular and have algebraic degree 7, nonlinearity 98 (linearity 60), differential uniformity 8, and autocorrelation 88. Additionally we obtained 8-bit S-boxes with nonlinearity 100 (linearity 56), differential uniformity 10, autocorrelation 88, and minimal algebraic degree 6. Relatively small set of performed experiments compared with the extremly large set of possible experiments suggests that these results can be improved in the future.

Keywords: 8-bit S-boxes, nonlinearity, differential uniformity, autocorrelation.

MSC 2010: 20N05, 94A60.

1 Introduction

The main building blocks for obtaining confusion in all modern block ciphers are so called substitution boxes, or S-boxes. Usually, they work with much less data (for example, 4 or 8 bits) than the block size, so they need to be highly nonlinear. Two of the most successful attacks against modern block ciphers are linear cryptanalysis (introduced by

Matsui [21]), which exploits input-output correlation, and differential cryptanalysis (introduced by Biham and Shamir [2]), which exploits difference propagation.

Designers of block ciphers very often choose S-boxes with special cryptographic properties, which means high nonlinearity (or low linearity), low differential uniformity, high algebraic degree, low autocorrelation and regularity (balance). AES S-box is the example of the best found 8x8 S-boxes, which is optimal with respect to most of these cryptographic properties. It has nonlinearity 112 (or linearity 32), algebraic degree 7, differential uniformity 4, and autocorrelation 32.

Mihajloska and Gligoroski [26] constructed optimal 4x4 S-boxes from quasigroups of order 4, by using four e quasigroup string transformations. Motivated by their work, we offer two constructions of the 8x8 S-boxes from quasigroups of order 4 and 16, by using different number of e quasigroup string transformations. Main contribution of this paper is a new construction of N-bit S-boxes which uses different number of two layers – the layer of bijectional quasigroup string transformations, and the layer of modular addition with N-bit constants. Specifically, we demonstrated this construction method with quasigroups of order 4 and 16 and modular addition with 8-bit constants. Quasigroups of order 4 can be seen as 4x2 S-boxes, while quasigroups of order 16 can be seen as 8x4 S-boxes, so, we offer an algebraic construction of 8x8 S-boxes from smaller ones. We investigate some of the cryptographic properties of the obtained S-boxes, without looking at the cost of their implementation in hardware.

This paper has the following structure: Section 2 is about mathematical preliminaries for quasigroup string transformations, basics about n-ary Boolean functions and Boolean maps, and definition of some cryptographic properties for them. Some existing methods for the generation of 8-bit S-boxes, together with the best obtained values of the cryptographic properties of these S-boxes are presented in Section 3. Section 4 presents the two constructions of 8-bit S-boxes by using e quasigroup string transformations produced by quasigroups of order 4 and 16, together with the experimental results. The new construction of N-bit S-boxes and obtained experimental results are presented in the Section 5. Finally, concluding remarks are given in Section 6.

2 Mathematical Preliminaries

2.1 Quasigroup String Transformations

A quasigroup $(Q, *)$ is a groupoid, i.e., a pair of nonempty set Q and a binary operation $*$, such that for all $a, b \in Q$ there exist unique $x, y \in Q$ satisfying the equalities $a * x = b$ and $y * a = b$ [1]. In the case when Q is finite, the multiplication table of $(Q, *)$ is a Latin square of order $|Q|$, where all rows and columns are permutations of Q. For the quasigroup operation $*$ on the set Q, another operation, a right division $\backslash$ can be derived by:

$$x \backslash y = z \Longleftrightarrow x * z = y.$$

Given a finite quasigroup $(Q, *)$, consider the set Q as an alphabet with word set $Q^+ = \{x_1 x_2 \dots x_t \mid x_i \in Q, t \geq 1\}$. For the fixed letter $l \in Q$ (called a leader), the transformations $e_l, d_l : Q^+ \to Q^+$ are defined in [20], as follows:

$$e_l(x_1 \dots x_t) = (z_1 \dots z_t) \Longleftrightarrow z_j = \begin{cases} l * x_1, \ j = 1 \\ z_{j-1} * x_j, \ 2 \leq j \leq t \end{cases}, \tag{1}$$

$$d_l(z_1 \dots z_t) = (x_1 \dots x_t) \Longleftrightarrow x_j = \begin{cases} l \backslash z_1, \ j = 1 \\ z_{j-1} \backslash z_j, \ 2 \leq j \leq t \end{cases}. \tag{2}$$

Any combination of these elementary quasigroup string transformations is a permutation and d_l is an inverse to e_l. Linear quasigroups produce linear e_l and d_l quasigroup string transformations [25]. Additionally, some non-linear quasigroups always produce linear e_l and d_l transformations. For example, there is a set of 48 non-linear quasigroups of order 4 that always produce linear e_l and d_l transformations [25]. In the rest of the paper we will use e and d instead e_l and d_l, respectively.

Definition 1. *[14] A finite quasigroup $(Q,*)$ of order r is said to be shapeless if and only if it is non-idempotent, non-commutative, non-associative, it does not have neither left nor right unit, it does not contain proper sub-quasigroups, and there is no $k < 2r$ such that identities of the kinds*

$$\underbrace{x*(x\cdots*(x}_{k}*y)) = y,\;\; y = ((y*\underbrace{x)*\cdots x)*x}_{k}$$

are satisfied in $(Q,*)$.

2.2 Some Cryptographic Properties of n-ary Boolean Functions and Boolean Maps

Let $\mathbb{F}_2$ denote the Galois field with two elements, and let $\mathbb{F}_2^n$ denote the vector space of binary n-tuples over $\mathbb{F}_2$ with respect to addition $\oplus$ (Boolean function XOR) and scalar multiplication (Boolean function conjunction). There is a correspondence between $\mathbb{F}_2^n$ and $\mathbb{Z}_{2^n}$ via

$$\varphi_1 : \mathbb{F}_2^n \to \mathbb{Z}_{2^n} : \mathbf{x} = (x_1,\dots x_n) \to x = \sum_{i=1}^{n} x_i 2^{i-1},$$

and there is a correspondence between $\mathbb{F}_2^n$ and $\mathbb{F}_{2^n}$ via

$$\varphi_2 : \mathbb{F}_2^n \to \mathbb{F}_{2^n} : \mathbf{x} = (x_1,\dots x_n) \to x = \sum_{i=1}^{n} x_i \beta_i,$$

where $\{\beta_1,\dots,\beta_n\}$ is a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$.

An $n-$*ary Boolean function* is a function $f : \mathbb{F}_2^n \to \mathbb{F}_2$. A *Boolean map* (or vector valued Boolean function or vectorial Boolean function) is a map $S : \mathbb{F}_2^n \to \mathbb{F}_2^m$, $(m \geq 1)$. Every Boolean map S can be represented by m $n-$ary Boolean functions $f_i : {\mathbb{F}_2}^n \to \mathbb{F}_2$, called *coordinate functions* of S, as follows:

$$S(x_1,\dots,x_n) = (f_1(x_1,\dots,x_n), f_2(x_1,\dots x_n),\dots,f_m(x_1,\dots,x_n)).$$

Each $n-$ary Boolean function f_i can be represented in Algebraic Normal Form as

$$f_i(x_1, x_2, \ldots, x_n) = \bigoplus_{I \subseteq \{1,2,\ldots,n\}} \alpha_I (\prod_{i \in I} x_i), \tag{3}$$

where $\alpha_I \in \mathbb{F}_2$. The right-hand side of (3) can be interpreted as a polynomial in the field $(\mathbb{F}_2, \oplus, \cdot)$ and the *algebraic degree* of f_i, $deg(f_i)$, is taken to be the degree of the polynomial.

Definition 2. *The (minimal) algebraic degree of a Boolean map S is defined as the minimum of the algebraic degrees of its non-trivial coordinate functions $(f_1, f_2, \ldots, f_m)$, and it can be expressed as:*

$$deg(S) = \min_{\boldsymbol{u} \in \mathbb{F}_2^m \setminus \{\boldsymbol{0}\}} deg(u_1 f_1 \oplus u_2 f_2 \oplus \ldots \oplus u_m f_m).$$

If $deg(f_i) \leq 1, \forall i \in \{1, 2, \ldots, m\}$, S is an *affine function.* A *linear function* is a non-constant affine function S for which $S(\mathbf{0}) = 0$.

The *(Hamming) weight* of a vector $\mathbf{x} \in \mathbb{F}_2^n$ is equal to the number of components equal to 1 and is denoted by $wt(\mathbf{x})$. The *(Hamming) distance* between two vectors $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$, denoted by $d(\mathbf{x}, \mathbf{y})$ is the number of positions in which they differ. The *(Hamming) weight* of a Boolean function f, $wt(f)$, is the number of function values equal to 1. A Boolean function f is *balanced* if and only if $wt(f) = 2^{n-1}$.

For two vectors $\mathbf{x} = (x_1, \ldots, x_n), \mathbf{y} = (y_1, \ldots, x_y) \in \mathbb{F}_2^n$, the *inner product* or *scalar product* is defined as $\mathbf{x} \cdot \mathbf{y} = \bigoplus_{i=1}^n x_i y_i$. A *selection vector* $\mathbf{a}$ is a binary vector that selects all components i of a vector that have $a_i = 1$. By $\mathbf{a} \cdot \mathbf{x}$ (or $\mathbf{a}^T \mathbf{x}$) the linear combination of the components of a vector $\mathbf{x}$ selected by $\mathbf{a}$, analogous to vector inner product, can be represented. A linear Boolean function $\varphi_{\mathbf{a}} = \mathbf{a} \cdot \mathbf{x}$ is completely specified by its corresponding selection vector $\mathbf{a}$.

A *bias* of an $n-$ary Boolean function f is defined as

$$\varepsilon(f) = \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{x})} = 2^n - 2wt(f).$$

So, balanced Boolean functions have $\varepsilon(f) = 0$.

An $n-$ary Boolean function f on $\mathbb{F}_2^n$ is uniquely determined by its Walsh-Hadamard transform (WHT). The Walsh-Hadamard transform $W_f : \mathbb{F}_2^n \to \mathbb{R}$ of f is defined for all $\mathbf{x} \in \mathbb{F}_2^n$ as

$$W_f(\mathbf{x}) = \sum_{\mathbf{a} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{a}) \oplus \mathbf{a} \cdot \mathbf{x}} (= \varepsilon(f \oplus \varphi_{\mathbf{a}})), \tag{4}$$

where $W_f(\mathbf{x}) \in [-2^n, 2^n]$ and is known as a spectral Walsh coefficient. The real-valued vector of all spectral Walsh coefficients is known as a WHT Spectrum. The WHT spectrum of f corresponds to the biases of all approximations of f by a linear function.

The Walsh transform $W_S : \mathbb{F}_2^n \times \mathbb{F}_2^m \to \mathbb{R}$ of a Boolean map S is defined for all pairs $(\mathbf{u}, \mathbf{v}) \in (\mathbb{F}_2^n, \mathbb{F}_2^m)$ as

$$W_S(\mathbf{u}, \mathbf{v}) = \sum_{\mathbf{a} \in \mathbb{F}_2^n} (-1)^{\mathbf{u} \cdot \mathbf{a} \oplus \mathbf{v} \cdot S(\mathbf{a})}. \tag{5}$$

Definition 3. *The nonlinearity of an $n-$ary Boolean function f (introduced in [22]), denoted by $NL(f)$, is defined as the distance to the nearest affine function on $\mathbb{F}_2^n$. It can be expressed in terms of the spectral Walsh coefficients by*

$$NL(f) = 2^{n-1} - \frac{1}{2} \max_{\boldsymbol{x} \in \mathbb{F}_2^n} |W_f(\boldsymbol{x})|. \tag{6}$$

$NL(f) = 0$ iff f is affine function.

Definition 4. *The linearity of an $n-$ary Boolean function f, denoted by $L(f)$, is defined as*

$$L(f) = \max_{\boldsymbol{x} \in \mathbb{F}_2^n} |W_f(\boldsymbol{x})|. \tag{7}$$

Linearity and nonlinearity of a given $n-$ary Boolean function f are connected by the following equation:

$$L(f) + 2NL(f) = 2^n. \tag{8}$$

For $L(f)$, the inequality $2^{\frac{n}{2}} \leq L(f) \leq 2^n$ holds. $L(f) = 2^n$ iff f is affine function. Boolean functions for which $L(f) = 2^{\frac{n}{2}}$ are called *bent* *functions* (introduced by Rothaus [31]), and they exist only for even n. Because bent functions are highly biased ($\varepsilon(f) = \pm 2^{\frac{n}{2}}$), they are of little use in cryptography.

Linear approximation table for Boolean map S is a $2^n \times 2^m$ table whose entries are defined for all pairs $(\mathbf{u}, \mathbf{v}) \in (\mathbb{F}_2^n, \mathbb{F}_2^m)$ as

$$LAT_S(\mathbf{u}, \mathbf{v}) = W_S(\mathbf{u}, \mathbf{v}).$$

Definition 5. *The nonlinearity and linearity of a Boolean map S [29] are defined as*

$$NL(S) = \min_{\boldsymbol{v} \in \mathbb{F}_2^m \setminus \{\boldsymbol{0}\}} NL(\boldsymbol{v} \cdot S) = 2^{n-1} - \frac{1}{2} \max_{\boldsymbol{a} \neq \boldsymbol{0}, \boldsymbol{b} \in \mathbb{F}_2^m} |W_S(\boldsymbol{a}, \boldsymbol{b})|, \quad (9)$$

$$L(S) = \max_{\boldsymbol{v} \in \mathbb{F}_2^m \setminus \{\boldsymbol{0}\}} L(\boldsymbol{v} \cdot S), \quad (10)$$

where $\boldsymbol{v} \cdot S = \bigoplus_{i=1}^{n} v_i f_i$ is the linear combination of the coordinate functions of S.

$L(S) \geq 2^{\frac{n}{2}}$, and Nyberg [27] showed that equality can hold only if $n \geq 2m$ and n is even. For $n = m$, $L(S) \geq 2^{\frac{n+1}{2}}$ with equality for odd n only (Chabaud-Vaudenay theorem [6]) . The functions achieving this bound are called *almost bent functions*. Because for even n and $n = m$, some $n \times n$ S-boxes with $L(S) = 2^{\frac{n+2}{2}}$ are known, Dobbertin [12] conjectured that this value is the minimum.

From linear approximation table, one can easily calculate *linear probability bias* $\varepsilon_S(\mathbf{u}, \mathbf{v})$, which is amount by which the probability of a linear expression holding deviates from $\frac{1}{2}$. The formula is $\varepsilon_S(\mathbf{u}, \mathbf{v}) = LAT_S(\mathbf{u}, \mathbf{v})/2^n - \frac{1}{2}$.

Difference distribution table for Boolean map S is a $2^n \times 2^m$ table whose entries are defined for all pairs $(\mathbf{u}, \mathbf{v}) \in (\mathbb{F}_2^n, \mathbb{F}_2^m)$ as

$$DDT_S(\mathbf{u}, \mathbf{v}) = \sharp\{\mathbf{x} \in \mathbb{F}_2^n | S(\mathbf{x}) \oplus S(\mathbf{x} \oplus \mathbf{u}) = \mathbf{v}\}.$$

Definition 6. *The differential uniformity of a Boolean map S [28], denoted by $\Delta(S)$, is defined as*

$$\Delta(S) = \max_{\boldsymbol{u} \in \mathbb{F}_2^n \setminus \{\boldsymbol{0}\}, \boldsymbol{v} \in \mathbb{F}_2^m} DDT_S(u, v). \quad (11)$$

For differential uniformity, $\Delta(S) \geq max\{2, 2^{n-m}\}$ holds, and for $n \geq m$, $\Delta(S)$ takes only even values in $[2^{n-m}, 2^n]$. Nyberg [27] showed that for $n > m$, $\Delta(S) = 2^{n-m}$ if and only if $n \geq 2m$ and n is even. This kind of functions are known as *perfect nonlinear* functions and they are the same as the bent functions. For $n \leq m$, $\Delta(S) = 2$, and this kind of functions are known as *almost perfect nonlinear*. So, bijective S-boxes can have the smallest differential uniformity of 2, and there are examples for odd n.

For the n-ary Boolean function f on $\mathbb{F}_2^n$ one can define an Autocorrelation transform (ACT) $ACT_f : \mathbb{F}_2^n \to \mathbb{R}$ for all $\mathbf{x} \in \mathbb{F}_2^n$ as

$$ACT_f(\mathbf{x}) = \sum_{\mathbf{a} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{a}) \oplus f(\mathbf{a} \oplus \mathbf{x})}, \tag{12}$$

where $ACT_f(\mathbf{x}) \in [-2^n, 2^n]$ is known as a spectral autocorrelation coefficient and $ACT_f(\mathbf{0}) = 2^n$. The real-valued vector of all spectral autocorrelation coefficients is known as an ACT Spectrum.

Definition 7. *The Absolute indicator of an n-ary Boolean function f, denoted by $AC(f)$, is defined as the maximal non-trivial absolute spectral autocorrelation coefficient, or*

$$AC(f) = \max_{\boldsymbol{x} \in \mathbb{F}_2^n \setminus \{\boldsymbol{0}\}} |ACT_f(\boldsymbol{x})|. \tag{13}$$

Definition 8. *The Absolute indicator of a Boolean map S is defined as*

$$AC(S) = \max_{\boldsymbol{v} \in \mathbb{F}_2^m \setminus \{\boldsymbol{0}\}} AC(\boldsymbol{v} \cdot S). \tag{14}$$

Two n-ary Boolean functions f and g belong to the same *equivalence class* (or are *affine equivalent*) if and only if there exist some non-singular binary matrix D, vectors $\mathbf{a}, \mathbf{b} \in \mathbb{F}_2^n$ and a scalar $c \in \mathbb{F}_2$, such that $g(\mathbf{x}) = f(D\mathbf{x} \oplus \mathbf{a}) \oplus \mathbf{b} \cdot \mathbf{x} \oplus c$. (Two n-ary Boolean functions f and g are affine equivalent if there exists an affine permutation A of $\mathbb{F}_2^n$ such that $g(\mathbf{x}) = f(A(\mathbf{x})$.)

The algebraic degree, nonlinearity and absolute indicator are invariant under affine equivalence [22], [30]. Any Boolean map S and its inverse have same linearity and differential uniformity (Nyberg [29]). In the same paper, Nyberg proved that differential uniformity is invariant under affine permutations onto the input space and the output space. Two S-boxes S_1 and S_2 are *affinely equivalent* if there exist two affine permutations A_1 and A_2, such that $S_2 = A_2 \circ S_1 \circ A_1$. So, the affinely equivalent S-boxes have same differential uniformity (and same algebraic degree, nonlinearity and absolute indicator).

Definition 9. *A Boolean map S is regular if and only if all non-zero its coordinate functions are balanced.*

With other words, this means that when $n \geq m$, for each output $y \in \mathbb{F}_2^m$ there are exactly 2^{n-m} inputs that are mapped to y. The well known fact is that the bijective S-boxes (permutations) are always regular.

S-boxes need to be:

- with high minimal algebraic degree to resist low order approximation attacks and higher order differential attacks
- with high nonlinearity (low linearity) to resist linear attacks
- with low differential uniformity to resist differential attacks
- with low absolute indicator (autocorrelation) to improve the avalanche effect of the cipher
- regular to resist trivial statistical attacks.

3 Some Existing Methods for Generation of 8-bit S-Boxes

Existing methods for generation of S-boxes can be divided mainly in three groups: algebraic constructions, pseudo-random generation and heuristic generation.

The first group of S-boxes are constructed by applying some mathematical operations and transformations, like finite field inversion

Table 1. A comparison between some of the cryptographic properties of the bijective 8x8 S-boxes produced by different generation methods (− stands for ”missing data”)

Method	NL(S)	L(S)	$\Delta(S)$	AC(S)	deg(S)
Finite Field Inversion [28] (AES S-box)	112	32	4	32	7
3-round Feistel [5]	96	64	8	–	–
4-uniform permutations method [33]	98	60	4	–	–
Finite Field Multiplication [11]	106 108	44 40	6	56 64	7
Hill climbing method [24]	100	56	–	–	–
Tweaking method [13]	106	44	6	56	7
Simulated annealing method [7]	102	52	–	80	–
GaT [32]	104	48	–	–	–
Gradient descent method [18]	104	48	8	80	7
Hybrid heuristic method [17]	102 104	52 48	6	96	4
Spectral-linear and spectral-difference methods [23]	104	48	6	–	7
GA1 [15]	106 108	44 40	6	56 48	6
GA2 [15]	110 112	36 32	6	40 32	7
SpImmAlg [16]	104	48	6	88	7
Quasigroup 4 method [this paper]	98	60	8	88	7
Quasigroup 16 method [this paper]	100 98	56 60	10 8	88	6 7

method (e.g., AES S-box), or using a smaller S-box as starting point (e.g., finite field multiplication method [11]). In this group one can find 8-bit S-boxes with the best known cryptographic properties. The second group of S-boxes are obtained by pseudo-random generation, and usually they do not have very good cryptographic properties, because of the large input space and very small number of strong S-boxes. The third group of S-boxes are generated by iteratively improving given S-box with respect to one or more cryptographic properties, with the help of the heuristic algorithms (e.g., simulated annealing method [7]). The main advantage of the last generation method is the large number of S-boxes close to the best known.

Our constructions are algebraic constructions, and Table 1 presents the comparisons of our results with the results of some existing methods for generating bijective 8-bit S-boxes. However, our results are based on the experiments made so far, and there is a big possibility these results to be improved by more performed experiments. The set of quasigroups of order 16 is extremly large, and here only one quasigroup with specific features is used, so the number of performed experiments is relatively small.

Mihajloska and Gligoroski [26] constructed optimal 4x4 S-boxes from quasigroups of order 4, by using four e quasigroup string transformations alternating in normal and reverse mode (in a sense that they apply the string in reverse order), on 4 bits. They obtained 9216 optimal Q-S-boxes - with nonlinearity 4 (linearity 8), differential uniformity 4, autocorrelation of 16, maximal algebraic degree of 3 and minimal algebraic degree of 2.

4 Constructions of 8-bit S-boxes with Quasigroups of order 4 and 16

We investigate several cryptographic properties of the 8x8 S-boxes obtained by constructions similar to the one presented in [26], by using quasigroup string transformations, produced by quasigroups of order 4 and 16. The reverse mode of e and d quasigroup string transformations we will denote here as *oe* and *od*, respectively (Figure 1). The argument of the quasigroup string transformations is the 8-bit string of 4 elements for quasigroups of order 4 and of 2 elements for quasigroups of order 16.

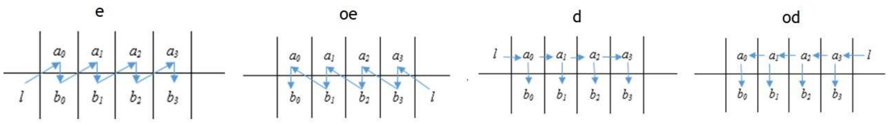


Figure 1. Application of *e* and *d* transformations in normal and reverse mode on 8-bit string of 4 elements

4.1 Construction with Quasigroups of order 4

For experiments with quasigroups of order 4, we use only 384 quasigroups out of the total 576. We excluded all linear quasigroups and 48 other non-linear quasigroups that always produce linear *e* and *d* transformations. In the representation of the type of used quasigroup string transformations, *n*eoe type means that there are total of *n* *e* quasigroup string transformations, used alternately in normal and reverse mode, while *n*dod type means that there are total of *n* *d* quasigroup string transformations, used alternately in normal and reverse mode. For each used type and used *n*, we generated all 8-bit S-boxes and calculated their cryptographic properties. The best obtained results are written in the tables given below, and the best S-boxes are memorized by the lexicographic order of the used quasigroup and the leaders.

Method 1 – In the first method we use different number of *e* transformations generated by quasigroups of order 4, alternately in normal and reverse mode, on the 8-bit string of 4 2-bit elements, as follows (see Algorithm 1):

```
Algorithm 1. Construction of 8-bit S-box by Method 1
Input:    Q - quasigroup of order 4, $neoe$ type and
          vector of leaders $L = (l_1, l_2, \ldots l_n)$
Output:   S
   For all possible input blocks $x_1, x_2, x_3, x_4$ in lexicographic ordering
     $(p_1, p_2, p_3, p_4) = (x_1, x_2, x_3, x_4)$
     For $i = 1$ to $n$
       If $i$ is odd
         $(t_1, t_2, t_3, t_4) = e_{l_i}(p_1, p_2, p_3, p_4)$
       else
         $(p_4, p_3, p_2, p_1) = e_{l_i}(t_4, t_3, t_2, t_1)$
  Use all output blocks from the last round to generate $S$
```

Taking into account that block ciphers that use S-boxes, need their inversions for decryption process, the construction of S^{-1} is given below (see Algorithm 2):

```
Algorithm 2. Construction of $S^{-1}$
Input:    Q - quasigroup of order 4, $neoe$ type and
          vector of leaders $L = (l_1, l_2, \ldots l_n)$
Output:   $S^{-1}$
   For all possible input blocks $x_1, x_2, x_3, x_4$ in lexicographic ordering
     $(p_1, p_2, p_3, p_4) = (x_1, x_2, x_3, x_4)$
     For $i = n$ down to 1
       If $n$ is even
         If $i$ is even
           $(t_4, t_3, t_2, t_1) = d_{l_i}(p_4, p_3, p_2, p_1)$
         else
           $(p_1, p_2, p_3, p_4) = d_{l_i}(t_1, t_2, t_3, t_4)$
       else
         If $i$ is odd
           $(t_1, t_2, t_3, t_4) = d_{l_i}(p_1, p_2, p_3, p_4)$
         else
           $(p_4, p_3, p_2, p_1) = d_{l_i}(t_4, t_3, t_2, t_1)$
  Use all output blocks from the last round to generate $S^{-1}$
```

The results for 8-bit S-boxes with best examined cryptographic properties for each $n = \{1, \ldots, 13\}$ are given in Table 2, while the graphical visualisation of 4*eoe* type is given on Figure 2.

The best produced 8x8 S-boxes are obtained by 13 e quasigroup transformations, alternating in normal and reverse mode, and they have differential uniformity 8, nonlinearity 98 (linearity 60), autocorrelation

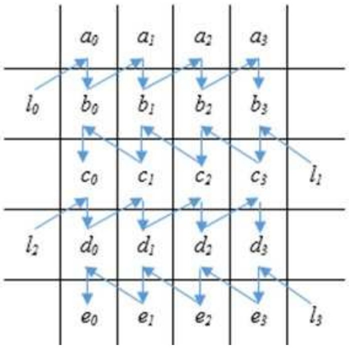


Figure 2. *4eoe* type – four *e* transformations, alternating in normal and reverse mode, on 8-bit string of 4 2-bit elements

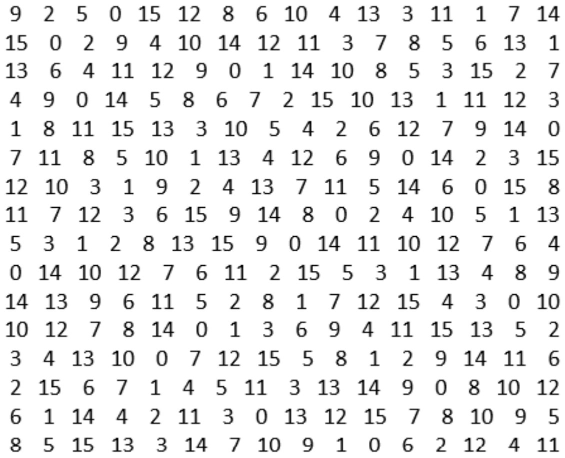
Table 2. The best results for S-boxes obtained by Method 1

Type	NL(S)	L(S)	$\Delta(S)$	AC(S)	$max\{deg(f_i)\}$	deg(S)	No. of S
1e	0	256	256	256	4	1	1152
2eoe	0	256	128	256	6	1	768
3eoe	64	128	64	256	6	3	9216
4eoe	64	128	24	256	7	4	192
5eoe	92	72	16	128	7	6	192
6eoe	96	64	10	104	7	6	96
7eoe	98	60	10	96	7	7	192
8eoe	98	60	10	88	7	6	288
9eoe	98	60	10	88	7	7	480
10eoe	98	60	10	88	7	7	8352
11eoe	98	60	8	112	7	6	96
12eoe	98	60	8	88 96	7	6 7	768 1632
13eoe	98	60	8	88	7	7	96

88 and maximal and minimal algebraic degree 7. There are 96 such S-boxes, obtained by 24 different quasigroups of order 4. One example is the S-box S1 (Table 4) obtained from the quasigroup 34 of order 4, with consecutive leaders (0, 3, 2, 3, 3, 3, 1, 1, 0, 2, 0, 0, 0).

4.2 Construction with quasigroups of order 16

All the experiments with quasigroups of order 16 are done with one, specifically chosen quasigroup of order 16. The requirements for choosing were quasigroup to be shapeless and with highest nonlinearity and lowest differential uniformity if you represent it as 8×4 S-box in a randomly generated set. From 1,000 different randomly tested quasigroups of order 16, we have chosen the best obtained, such as the quasigroup, presented in Figure 3, with differential uniformity 38, nonlinearity 100 (linearity 56), autocorrelation 64 and maximal and minimal algebraic degree 6. The best S-boxes are memorized by the used leaders.



9	2	5	0	15	12	8	6	10	4	13	3	11	1	7	14
15	0	2	9	4	10	14	12	11	3	7	8	5	6	13	1
13	6	4	11	12	9	0	1	14	10	8	5	3	15	2	7
4	9	0	14	5	8	6	7	2	15	10	13	1	11	12	3
1	8	11	15	13	3	10	5	4	2	6	12	7	9	14	0
7	11	8	5	10	1	13	4	12	6	9	0	14	2	3	15
12	10	3	1	9	2	4	13	7	11	5	14	6	0	15	8
11	7	12	3	6	15	9	14	8	0	2	4	10	5	1	13
5	3	1	2	8	13	15	9	0	14	11	10	12	7	6	4
0	14	10	12	7	6	11	2	15	5	3	1	13	4	8	9
14	13	9	6	11	5	2	8	1	7	12	15	4	3	0	10
10	12	7	8	14	0	1	3	6	9	4	11	15	13	5	2
3	4	13	10	0	7	12	15	5	8	1	2	9	14	11	6
2	15	6	7	1	4	5	11	3	13	14	9	0	8	10	12
6	1	14	4	2	11	3	0	13	12	15	7	8	10	9	5
8	5	15	13	3	14	7	10	9	1	0	6	2	12	4	11

Figure 3. Shapeless quasigroup of order 16

Method 2 – The second method is like Method 1, but with the randomly generated shapeless quasigroup of order 16 (Figure 3) and using 8-bit string of 2 4-bit elements, as follows (see Algorithm 3):

```
Algorithm 3. Construction of 8-bit S-box by Method 2
Input:    Q - quasigroup of order 16, neoe type and
          vector of leaders $L = (l_1, l_2, \dots l_n)$
Output:   S
   For all possible input blocks $x_1, x_2$ in lexicographic ordering
     $(p_1, p_2) = (x_1, x_2)$
     For $i = 1$ to $n$
       If $i$ is odd
         $(t_1, t_2) = e_{l_i}(p_1, p_2)$
       else
         $(p_2, p_1) = e_{l_i}(t_2, t_1)$
 Use all output blocks from the last round to generate $S$
```

The construction of S^{-1} is given below (see Algorithm 4):

```
Algorithm 4. Construction of $S^{-1}$
Input:    Q - quasigroup of order 16, neoe type and
          vector of leaders $L = (l_1, l_2, \dots l_n)$
Output:   $S^{-1}$
   For all possible input blocks $x_1, x_2$ in lexicographic ordering
     $(p_1, p_2) = (x_1, x_2)$
     For $i = n$ down to 1
       If $n$ is even
         If $i$ is even
           $(t_2, t_1) = d_{l_i}(p_2, p_1)$
         else
          $(p_1, p_2) = d_{l_i}(t_1, t_2)$
       else
         If $i$ is odd
           $(t_1, t_2) = d_{l_i}(p_1, p_2)$
         else
           $(p_2, p_1) = d_{l_i}(t_2, t_1)$
 Use all output blocks from the last round to generate $S^{-1}$
```

The results for 8-bit S-boxes with best examined cryptographic properties for each $n = \{1, \dots, 7\}$ are presented in Table 3, while one of the best produced 8x8 S-boxes is S2 (Table 4), obtained by 5 e quasigroup transformations, alternating in normal and reverse mode, with consecutive leaders (3, 2, 0, 10, 9). This S-box is with differential uniformity 8, nonlinearity 98 (linearity 60), autocorrelation 88, maximal and minimal algebraic degree 7, and without fixed points.

Table 3. The best results for S-boxes obtained by Method 3

Type	NL(S)	L(S)	$\Delta(S)$	AC(S)	$max\{deg(f_i)\}$	deg(S)	No. of S
1e	32	192	34	256	6	3 2	5 11
1oe	32	192	34	256	6	3 2	5 11
2eoe	96 94	64 68	10	96 88	7	6	2 1
3eoe	98 96	60 64	10	96 88	7	7 (6)	0 (2) 2 (12)
4eoe	98	60	10	88	7	7 6	1 5
5eoe	98	60	8	88	7	7	1
6eoe	98	60	8 10	96 80	7	7 (6)	1 (3) 2 (0)
7eoe	98	60	8	88	7	7 6	2 5

Table 4. Some best S-boxes obtained by Method 1 and Method 2

S-box S1	S-box S2

Q34, 13eoe,
$L = (0, 3, 2, 3, 3, 3, 1, 1, 0, 2, 0, 0, 0)$
NL (L) = 98 (60),
$\Delta = 8$, AC = 88, deg = 7
`47 04 69 8D 30 CF E0 2B D6 1C C2 E8 79 56 32 6A`
`FC F5 52 10 19 8A 9C 01 AB 7A 9E 7B 55 EC 63 8F`
`26 BA 21 AE E2 D3 A9 C5 0E C3 45 44 FA 31 DD D5`
`DE 48 39 DF 2E C9 D9 46 77 B2 BC CA 17 FE A8 BE`
`CC 94 11 0C 97 E4 A5 25 8E F9 CB 14 3B 99 12 FB`
`8C 54 AA E1 6E F0 38 87 7D BB 08 EA 73 A1 5E 96`
`A0 3F D8 6C 05 1B 34 A6 1E AF 7F E9 37 AC 4E 23`
`A2 15 80 9A DA A4 0B 6D C8 81 E7 5D FD 9D 68 67`
`51 93 3A 03 71 C4 A3 BD 50 C7 36 5B 86 9B 06 6B`
`66 E3 62 85 1D 3D EE 0F D2 40 A7 C6 B8 91 29 B1`
`B3 5A D4 84 B5 49 28 B7 3E 27 CD 18 F4 2F 02 B4`
`2C D0 F7 74 70 64 EB 92 D7 F2 78 65 C1 4B E6 2D`
`E5 98 7C BF 4F 20 4D 60 1F 4A 07 0A 61 22 89 F6`
`7E 4C DB 5C 0D 75 6F 76 83 9F EF 95 C0 00 59 41`
`90 5F 1A 42 2A 53 F3 DC 35 16 88 33 F1 B6 FF AD`
`B0 F8 B9 24 8B 43 58 57 13 09 D1 82 ED 3C CE 72`
	5eoe,
	$L = (3, 2, 0, 10, 9)$
	NL (L) = 98 (60),
	$\Delta = 8$, AC = 88, deg = 7
	`0B A2 4C FA 57 C2 87 27 9C D9 A9 5E 96 31 32 59`
	`B7 9A DF 6E 04 E1 A6 23 6B 6A 4D 12 ED 74 0C 43`
	`A7 14 B0 B9 A1 CA 81 EA 8D FB E8 6D 13 52 3B 8E`
	`35 9B 39 2F EE E2 42 BC 11 F5 BD E9 90 4E 1E 1B`
	`C1 DB 97 34 68 FD 2B 05 FF A4 01 0F C6 8B 49 53`
	`88 66 E7 F7 55 A0 26 AD A3 69 22 28 EB CF 70 37`
	`95 D7 FE 78 92 FC 93 83 5C 7A B4 F2 41 1F 38 67`
	`85 D1 60 D5 D4 BA BE 25 C4 40 F4 48 8A 58 AE 5A`
	`C7 B1 1A 51 AB D6 0A 9E 3A 6C 16 19 F8 8F 62 84`
	`AA 2A F3 E3 1D 79 7C 45 E6 C8 4F 33 80 B5 76 7D`
	`A8 06 18 46 5D 3D 10 E0 2C D0 2E 03 CC 24 7F DD`
	`61 72 00 20 E5 9D D8 75 02 EC 2D 73 64 8C 9F 09`
	`B8 15 0E C5 56 C9 CE 17 5B B2 7B 3F 07 44 CD A5`
	`08 21 3E AC E4 B3 89 82 1C 0D D2 30 BF BB 47 C3`
	`B6 F9 65 63 50 91 99 DC 36 98 EF 54 6F 29 F0 F6`
	`3C 5F CB 71 7E AF DA 77 F1 4B C0 94 86 D3 4A DE`

5 New Construction

Our new construction of N-bit S-boxes is a generalization of the constructions with e quasigroup string transformations (and d quasigroup string transformations used for the inverse S-boxes) (see Algorithm 5). We mixed two different layers – the layer of bijectional quasigroup string transformations, and the layer of modular addition with N-bit constants. We choose a quasigroup of order q, such that $N = w{\cdot}log2(q)$. In any other case, we have $q = N$ and $w = 1$. We choose a vector of n bijectional quasigroup string transformations $T = (qst_1, qst_2, \dots, qst_n)$, which has a corresponding vector of inverse quasigroup string transformations $T^{-1} = (qst_1^{-1}, qst_2^{-1}, \dots, qst_n^{-1})$.

Algorithm 5. New construction of N-bit S-box

Input: Q - quasigroup of order q, vector of n bijectional quasigroup string transformations $T = (qst_1, qst_2, \dots, qst_n)$, vector of leaders $L = (l_1, l_2, \dots l_n)$ and vector of n-bit constants $C = (c_0, c_1, c_2, \dots c_n)$

Output: S

```
For all possible input blocks $x_1, x_2, \dots, x_w$ in lexicographic ordering
  $(p_1, p_2, \dots, p_w) = (x_1, x_2, \dots, x_w) + c_0 (mod\ \ 2^N)$
  For $i = 1$ to $n$
    If $i$ is odd
      $(t_1, t_2, \dots, t_w) = (qst_i)_{l_i}(p_1, p_2, \dots, p_w) + c_i (mod\ \ 2^N)$
    else
      $(p_w, \dots, p_2, p_1) = (qst_i)_{l_i}(t_w, \dots, t_2, t_1)$
      $(p_1, p_2, \dots, p_w) = (p_1, p_2, \dots, p_w) + c_i (mod\ \ 2^N)$
Use all output blocks from the last round to generate $S$
```

The construction of the S^{-1} is given below (Algorithm 6):

```
Algorithm 6. Construction of $S^{-1}$
Input:  Q - quasigroup of order $q$, vector of $n$ bijectional quasigroup
        string transformations $T = (qst_1, qst_2, \dots, qst_n)$, vector of leaders
        $L = (l_1, l_2, \dots l_n)$ and vector of $n$-bit constants $C = (c_0, c_1, c_2, \dots c_n)$
Output: $S^{-1}$
  For all possible input blocks $x_1, x_2, \dots, x_w$ in lexicographic ordering
   $(p_1, p_2, \dots, p_w) = (x_1, x_2, \dots, x_w) - c_n (mod\ \ 2^N)$
   For $i = n$ down to 1
     If $n$ is even
       If $i$ is even
         $(t_w, \dots, t_2, t_1) = (qst_i^{-1})_{l_i}(p_w, \dots, p_2, p_1) - c_{i-1}(mod\ \ 2^N)$
       else
         $(p_1, p_2, \dots, p_w) = (qst_i^{-1})_{l_i}(t_1, t_2, \dots, t_w) - c_{i-1}(mod\ \ 2^N)$
     else
       If $i$ is odd
         $(t_1, t_2, \dots, t_w) = (qst_i^{-1})_{l_i}(p_1, p_2, \dots, p_w) - c_{i-1}(mod\ \ 2^N)$
       else
         $(p_w, \dots, p_2, p_1) = (qst_i^{-1})_{l_i}(t_w, \dots, t_2, t_1) - c_{i-1}(mod\ \ 2^N)$
  Use all output blocks from the last round to generate $S^{-1}$
```

Method 3 – The third method generates 8-bit S-boxes by using our new construction with parameters $N = 8$, $q = 4$, $w = 4$ and by using only e quasigroup string transformations generated by quasigroups of order 4. Method 1 can be seen as a special case of the Method 3, where all used constants are zeros. The results for 8-bit S-boxes with best examined crypographic properties for each $n = \{1, \dots, 4\}$ and several different constant vectors, are presented in Table 5.

Method 4 – The fourth method generates 8-bit S-boxes by using our new construction with parameters $N = 8$, $q = 16$, $w = 2$ and by using only e quasigroup string transformations generated by the quasigroup of order 16 (Figure 2). Method 2 can be seen as a special case of Method 4, where all used constants are zeros. The results for 8-bit S-boxes with best examined crypographic properties for each $n = \{1, \dots, 5\}$ and several different constant vectors, are presented in Table 6. The best produced 8x8 S-boxes are obtained by only 3 e quasigroup transformations, alternating in normal and reverse mode. There are two different best groups. One group has differential uniformity 8, nonlinearity 98 (linearity 60), autocorrelation 88, and minimal algebraic degree 7. One representative of this group is S3 (Table 7), ob-

Table 5. Method 3 – part of the results

Type	NL(S)	L(S)	$\Delta(S)$	AC(S)	$max\{deg(f_i)\}$	deg(S)	No. of S
1e, $C = (0, c_1)$	4 32	248 192	132 164	256	7	3	6144 1536
1e, $C = (c_0, c_1)$	64	128	64	216	7	6	640
2eoe, $C = (0, 0, c_2)$	64	128	128	256	7	3	3968
3eoe, $C = (0, 0, 0, c_3)$	80	96	32	152	7	6	32
3eoe, $C = (0, c_1, 0, c_3)$	88	80	18	128	7	6	64
4eoe, $C = (0, 0, 0, 0, c_4)$	88	80	24	160	7	5	32
5eoe, $C = (0, 0, 0, 0, 0, c_5)$	96	64	10 12	96 88	7	6	32 32
6eoe, $C = (0, 0, 0, 0, 0, 0, c_6)$	98	60	10	88	7	6	32
7eoe, $C = (0, 0, 0, 0, 0, 0, 0, c_7)$	98	60	10	88	7	7	3056

tained by using leaders $(5, 1, 5)$ and constants $(0, 1, 90, 9)$. The second group has differential uniformity 10, nonlinearity 100 (linearity 56), autocorrelation 88, minimal algebraic degree 6, and maximal algebraic degree 7. One representative of this group is S4 (Table 7), obtained by using leaders $(13, 3, 7)$ and constants $(0, 8, 136, 70)$.

6 Conclusion

The main contribution of this paper is a new generic construction of N-bit S-boxes, presented with mixed layers of bijective quasigroup string transformations and modular addition with N-bit constants. Special case of 8-bit S-boxes are investigated, together with their main cryptographic properties. The results are very promising, and further experiments are needed to obtain 8-bit S-boxes with even better cryptographic properties. This can be done, because only a very small subset of S-boxes produced by only one specially selected quasigroup of order 16, and also, very small subset of S-boxes produced by quasigroups of order 4 with several constant vectors are investigated.

References

[1] V. D. Belousov, *Foundations of quasigroups and loops*, Moscow: Nauka, 1967.

[2] E. Biham and A. Shamir, “Differential cryptanalysis of DES-like cryptosystems,” *J. Cryptology*, vol. 4, no. 1, pp. 3–72, 1991.

[3] A. Bogdanov, L.R. Knudsen, G. Le, C. Paar, A. Poschmann, M.J.B. Robshaw, Y. Seurin, and C. Vikkelsoe, “PRESENT: An Ultra-Lightweight Block Cipher,” in *Cryptographic Hardware and Embedded Systems - CHES 2007. CHES 2007* (Lecture Notes in Computer Science, vol 4727), P. Paillier and I. Verbauwhede, Eds. Berlin Heidelberg: Springer, 2007, pp. 450–466. https://doi.org/10.1007/978-3-540-74735-2_31.

Table 6. Method 4 – part of the results

Type	NL(S)	L(S)	$\Delta(S)$	AC(S)	$max\{deg(f_i)\}$	deg(S)	No. of S
1e, $C = (0, c_1)$	64	128	26	240	7	6	32
1e, $C = (c_0, 0)$	64	128	26	232	7	6	24
1e, $C = (c_0, c_1)$	84	88	18	200	7	6	16
2eoe, $C = (0, 0, c_2)$	98	60	10	96	7	6	12
2eoe, $C = (c_0, c_1, c_2)$	100 98 98	56 60 60	10 8 10	104 96 88	7	6	24 56 72540
3eoe, $C = (0, 0, 0, c_3)$	98	60	10	88	7	7	12
3eoe, $C = (0, c_1, c_2, 0)$	98	60	8	96	7	7	256
3eoe, $C = (0, 93, c_2, c_3)$	98	60	8	96	7	7	1024
3eoe, $C = (0, 0..12, c_2, c_3)$	100 98	56 60	10 8	88	7	6 7	4 20
4eoe, $C = (0, 0, 0, 0, c_4)$	98	60	10	88	7	7 6	368 856
4eoe, $C = (0, 0, c_2, 0, 0)$	98	60	8 10	96 88	7	7 (6)	0 (2) 327 (860)
4eoe, $C = (0, 0, c_2, 0, c_4)$	98	60	8	88	7	7	28
5eoe, $C = (0, 0, 0, 0, 0, c_5)$	98	60	8	88	7	7	4

Table 7. Some best S-boxes obtained by Method 4

S-box S3	S-box S4
3eoe, $L = (5, 1, 5)$, $C = (0, 1, 90, 9)$ NL (L) = 98 (60), $\Delta = 8$, AC = 88, deg = 7 71 6B 60 A1 27 FA B6 C4 F3 16 D3 3E 08 DC D9 BC 85 B7 B9 90 2E CA A6 BE D5 A7 1D 1A D1 03 37 58 65 78 67 22 52 76 4B 42 F9 7D BB DF 54 F4 11 56 DD E5 38 BF 61 3A 9B 18 CC 29 19 BD FF ED D4 33 F0 B1 CD 53 3C 24 6A 05 2C 9F 12 F5 91 10 94 C0 1C 4F AF 2F 63 6C 21 84 86 2B 96 44 4D A4 25 14 A5 9E AB 5A AD 72 81 49 45 40 0C 0B E7 7E 2D DB C8 9D 04 B0 4E 8F 39 CE C7 34 DE 01 AE EA 77 B5 F2 A0 E4 8A 7B 23 EF 97 3B E1 D2 5E 80 9A 68 00 99 1B FD 1E FE C1 C9 0F 4C 8D 70 59 98 31 79 0A 6E CB B2 C3 07 3F 17 09 E6 89 57 FB 5D 35 AC E8 C5 E0 F6 43 0D 8E 69 6D 0E B4 D8 E3 EE 95 88 B8 BA 50 93 DA 47 CF 5C F8 87 28 C2 15 C6 F7 51 02 E9 66 FC 30 75 8C 9C 6F 55 54 1F AA 7A 5F 7C 32 EB 73 20 46 A8 5B 82 41 8B 74 D6 2A 83 A2 4A A9 D7 13 48 92 26 E2 D0 A3 64 F1 62 EC 06 3D 7F B3	3eoe, $L = (13, 3, 7)$, $C = (0, 8, 136, 70)$ NL (L) = 100 (56), $\Delta = 10$, AC = 88, deg = 6 87 DD 70 A3 98 3B F2 CF 4D C6 2E FE 1A 86 13 D0 51 95 79 65 44 B5 92 BE 48 B3 24 17 76 1E 4A 1B E9 61 60 F9 8E 91 DB 09 5E 4E 71 3A 39 D1 DF A4 E1 1F A6 A8 CE F8 C9 20 EA 53 C2 B1 0B EC 7D 4F AE 5D E0 7F D4 A2 94 03 29 D3 BA 77 43 A0 73 62 EE 8D AA 2B D6 6F AD 2A ED A9 55 47 96 25 68 AB 01 E8 0F 46 FC 26 CB 0E 42 04 B0 B8 E6 58 97 C3 78 DA 3C 16 63 9F 21 0D 93 E4 FF BF 0C 3E A7 C7 B6 02 80 B7 B9 38 7B D7 1C 57 33 C1 D8 90 14 F6 EF 54 28 83 40 59 E2 12 C5 18 2F BD 35 E3 19 8F AF 9A FB 37 4B 64 7E 6E 9D 30 41 B4 D2 E5 0A 5F 07 99 3F BB 2D BC D5 FD 6D 10 DC 67 B2 88 5B F3 27 34 84 36 22 81 05 F1 74 32 F4 89 66 C4 F5 11 1D EB 15 6A 69 2C CA 56 D9 82 3D E7 5C 6B 5A 85 DE 7A 6C 72 F7 9B 45 AC 4C 08 CD F0 23 31 FA 8A 52 9C 00 50 8C 49 75 A5 C8 C0 8B 9E A1 CC 7C 06

[4] A. Breaken, “Cryptographic properties of Boolean Functions and S-boxes,” Ph.D. dissertation, Katholieke Universiteit Leuven, 2006.

[5] A. Canteaut, S. Duval and G. Leurent, “Construction of Lightweight S-Boxes using Feistel and MISTY structures (Full Version),” *Cryptology ePrint Archive*, Report 2015/711, 2015.

[6] F. Chabaud and S. Vaudenay, “Links between differential and linear cryptanalysis,” in *Advances in Cryptology - EUROCRYPT 1994* (Lecture Notes in Computer Science, vol. 950), Springer-Verlag, 1995, pp. 356–365.

[7] J.A. Clark, J.L. Jacob, and S. Stepney, “The design of s-boxes by simulated annealing,” *New Generation Computing*, vol. 23, no. 3, pp. 219–231, 2004.

[8] J. Daemen, R. Govaerts, and J. Vandewalle, “Correlation matrices,” in *FSE 1994* (Lecture Notes in Computer Science, vol. 1008), B. Preneel, Ed. Berlin Heidelberg: Springer, 1994, pp. 275–285.

[9] J. Daemen, “Cipher and Hash Function Design. Strategies based on Linear and Differential Cryptanalysis,” Ph.D. dissertation, Katholieke Universiteit Leuven, 1995.

[10] J. Daemen and V. Rijmen, *The Design of Rijndael: AES*, The Advanced Encryption Standard. Springer-Verlag, 2002.

[11] R.A. de la Cruz Jimenez, “Generation of 8-Bit S-Boxes Having Almost Optimal Cryptographic Properties Using Smaller 4-Bit S-Boxes and Finite Field Multiplication,” in *Progress in Cryptology - LATINCRYPT 2017* (Lecture Notes in Computer Science, vol.11368), T. Lange, O. Dunkelman, Eds. Cham: Springer, 2017.

[12] H. Dobbertin, “One-to-one highly nonlinear power functions on GF(2n),” *Appl. Algebra Engrg. Comm. Comput.*, vol. 9, pp. 139–152, 1998.

[13] J. Fuller and W. Millan, “Linear redundancy in S-boxes,” in *Fast Software Encryption 2003 (FSE’03)* (Lecture Notes in Computer Science, vol. 2887), T. Johansson, Ed. Berlin Heidelberg: Springer, 2003, pp. 74–86.

[14] D. Gligoroski, S. Markovski, and L. Kocarev, “Edon-R, an Infinite Family of Cryptographic Hash Functions,” in *The Second NIST Cryptographic Hash Workshop*, (UCSB, Santa Barbara, CA), 2006.

[15] G. Ivanov, N. Nikolov, and S. Nikova, “Reversed genetic algorithms for generation of bijective S-boxes with good cryptographic properties,” *Cryptogr. Commun.*, vol. 8, no. 2, pp. 247–276, 2016.

[16] G. Ivanov, N. Nikolov, and S. Nikova, “Cryptographically Strong S-Boxes Generated by Modified Immune Algorithm,” in *Cryptography and Information Security in the Balkans* (Lecture Notes in Computer Science, vol. 9540), 2016, pp. 31–42.

[17] H. Isa, N. Jamil, and M. Z’aba, “Hybrid Heuristic Methods in Constructing Cryptographically Strong S-boxes,” *International Journal of Cryptology Research*, vol. 6, no. 1, pp. 247–276, 2016.

[18] O.V. Kazymyrov, V.N. Kazymyrova, and R.V. Oliynykov, “A method for generation of high-nonlinear S-Boxes based on gradient descent,” *Mat. Vopr. Kriptogr.*, vol. 5, no. 2, pp. 71–78, 2014.

[19] G. Leander and A. Poschmann, “On the Classification of 4 Bit S-Boxes,” in *Arithmetic of Finite Fields* (Lecture Notes in Computer Science, vol. 4547), C. Carlet, B. Sunar, Eds. Berlin Heidelberg: Springer, 2007, pp. 159–176.

[20] S. Markovski, D. Gligoroski, and S. Andova, “Using quasigroups for one-one secure encoding,” in *VIII Conf. Logic and Computer Science LIRA 1997*, (Novi Sad, Serbia), 1997, pp. 157–162.

[21] M. Matsui, “Linear Cryptanalysis Method for DES Cipher,” in *Advances in Cryptology, EUROCRYPT 1993* (Lecture Notes in

Computer Science, vol. 765), T. Helleseth, Ed. Berlin Heidelberg: Springer, 1993, pp. 386–397.

[22] W. Meier and O. Staffelbach, "Nonlinearity criteria for cryptographic functions," in *Workshop on the theory and application of cryptographic techniques on Advances in cryptology*, New York, USA: Springer-Verlag New York, Inc., 1990, pp. 549–562.

[23] A. Menyachikhin, "Spectral-linear and spectral-difference methods for generating cryptographically strong S-Boxes," in *Preproceedings of CTCrypt'16*, (Yaroslavl, Russia), 2016, pp. 232–252.

[24] W. Millan, "How to improve the nonlinearity of bijective S-boxes," in *Third Australian Conference on Information Security and Privacy 1998* (Lecture Notes in Computer Science, vol. 1438), Springer-Verlag, 1998, pp. 181–192.

[25] A. Mileva, "Analysis of Some Quasigroup Transformations as Boolean Functions," *Math. Balkanica*, vol. 26, Fasc. 3-4, 359–368, 2012.

[26] H. Mihajloska and D. Gligoroski, "Construction of Optimal 4-bit S-boxes by Quasigroups of Order 4," in *SECURWARE 2012*, 2012.

[27] K. Nyberg, "Perfect nonlinear S-boxes," in *Eurocrypt 1991* (Lecture Notes in Computer Science, vol. 547), D.W. Davies, Ed. Springer, 1991, pp. 378–385.

[28] K. Nyberg, "Differentially uniform mappings for cryptography," in *Advances in Cryptology - EUROCRYPT 1993* (Lecture Notes in Computer Science, vol. 765), Springer-Verlag, 1994, pp. 55–64.

[29] K. Nyberg, "S-boxes and round functions with controllable linearity and differential uniformity," in *FSE 1995* (Lecture Notes in Computer Science, vol. 1008), B. Preneel, Ed., Berlin Heidelberg: Springer, 1995, pp. 111–130.

[30] B. Preneel, "Analysis and Design of Cryptographic Hash Functions," Ph.D. dissertation, Katholieke Universiteit Leuven, 1994.

[31] O.S. Rothaus, “On ”bent” functions,” *J. Comb. Theory, Ser. A*, vol. 20, no. 3, pp. 300–305, 1976.

[32] P. Tesař, “A new method for generating high non-linearity S-boxes,” *Radioengineering*, vol. 19, no. 1, pp. 23–26, 2010.

[33] L. Qu, Y. Tan, C. Tan, and C. Li, “Constructing differentially 4-uniform permutations over $\mathbb{F}_2^{2^k}$ via the switching method,” *IEEE Transactions on Inform. Theory*, vol. 59, no. 7, pp. 4675–4686, 2013.

Aleksandra Mileva, Aleksandra Stojanova,
Dušan Bikov, Yunqing Xu

Received June 25, 2020
Accepted August 23, 2020

Aleksandra Mileva
Faculty of Computer Science, University ”Goce Delcev”
Stip, Republic of N. Macedonia
Phone: ++38932550106
E–mail: aleksandra.mileva@ugd.edu.mk

Aleksandra Stojanova
Faculty of Computer Science, University ”Goce Delcev”
Stip, Republic of N. Macedonia
Phone: ++38932550123
E–mail: aleksandra.stojanova@ugd.edu.mk

Dušan Bikov
Faculty of Computer Science, University ”Goce Delcev”
Stip, Republic of N. Macedonia
E–mail: dusan.bikov@ugd.edu.mk

Yunqing Xu
Ningbo University, Peoples Republic of China
Ningbo, Peoples Republic of China
E–mail: xuyunqing@nbu.edu.cn