R. A. de la Cruz Jiménez, Построение 8-битовых подстановок, 8-битовых инволюций и 8-битовых ортоморфизмов с почти оптимальными криптографическими параметрами, *Матем. вопр. криптогр.*, 2021, том 12, выпуск 3, 89–124

DOI: 10.4213/mvk377

МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2021 Т. 12 № 3 С. 89–124

УДК 519.719.2 DOI https://doi.org/10.4213/mvk377

Constructing 8-bit permutations, 8-bit involutions and 8-bit orthomorphisms with almost optimal cryptographic parameters*

R. A. de la Cruz Jiménez

Institute of Cryptography, Havana University, Cuba

Получено 22.XI.2020

Abstract. Nonlinear bijective transformations are crucial components in the design of many symmetric ciphers. To construct permutations having cryptographic properties close to the optimal ones is not a trivial problem. We propose a new construction based on the well-known Lai – Massey structure for generating binary permutations of dimension $n = 2k$, $k \geqslant 2$. The main cores of our constructions are: the inversion in $\mathbb{F}_{2^k}$, an arbitrary k-bit non-bijective function (which has no preimage for 0) and any k-bit permutation. Combining these components with the finite field multiplication, we provide new 8-bit permutations with high values of its basic cryptographic parameters. Also, we show that our approach may be used for constructing 8-bit involutions and 8-bit orthomorphisms that have strong cryptographic properties.

Keywords: S-Box, permutation, involution, orthomorphism

Построение 8-битовых подстановок, 8-битовых инволюций и 8-битовых ортоморфизмов с почти оптимальными криптографическими параметрами

Р. А. де ла Крус Хименес

Институт криптографии, Гаванский университет, Куба

Аннотация. Нелинейные биективные преобразования являются важным структурным элементом при синтезе современных шифрсистем. Задача построения S-боксов с близкими к оптимальным значениям криптографических параметров нетривиальна. Предлагается новая конструкция для построения двоичных нелинейных биективных преобразований размерностей $n = 2k, k \geqslant 2$, основанная на схеме Лаи – Месси. Основные узлы предлагаемой конструкции — функция обращения элемента в конечном поле $\mathbb{F}_{2^k}$, k-битовое небиективное отображение без прообраза для нулевого элемента поля $\mathbb{F}_{2^k}$ и произвольная k-битовая

* The article was submitted by the Organizing Committee of the Symposium CTCrypt'2020.

Citation: Matematicheskie Voprosy Kriptografii, 2021, v. 12, № 3, pp. 89–124 (Russian)

подстановка. Комбинация этих компонентов с операцией умножения в конечном поле позволяет найти 8-битовые подстановки, 8-битовые инволюции и 8-битовые ортоморфизмы, имеющие высокие значения основных криптографических параметров.

Ключевые слова: S-бокс, подстановка, инволютивная подстановка, ортоморфизм

Introduction

Modern block ciphers realize iterations of several rounds. Each round (which should depend on the key) consists of a confusion layer and a diffusion layer. The confusion layers are usually formed by local nonlinear mappings (S-Boxes) while the diffusion layers are formed by global linear mappings mixing the output of the different S-Boxes. Block ciphers may be built using a well-known structure such as a Feistel network and its variants (see, e.g. [1]), a Substitution-Permutation network (SPN) [1], or a Lai – Massey structure [48]. Cryptographic properties of S-boxes deal with the application of several logical attacks on ciphers, namely, linear attack [27], differential attack [27], higher order differential attack [30], and algebraic attack [10] (which is not yet efficient but represents some threat and should be keeped in mind by designers of next generation block ciphers). For this reason S-boxes should satisfy various criteria for providing high level of protection against such attacks.

Besides the linear, differential and algebraic attacks, today the most prominent attacks on the cryptographic algorithms are based on supervision of physical processes in cryptographic device. In literature, this kind of attack has received the name of side-channel attacks (SCAs). Examples of such attacks are: Simple Power Analysis (SPA) [28], Differential Power Analysis (DPA) [28], Timing Analysis (TA) [29] , Correlation Power Analysis (CPA) [7], Mutual Information Attack (MIA)[15]. S-boxes represent the most vulnerable part in an implementation when considering side-channel adversary and it is not a trivial task to construct S-boxes having good resistive properties for classical cryptanalysis as well as for side-channel attacks.

The known methods for constructing S-boxes may be divided into four main classes: algebraic constructions, pseudo-random generation, heuristic techniques and constructions from small to large S-boxes. Each approach has its advantages and disadvantages. In this paper we propose (using the last approach) a new construction based on the Lai – Massey structure for generating ordinary permutations, involutions and orthomorphisms with strong cryptographic properties and therefore study the resilience of such construction against side-channel attacks in terms of its masking complexity.

This paper is structured as follows. In Section 1 we give the basic definitions. In Section 2, we present our design criteria. In section 3 we present a new class of permutations which may be used for constructing ordinary S-boxes, involutions and orthomorphisms with high values of its basic cryptographic parameters. In this section, we also derive some properties of the suggested class of permutations. In Section 4 we give some examples of 8-bit S-boxes constructed by our approach. The masking complexity of our S-boxes is estimated in Section 5. We conclude in Section 6.

1. Basic definitions and notation

Let V_n be n-dimensional vector space over the field $\mathbb{F}_2$ and $V_n^* = V_n \setminus \{0\}$. By $S(V_n)$ we denote the symmetric group on V_n. The finite field of size 2^n is denoted by $\mathbb{F}_{2^n}$, where $\mathbb{F}_{2^n}{=}\mathbb{F}_2[\xi]/g(\xi)$ for some irreducible polynomial $g(\xi)$ of degree n. We use the notation $\mathbb{Z}/2^n$ for the ring of integers modulo 2^n. The set of all binary bijective linear maps $V_n \to V_n$ is denoted by $\mathsf{GL}_n(\mathbb{F}_2)$. Given a natural number l, throughout the article we shall use the following operations and notation:

$\#A$	- cardinality of a set A,
$\lfloor u \rfloor$	- integer part of a real number u,
$a\|b$	- concatenation of vectors a, b of V_l, i. e., a vector from V_{2l},
0	- the null vector of V_l,
$\oplus$	- bitwise eXclusive-OR, i. e. addition in $\mathbb{F}_{2^l}$,
$\langle a, b\rangle$	- the scalar product of vectors $a = (a_0, \ldots, a_{l-1}), b = (b_0, \ldots, b_{l-1})$ from V_l: $\langle a, b\rangle = \bigoplus_{i=0}^{l-1} a_i b_i \in \mathbb{F}_2$,
$\otimes$	- finite field multiplication,
$\Lambda \circ \Psi$	- a composition of mappings, where Ψ is the first to operate,
Ψ^{-1}	- the inverse transformation for some bijective mapping Ψ,
$\chi(\Phi_1, \Phi_2)$	- the Hamming distance between $\Phi_1, \Phi_2 \in S(V_l)$,
$\mathsf{ord}(a)$	- the multiplicative order of the element $a \in \mathbb{F}_{2^l}$.

There are bijective mappings between $\mathbb{Z}/2^n, V_n$ and $\mathbb{F}_{2^n}$ defined by the correspondences

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

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

We define the indicator function

$$\mathsf{Ind}(x,y)=\begin{cases}1, & \text{if} \quad x=y,\\ 0, & \text{if} \quad x\neq y.\end{cases}$$

Now, we introduce some basic concepts necessary to describe and analyze S-boxes with respect to linear, differential, and algebraic attacks. For this purpose, we consider an n-bit S-box Φ as a vector of Boolean functions:

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

For any fixed $i\in\{0,1,\dots,n-1\}$ the Boolean function f_i may be written as a sum over V_1 of distinct t-order products of its arguments, $0\leqslant t\leqslant n-1$; this representation is called the algebraic normal form (in brief, ANF) of f_i. The degree of the ANF of a Boolean function f with n variables is called the algebraic degree of f, is defined as the maximum order of terms appeared in its ANF [8], and is denoted by $d_{alg}(f)$.

Functions f_i written in (1) are called coordinate Boolean functions of the S-box Φ. It is well known that many the desirable cryptographic properties of Φ may be defined in terms of their linear combinations, also called S-box component functions (see [8, p. 112]).

Definition 1 ([8])**.** For $a,b\in V_n$ the Walsh transform $\mathcal{W}_\Phi(a,b)$ of an n-bit S-box Φ is defined as

$$\mathcal{W}_\Phi(a,b)=\sum_{x\in V_n}(-1)^{\langle b,\Phi(x)\rangle\oplus\langle a,x\rangle}. \tag{2}$$

Definition 2 ([8])**.** The nonlinearity of an n-bit S-box Φ, denoted by $\mathcal{NL}(\Phi)$, is defined as

$$\mathcal{NL}(\Phi)=2^{n-1}-\frac{1}{2}\cdot\max_{b\neq 0,a\in V_n}|\mathcal{W}_\Phi(a,b)|. \tag{3}$$

From a cryptographic point of view S-boxes with small values of Walsh coefficients offer better resistance against linear attacks [8].

Definition 3 ([5])**.** The differential uniformity (also called δ-uniformity) of an n-bit S-box Φ, denoted by δ_Φ, is defined as

$$\delta_\Phi=\max_{a\neq 0,b\in V_n}\Delta_\Phi(a,b), \tag{4}$$

where
$\Delta_\Phi(a,b)=\#\{x\in V_n|\,\Phi(x\oplus a)\oplus\Phi(x)=b\}=\sum_{x\in V_n}\mathsf{Ind}(\Phi(x\oplus a)\oplus\Phi(x),b)$.

The resistance offered by an S-box against differential attacks is related with 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 (see [5, 8]).

Definition 4 ([8])**.** The algebraic degree of an n-bit S-box Φ, denoted by $d_{alg}(\Phi)$, is defined as the maximal algebraic degree of the component functions Φ, that is

$$d_{alg}(\Phi) = \max_{a \neq 0 \in V_n} d_{alg}(\langle a, \Phi(x) \rangle). \tag{5}$$

Definition 5 ([8])**.** The minimum algebraic degree (often called the minimum degree) of an n-bit S-box Φ, denoted by $d_{min}(\Phi)$, is defined as the minimum algebraic degree of all the component functions, that is

$$d_{min}(\Phi) = \min_{a \neq 0 \in V_n} d_{alg}(\langle a, \Phi(x) \rangle). \tag{6}$$

It is well-known that $d_{min}(\Phi) \leqslant d_{alg}(\Phi)$ for any permutation $\Phi \in S(V_n)$, and these parameters are upper bounded by $n-1$ (see [8]). In general, S-boxes should have high values of $d_{min}(\cdot), d_{alg}(\cdot)$ because S-boxes with low values of these parameters are susceptible to algebraic attack, higher-order differential, interpolation, cube attacks, etc. (see [8, 12]).

Definition 6 ([8])**.** The univariate polynomial representation of an n-bit S-box Φ over $\mathbb{F}_{2^n}$ is defined in a unique fashion as

$$\Phi(X) = \sum_{i=0}^{2^n-1} \nu_i X^i, \nu_i \in \mathbb{F}_{2^n}, \tag{7}$$

where coefficients $\nu_i, i = 0, \ldots, 2^n - 1$, may be obtained from the n-bit S-box Φ by applying Lagrange's Interpolation theorem (see, for example, [8]).

Definition 7 ([34])**.** For $i > 0$ the $r_\Phi^{(i)}$ parameter of an n-bit S-box Φ is defined as

$$r_\Phi^{(i)} = \dim H_\Phi^{(i)}, \tag{8}$$

where

$$H_\Phi^{(i)} = \left\{ p \in \mathbb{F}_2[z_1, \ldots, z_{2n}] \middle| \forall x \in V_n, p(x, \Phi(x)) = 0, 0 < d_{alg}(p) \leqslant i \right\}.$$

Definition 8 ([34])**.** The r_Φ-parameter of an n-bit S-box Φ is defined as

$$r_\Phi = \min \left\{ i \middle| r_\Phi^{(i)} > 0 \right\}. \tag{9}$$

It is well-known that there exist certain methods of analysis of block ciphers (see [10]) exploiting the existence of polynomial relations involving the input x to the S-box Φ and its output $\Phi(x)$. In order to increase the strength of a block cipher against these methods we have to minimize parameters $r_\Phi^{(i)}, i = r_\Phi, \ldots, n$, and maximize parameters $d_{min}(\Phi)$ и r_Φ (see [24, 35, 37]).

It should be pointed that in [8, 43] the parameter r_Φ (defined in a slightly different way) is called graph algebraic immunity of Φ and is denoted by $AI_{gr}(\Phi)$ in these references.

Definition 9 ([25]). An element $x \in V_n$ is called a fixed point of an n-bit S-box Φ if $\Phi(x) = x$.

We denote by $\mathsf{FixP}(\Phi)$ the set of all fixed points of Φ, i. e., $\mathsf{FixP}(\Phi) = \{x \in V_n \mid \Phi(x) = x\}$.

Definition 10 ([24]). Two n-bit S-boxes Φ_1 and Φ_2 are linear (respectively, affine) equivalent if there exist linear (respectively, affine) mappings A_1, A_2 such that $\Phi_2 = A_2 \circ \Phi_1 \circ A_1$.

It is well-known (see, e.g., [8]) that the following cryptographic parameters: δ-uniformity, nonlinearity and (minimum) algebraic degree — remain invariant under linear (respectively, affine) equivalence.

2. General S-box Design Criteria

Our goal is to find $2k$-bit permutations constructed from k-bit ones that satisfy the following criteria (which in what follows are called almost optimal).

1) Maximum value of minimum degree.

2) Maximum value of r_Φ with the minimum value of $r_\Phi^{(i)}$.

3) Minimum value of δ-uniformity limited by parameter listed above.

4) Maximum value of nonlinearity limited by parameter listed above.

For example,when $n = 8$ an almost optimal nonlinear bijective transformation Φ should satisfy the following

Set of cryptographic criteria for 8-bit permutations:

- $d_{min}(\Phi) = 7$,
- $\delta_\Phi \leqslant 8$,
- $r_\Phi = 3$ with $r_\Phi^{(3)} = 441$,
- $\mathcal{NL}(\Phi) \geqslant 100$.

Our design criteria are basically the same as those included in the target set of criteria for the Gradient descent method [24]. However, we concentrate on generating 8-bit S-boxes with almost optimal cryptographic parameters having good resistance properties both against classical cryptanalysis as well as side-channel attacks with some given level of masking.

3. Construction of permutations, involutions and orthomorphisms

Now, we present a special algorithmic-algebraic scheme based on the well-known Lai – Massey structure which may be used not only for constructing permutations, but also involutions and orthomorphisms having almost optimal cryptographic properties.

Let $n = 2k$ be a natural number, where $k \geqslant 2$. Choose:

– finite field inversion function $\mathcal{I}(x) = \begin{cases} 0, & \text{if} \quad x = 0, \\ x^{-1}, & \text{if} \quad x \neq 0, \end{cases}$ over $\mathbb{F}_{2^k}$,

– non-bijective k-bit function ψ which has no preimage for 0,

– arbitrary permutation $h \in S(V_k)$,

– arbitrary bijective linear maps $\mathcal{L}_i \in \mathsf{GL}_{2k}(\mathbb{F}_2), i = 1, 2$.

We construct the following class of $2k$-bit permutations π from V_{2k} to V_{2k} as follows.

Construction of $\hat{\pi}$
For the input value $(l\|r) \in V_{2k}$ we define the corresponding output value $\hat{\pi}(l\|r) = (l_1\|r_1)$ as a result of the following computations:
$(l_1\|r_1) := \mathcal{L}_1(l\|r)$;
$(l_1\|r_1) := (\mathcal{I}(l_1) \otimes \psi(l_1 \otimes r_1))\big\|h(r_1 \otimes \psi(l_1 \otimes r_1))$;
$(l_1\|r_1) := \mathcal{L}_2(l_1\|r_1)$.

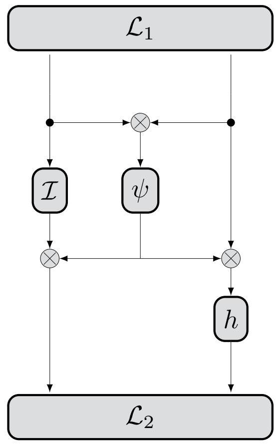

Fig. 1. High level structure of the S-box $\hat{\pi}$

Notice that the finite field multiplication $\otimes$ in the above construction correspond to multiplication operation in $\mathbb{F}_{2^k}$. The binary matrices $\mathcal{L}_1$ and $\mathcal{L}_2$ were inserted to break the cycle structure of π and also to eliminate the existence of fixed points. Defining π as $\mathcal{L}_2^{-1} \circ \hat{\pi} \circ \mathcal{L}_1^{-1}$ we can see in Fig. 1 that π share similarities with 1-round Lai – Massey structure replacing in the latter the XORs by finite field multiplications. The non-bijective k-bit function ψ (which has no preimage for 0) was chosen in such a way to make the whole structure invertible. Moreover, from the following construction:

- $\pi^{-1}(l_1\|r_1) = l\|r$, where
  $l = h^{-1}(l_1) \otimes \mathcal{I}\big(\psi(h^{-1}(l_1) \otimes \mathcal{I}(r_1))\big), r = \mathcal{I}\big(r_1 \otimes \mathcal{I}\big(\psi(h^{-1}(l_1) \otimes \mathcal{I}(r_1))\big)\big)$,

we can easily derive the bijectivity of the π which is a necessary design criteria for SPN ciphers and quite useful for Feistel and Lai – Massey ciphers.

In more detail, the nonlinear bijective transformation π may be written as follows:

$$\pi(l\|r) = \begin{cases} 0, & \text{if} \quad l = r = 0, \\ 0\big\|h(r \otimes \psi(0)), & \text{if} \quad l = 0 \text{ and } r \neq 0, \\ \big(\mathcal{I}(l) \otimes \psi(0)\big)\big\|0, & \text{if} \quad l \neq 0 \text{ and } r = 0, \\ (\mathcal{I}(l) \otimes \psi(l \otimes r))\big\|h(r \otimes \psi(l \otimes r)), & \text{if} \quad l \neq 0 \text{ and } r \neq 0. \end{cases} \tag{10}$$

In what follows (and also in the remainder of this paper) we restricted ourselves to the case when $h = \mathcal{I}$ and we shall write π_ψ instead of π.

The next well-known result is useful when studying some properties of the suggested class of permutations.

Lemma 1 ([3, 31]). *For any $b \in V_n^*, a \in V_n$, the following inequality holds*:

$$\left|\sum_{x \in V_k} (-1)^{\langle b, \mathcal{I}(x)\rangle \oplus \langle a, x\rangle}\right| \leqslant \lfloor 2^{\frac{k}{2}+1} \rfloor. \tag{11}$$

Proposition 1. *For any mapping $\psi \colon V_k \to V_k^*$ the following inequality holds*:

$$\mathcal{NL}(\hat{\pi}) \geqslant 2^k - \lfloor 2^{\frac{k}{2}+1} \rfloor - 1. \tag{12}$$

Proof. It is not difficult to see that permutations $\pi, \hat{\pi}$ are linear equivalent, hence $\mathcal{NL}(\hat{\pi}) = \mathcal{NL}(\pi_\psi)$. Let us calculate the Walsh transform of the nonlinear bijective transformation π

$$\begin{aligned} \mathcal{W}_\pi(a_1\|a_2, b_1\|b_2) &= \sum_{l\|r \in V_{2k}} (-1)^{\langle b_1\|b_2, \hat{\pi}(l\|r)\rangle \oplus \langle a_1\|a_2, l\|r\rangle} \\ &= -1 + \sum_{r \in V_k} (-1)^{\langle b_2, \mathcal{I}(r \otimes \psi(0))\rangle \oplus \langle a_2, r\rangle} + \sum_{l \in V_k} (-1)^{\langle b_1, \mathcal{I}(l) \otimes \psi(0)\rangle \oplus \langle a_1, l\rangle} \\ &\quad + \sum_{l \in V_k^*} \sum_{r \in V_k^*} (-1)^{\langle b_1, \mathcal{I}(l) \otimes \psi(l \otimes r)\rangle \oplus \langle b_2, \mathcal{I}(r \otimes \psi(l \otimes r))\rangle \oplus \langle a_1, l\rangle \oplus \langle a_2, r\rangle}. \end{aligned}$$

Let us now estimate the Walsh transform $|\mathcal{W}_\pi(a_1\|a_2, b_1\|b_2)|$. Directly from Lemma 1 we can derive the following inequalities:

- $\left|\sum_{r \in V_k} (-1)^{\langle b_2, \mathcal{I}(r \otimes \psi(0))\rangle \oplus \langle a_2, r\rangle}\right| \leqslant \lfloor 2^{\frac{k}{2}+1} \rfloor,$
- $\left|\sum_{l \in V_k} (-1)^{\langle b_1, \mathcal{I}(l) \otimes \psi(0)\rangle \oplus \langle a_1, l\rangle}\right| \leqslant \lfloor 2^{\frac{k}{2}+1} \rfloor.$

In addition, it is obvious that

$$\left|\sum_{l \in V_k^*} \sum_{r \in V_k^*} (-1)^{\langle b_1, \mathcal{I}(l) \otimes \psi(l \otimes r)\rangle \oplus \langle b_2, \mathcal{I}(r \otimes \psi(l \otimes r))\rangle \oplus \langle a_1, l\rangle \oplus \langle a_2, r\rangle}\right| \leqslant (2^k - 1) \cdot (2^k - 1).$$

Hence,

$$|\mathcal{W}_\pi(a_1\|a_2, b_1\|b_2)| \leqslant 2^{2k} - 2^{k+1} + 2 \cdot \lfloor 2^{\frac{k}{2}+1} \rfloor + 2. \tag{13}$$

Thus, from (13) we obtain

$$\mathcal{NL}(\hat{\pi}) = 2^{2k-1} - \frac{1}{2} \cdot \max_{\substack{(b_1,b_2)\in V_{2k}^* \\ (a_1,a_2)\in V_{2k}}} |\mathcal{W}_{\hat{\pi}}(a_1\|a_2, b_1\|b_2)| \geqslant 2^k - \lfloor 2^{\frac{k}{2}+1} \rfloor - 1.$$

□

3.1. The Hamming distance between two instances of $\hat{\pi}$

In this section we are interested in the Hamming distance between two permutations $\pi_\psi, \pi_{\psi'} \in S(V_{2k})$ having non-bijective functions ψ, ψ' such that $\chi(\psi, \psi') = 1$. In other words, the lookup-tables of ψ and ψ' differ only in one position.

Proposition 2. *Let $\psi, \psi' \colon V_k \to V_k^*$ be two arbitrary mappings with $\chi(\psi, \psi') = 1$. Then for permutations $\pi_\psi, \pi_{\psi'}$ the following relation holds*:

$$\chi(\pi_\psi, \pi_{\psi'}) = \begin{cases} 2 \cdot (2^k - 1), & \text{if} \quad \psi(0) \neq \psi'(0), \\ 2^k - 1, & \text{if} \quad \exists\, i \neq 0 \colon \psi(i) \neq \psi'(i). \end{cases} \tag{14}$$

Proof. Consider the following possible cases:

1) If $\psi(0) \neq \psi'(0)$, then $\pi_\psi(l\|r) = \pi_{\psi'}(l\|r)$ for any $l\|r \in V_k^* \times V_k^*$. If $l = 0$, then the inequality $\pi_\psi(0\|r) \neq \pi_{\psi'}(0\|r)$ holds for all $r \in V_k^*$. Analogously, for $r = 0$ and any $l \in V_k^*$ the output $\pi_\psi(l\|0) \neq \pi_{\psi'}(l\|0)$. So we have exactly $2 \cdot (2^k - 1)$ values at which the outputs π_ψ and $\pi_{\psi'}$ are different.

2) If there exist an element $i \neq 0$ such that $\psi(i) \neq \psi'(i)$, then for each fixed $l \in \mathbb{F}_{2^k} \setminus \{0\}$ there exist a unique $r \in \mathbb{F}_{2^k} \setminus \{0\}$ such that $l \otimes r = i$, therefore, there are exactly $2^k - 1$ values of the form $(l\|r) \in V_{2k}$ such that $\pi_\psi(l\|r) \neq \pi_{\psi'}(l\|r)$.

Notice that we have exclude the case $l = r = 0$ because in this situation we always have $\pi_\psi(0) = \pi_{\psi'}(0)$. So, we can conclude that $\chi(\pi_\psi, \pi_{\psi'}) \in \{2^k - 1, 2 \cdot (2^k - 1)\}$. □

3.2. Bounds on nonlinearity and δ-uniformity of two instances of $\hat{\pi}$

In this section, we study the nonlinearity and δ-uniformity parameters of two permutations $\pi_\psi, \pi_{\psi'} \in S(V_{2k})$ for which $\chi(\psi, \psi') = 1$. Recall that we have restricted ourselves to the case when $h = \mathcal{I}$.

Proposition 3. *Let $\psi, \psi' \colon V_k \to V_k^*$ be two arbitrary mappings with $\chi(\psi, \psi') = 1$. Then for permutations $\pi_\psi, \pi_{\psi'}$ the following inequalities holds:*

1) $|\mathcal{NL}(\pi_\psi) - \mathcal{NL}(\pi_{\psi'})| \leqslant 2 \cdot \lfloor 2^{\frac{k}{2}+1} \rfloor$, *if* $\psi(0) \neq \psi'(0)$,

2) $|\mathcal{NL}(\pi_\psi) - \mathcal{NL}(\pi_{\psi'})| \leqslant (2^k - 1)$, *if* $\psi(i) \neq \psi'(i)$ *for some* $i \neq 0$.

Proof. Directly by definition of nonlinearity we have

$$|\mathcal{NL}(\pi_\psi) - \mathcal{NL}(\pi_{\psi'})| \\ = \frac{1}{2} \left| \max_{\substack{(a_1,a_2) \in V_{2k} \\ (b_1,b_2) \in V_{2k}^*}} \left| \mathcal{W}_{\pi_\psi}(a_1 \| a_2, b_1 \| b_2) \right| - \max_{\substack{(a_1,a_2) \in V_{2k} \\ (b_1,b_2) \in V_{2k}^*}} \left| \mathcal{W}_{\pi_{\psi'}}(a_1 \| a_2, b_1 \| b_2) \right| \right|. \tag{15}$$

Let us prove the first item of the proposition. From relations $\psi(0) \neq \psi'(0)$ and $\psi(j) = \psi'(j)$ for $j \in \{1, \ldots, 2^k - 1\}$ we obtain

$$\begin{aligned} \mathcal{W}_{\pi_\psi}(a_1 \| a_2, b_1 \| b_2) &= \sum_{l \| r \in V_{2k}} (-1)^{\left\langle b_1 \| b_2, \pi_\psi(l \| r) \right\rangle \oplus \langle a_1 \| a_2, l \| r \rangle} \\ &= -1 + \sum_{r \in V_k} (-1)^{\langle b_2, \mathcal{I}(r \otimes \psi(0)) \rangle \oplus \langle a_2, r \rangle} + \sum_{l \in V_k} (-1)^{\langle b_1, \mathcal{I}(l) \otimes \psi(0) \rangle \oplus \langle a_1, l \rangle} \\ &\quad + \sum_{l \in V_k^*} \sum_{r \in V_k^*} (-1)^{\langle b_1, \mathcal{I}(l) \otimes \psi'(l \otimes r) \rangle \oplus \langle b_2, \mathcal{I}(r \otimes \psi'(l \otimes r)) \rangle \oplus \langle a_1, l \rangle \oplus \langle a_2, r \rangle}. \end{aligned}$$

Let $\mathcal{T}(a_1 \| a_2, b_1 \| b_2) = \sum_{l \in V_k^*} \sum_{r \in V_k^*} (-1)^{\langle b_1, \mathcal{I}(l) \otimes \psi'(l \otimes r) \rangle \oplus \langle b_2, \mathcal{I}(r \otimes \psi'(l \otimes r)) \rangle \oplus \langle a_1, l \rangle \oplus \langle a_2, r \rangle}$.
It is not difficult to see that

$$\begin{aligned} \mathcal{T}(a_1 \| a_2, b_1 \| b_2) = \mathcal{W}_{\pi_{\psi'}}(a_1 \| a_2, b_1 \| b_2) &- \sum_{r \in V_k} (-1)^{\langle b_2, \mathcal{I}(r \otimes \psi'(0)) \rangle \oplus \langle a_2, r \rangle} \\ &- \sum_{l \in V_k} (-1)^{\langle b_1, \mathcal{I}(l) \otimes \psi'(0) \rangle \oplus \langle a_1, l \rangle} + 1. \end{aligned}$$

Hence, we can express $\mathcal{W}_{\pi_\psi}(a_1\|a_2, b_1\|b_2)$ by $\mathcal{W}_{\pi_{\psi'}}(a_1\|a_2, b_1\|b_2)$ as follows

$$\begin{aligned}
&\mathcal{W}_{\pi_\psi}(a_1\|a_2, b_1\|b_2)\\
&\quad = \Big(\sum_{r\in V_k}(-1)^{\langle b_2,\mathcal{I}(r\otimes\psi(0))\rangle\oplus\langle a_2,r\rangle} + \sum_{l\in V_k}(-1)^{\langle b_1,\mathcal{I}(l)\otimes\psi(0)\rangle\oplus\langle a_1,l\rangle}\Big)\\
&\quad - \Big(\sum_{r\in V_k}(-1)^{\langle b_2,\mathcal{I}(r\otimes\psi'(0))\rangle\oplus\langle a_2,r\rangle} + \sum_{l\in V_k}(-1)^{\langle b_1,\mathcal{I}(l)\otimes\psi'(0)\rangle\oplus\langle a_1,l\rangle}\Big)\\
&\qquad\qquad + \mathcal{W}_{\pi_{\psi'}}(a_1\|a_2, b_1\|b_2).
\end{aligned}$$

Then by using Lemma 1 we find that
$\left|\mathcal{W}_{\pi_\psi}(a_1\|a_2, b_1\|b_2)\right| \leqslant 4\cdot\lfloor 2^{\frac{k}{2}+1}\rfloor + \left|\mathcal{W}_{\pi_{\psi'}}(a_1\|a_2, b_1\|b_2)\right|$ and consequently

$$\max_{\substack{(a_1,a_2)\in V_{2k}\\(b_1,b_2)\in V_{2k}^*}}\left|\mathcal{W}_{\pi_\psi}(a_1\|a_2, b_1\|b_2)\right| \leqslant 4\cdot\lfloor 2^{\frac{k}{2}+1}\rfloor + \max_{\substack{(a_1,a_2)\in V_{2k}\\(b_1,b_2)\in V_{2k}^*}}\left|\mathcal{W}_{\pi_{\psi'}}(a_1\|a_2, b_1\|b_2)\right|.$$

Thus, from the previous relation and (15) we conclude that $|\mathcal{NL}(\pi_\psi) - \mathcal{NL}(\pi_{\psi'})| \leqslant 2\cdot\lfloor 2^{\frac{k}{2}+1}\rfloor$.

Now, we prove the second item of the proposition. For each element $l\in V_k^*$ there exist a unique element $r\in V_k^*$ such that $l\otimes r = i$. Then, the Walsh transforms of permutation π_ψ may be expressed as follows

$$\begin{aligned}
\mathcal{W}_{\pi_\psi}(a_1\|a_2, b_1\|b_2) &= \sum_{l\|r\in V_{2k}}(-1)^{\left\langle b_1\|b_2,\pi_\psi(l\|r)\right\rangle\oplus\langle a_1\|a_2,l\|r\rangle}\\
&= 1 + \sum_{r\in V_k^*}(-1)^{\langle b_2,\mathcal{I}(r\otimes\psi(0))\rangle\oplus\langle a_2,r\rangle} + \sum_{l\in V_k^*}(-1)^{\langle b_1,\mathcal{I}(l)\otimes\psi(0)\rangle\oplus\langle a_1,l\rangle}\\
&\qquad + \sum_{l\in V_k^*}\sum_{r\in V_k^*}(-1)^{\langle b_1,\mathcal{I}(l)\otimes\psi(l\otimes r)\rangle\oplus\langle b_2,\mathcal{I}(r\otimes\psi(l\otimes r))\rangle\oplus\langle a_1,l\rangle\oplus\langle a_2,r\rangle}.
\end{aligned}$$

Let $\mathcal{S}(a_1\|a_2, b_1\|b_2) = \sum_{l\in V_k^*}\sum_{r\in V_k^*}(-1)^{\langle b_1,\mathcal{I}(l)\otimes\psi(l\otimes r)\rangle\oplus\langle b_2,\mathcal{I}(r\otimes\psi(l\otimes r))\rangle\oplus\langle a_1,l\rangle\oplus\langle a_2,r\rangle}$.
Then

$$\mathcal{S}(a_1\|a_2, b_1\|b_2) = \sum_{l\in V_k^*}\mathcal{T}(a_1\|a_2, b_1\|b_2), \tag{16}$$

where $\mathcal{T}(a_1\|a_2, b_1\|b_2) = \sum_{r\in V_k^*}(-1)^{\langle b_1,\mathcal{I}(l)\otimes\psi(l\otimes r)\rangle\oplus\langle b_2,\mathcal{I}(r\otimes\psi(l\otimes r))\rangle\oplus\langle a_1,l\rangle\oplus\langle a_2,r\rangle}$.

For each fixed $l \in V_k^*$, the term $\mathcal{T}(a_1\|a_2, b_1\|b_2)$ may be rewritten as

$$\mathcal{T}(a_1\|a_2, b_1\|b_2) = \sum_{r \in V_k^* \setminus \{i \otimes l^{-1}\}} (-1)^{\langle b_1, \mathcal{I}(l) \otimes \psi(l \otimes r)\rangle \oplus \langle b_2, \mathcal{I}(r \otimes \psi(l \otimes r))\rangle \oplus \langle a_1, l\rangle \oplus \langle a_2, r\rangle} + (-1)^{\langle b_1, \mathcal{I}(l) \otimes \psi(i)\rangle \oplus \left\langle b_2, \mathcal{I}((i \otimes l^{-1}) \otimes \psi(i))\right\rangle \oplus \langle a_1, l\rangle \oplus \left\langle a_2, i \otimes l^{-1}\right\rangle}.$$

Substituting $\mathcal{T}(a_1\|a_2, b_1\|b_2)$ in (16) we obtain

$$\mathcal{S}(l, r) = \sum_{l \in V_k^*} \sum_{r \in V_k^* \setminus \{i \otimes l^{-1}\}} (-1)^{\langle b_1, \mathcal{I}(l) \otimes \psi(l \otimes r)\rangle \oplus \langle b_2, \mathcal{I}(r \otimes \psi(l \otimes r))\rangle \oplus \langle a_1, l\rangle \oplus \langle a_2, r\rangle} + \sum_{l \in V_k^*} (-1)^{\langle b_1, \mathcal{I}(l) \otimes \psi(i)\rangle \oplus \left\langle b_2, \mathcal{I}((i \otimes l^{-1}) \otimes \psi(i))\right\rangle \oplus \langle a_1, l\rangle \oplus \left\langle a_2, (i \otimes l^{-1})\right\rangle}.$$

Thus,

$$\begin{aligned}
\mathcal{W}_{\pi_\psi}(a_1\|a_2, b_1\|b_2) &= \sum_{l\|r \in V_{2k}} (-1)^{\left\langle b_1\|b_2, \pi_\psi(l\|r)\right\rangle \oplus \langle a_1\|a_2, l\|r\rangle} \\
&= 1 + \sum_{r \in V_k^*} (-1)^{\langle b_2, \mathcal{I}(r \otimes \psi(0))\rangle \oplus \langle a_2, r\rangle} + \sum_{l \in V_k^*} (-1)^{\langle b_1, \mathcal{I}(l) \otimes \psi(0)\rangle \oplus \langle a_1, l\rangle} \\
&+ \sum_{l \in V_k^*} \sum_{r \in V_k^* \setminus \{i \otimes l^{-1}\}} (-1)^{\langle b_1, \mathcal{I}(l) \otimes \psi(l \otimes r)\rangle \oplus \langle b_2, \mathcal{I}(r \otimes \psi(l \otimes r))\rangle \oplus \langle a_1, l\rangle \oplus \langle a_2, r\rangle} \\
&+ \sum_{l \in V_k^*} (-1)^{\langle b_1, \mathcal{I}(l) \otimes \psi(i)\rangle \oplus \left\langle b_2, \mathcal{I}((i \otimes l^{-1}) \otimes \psi(i))\right\rangle \oplus \langle a_1, l\rangle \oplus \left\langle a_2, (i \otimes l^{-1})\right\rangle}.
\end{aligned}$$

Now, taking into account that $\psi(i) \neq \psi'(i)$ for some $i \in V_k^*$, and $\psi(j) = \psi'(j)$ for any $j \in V_k \setminus \{i\}$, we can link $\mathcal{W}_{\pi_\psi}(a_1\|a_2, b_1\|b_2)$ and $\mathcal{W}_{\pi_{\psi'}}(a_1\|a_2, b_1\|b_2)$ as follows

$$\begin{aligned}
\mathcal{W}_{\pi_\psi}(a_1\|a_2, b_1\|b_2) &= \mathcal{W}_{\pi_{\psi'}}(a_1\|a_2, b_1\|b_2) \\
&\sum_{l \in V_k^*} (-1)^{\langle b_1, \mathcal{I}(l) \otimes \psi(i)\rangle \oplus \left\langle b_2, \mathcal{I}((i \otimes l^{-1}) \otimes \psi(i))\right\rangle \oplus \langle a_1, l\rangle \oplus \left\langle a_2, (i \otimes l^{-1})\right\rangle} \\
&- \sum_{l \in V_k^*} (-1)^{\langle b_1, \mathcal{I}(l) \otimes \psi'(i)\rangle \oplus \left\langle b_2, \mathcal{I}((i \otimes l^{-1}) \otimes \psi'(i))\right\rangle \oplus \langle a_1, l\rangle \oplus \left\langle a_2, (i \otimes l^{-1})\right\rangle}.
\end{aligned}$$

Hence, $\left|\mathcal{W}_{\pi_\psi}(a_1\|a_2, b_1\|b_2)\right| \leqslant \left|\mathcal{W}_{\pi_{\psi'}}(a_1\|a_2, b_1\|b_2)\right| + 2 \cdot (2^k - 1)$ and as a consequence

$$\max_{\substack{(a_1, a_2) \in V_{2k} \\ (b_1, b_2) \in V_{2k}^*}} \left|\mathcal{W}_{\pi_\psi}(a_1\|a_2, b_1\|b_2)\right| \leqslant \max_{\substack{(a_1, a_2) \in V_{2k} \\ (b_1, b_2) \in V_{2k}^*}} \left|\mathcal{W}_{\pi_{\psi'}}(a_1\|a_2, b_1\|b_2)\right| + 2 \cdot (2^k - 1).$$

Thus, from the previous inequality and (15) we conclude that $|\mathcal{NL}(\pi_\psi) - \mathcal{NL}(\pi_{\psi'})| \leqslant (2^k - 1)$. $\square$

Proposition 3 may be used to increase the nonlinearity of permutation π_ψ, which is very useful for searching nonlinear bijective transformations having good values of its basic cryptographic parameters.

The following proposition shows the behavior of the δ-uniformity parameter of permutations $\pi_\psi, \pi_{\psi'}$ with $\chi(\psi, \psi') = 1$.

Proposition 4. *Let $\psi, \psi' \colon V_k \to V_k^*$ be two arbitrary mappings with $\chi(\psi, \psi') = 1$. Then for permutations $\pi_\psi, \pi_{\psi'}$ the following inequalities holds*:

1) $\left|\delta_{\pi_\psi} - \delta_{\pi_{\psi'}}\right| \leqslant 4(2^k - 1)$ *if* $\psi(0) \neq \psi'(0)$,

2) $\left|\delta_{\pi_\psi} - \delta_{\pi_{\psi'}}\right| \leqslant 2(2^k - 1)$ *if* $\psi(i) \neq \psi'(i)$ *for some* $i \neq 0$.

Proof. To prove the proposition it is sufficient to bound the sums

$$\Delta_{\pi_\psi}(a, b) = \sum_{x \in V_n} \mathsf{Ind}(\pi_\psi(x \oplus a) \oplus \pi_\psi(x), b),$$

$$\Delta_{\pi_{\psi'}}(a, b) = \sum_{x \in V_n} \mathsf{Ind}(\pi_{\psi'}(x \oplus a) \oplus \pi_{\psi'}(x), b).$$

1) Consider the case $\psi(0) \neq \psi'(0)$. According to Proposition 2 denote by ω_t, $t = 1, \ldots, 2 \cdot (2^k - 1)$, all points of V_{2k} such that $\pi_\psi(\omega_t) \neq \pi_{\psi'}(\omega_t)$. If $\mathsf{Ind}(\pi_\psi(x \oplus a) \oplus \pi_\psi(x), b) \neq \mathsf{Ind}(\pi_{\psi'}(x \oplus a) \oplus \pi_{\psi'}(x), b)$, then $x = \omega_t$ or $x = \omega_t \oplus a$ for some $t = 1, \ldots, 2(2^k - 1)$. Therefore

$$\left|\Delta_{\pi_\psi}(a, b) - \Delta_{\pi_{\psi'}}(a, b)\right| \leqslant 2(2^k - 1),$$

and

$$\left|\delta_{\pi_\psi} - \delta_{\pi_{\psi'}}\right| \leqslant 2(2^k - 1).$$

2) In the case $\psi(0) = \psi'(0)$ the proof is quite similar to the proof of the first item. $\square$

Proposition 4 tell us that under changing only one output value of ψ the δ-uniformity of π_ψ may decrease, which is quite useful when searching nonlinear bijective transformations with good values of its basic cryptographic parameters based on the construction of π_ψ.

3.3. Algorithms for finding almost optimal S-boxes

By using Propositions 3 and 4 we have conducted two search algorithms (implemented in SAGE [45]) for finding ordinary 8-bit S-boxes π_ψ having the following cryptographic parameters:

- $d_{min}(\pi_\psi) = 7$,
- $\delta_{\pi_\psi} \in \{6, 8\}$,
- $r_{\pi_\psi} = 3$ with $r^{(3)}_{\pi_\psi} = 441$,
- $100 \leqslant \mathcal{NL}(\pi_\psi) \leqslant 104$.

The algorithms are slightly modified versions of algorithms for implementing the spectral-linear and spectral-differential methods presented in [34] and both of them operates with the following objects:

$$(a, b, c, d, e) \in S(V_{2k}) \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \Xi_0(V_k),$$

where $\Xi_0(V_k)$ denotes the set of all functions $\psi\colon V_k \to V_k^*$. On the set of these objects we define the order relation as follows

$$(\tilde{a}, \tilde{b}, \tilde{c}, \tilde{d}, \tilde{e}) \leqslant (a, b, c, d, e), \text{ if } \begin{cases} \tilde{b} < b, \tilde{d} \leqslant d \text{ or} \\ \tilde{b} = b, \tilde{c} \leqslant c, \tilde{d} \leqslant d. \end{cases} \quad (17)$$

To help fully understanding how our algorithms work, we introduce the following concepts.

Definition 11 ([34]). The Difference Distribution Table (DDT) of an S-box $\Phi \in S(V_n)$ is a $2^n \times 2^n$ matrix, denoted by DDT_Φ and defined as

$$\mathsf{DDT}_\Phi[a, b] = \frac{1}{2^n}\Delta_\Phi(a, b) = \frac{1}{2^n}\#\{x \in V_n | \Phi(x \oplus a) \oplus \Phi(x)) = b\}.$$

Definition 12 ([34]). The Linear Approximation Table (LAT) of an S-box $\Phi \in S(V_n)$ is a $2^n \times 2^n$ matrix, denoted by LAT_Φ and defined as

$$\mathsf{LAT}_\Phi[a, b] = \frac{2}{2^n}\#\{x \in V_n | \langle a, x\rangle = \langle b, \Phi(x)\rangle\} - 1.$$

For $\Phi \in S(V_n)$ and numbers $p_1 \in P_{n-1}$ and $p_2 \in P_{n-2}$, where

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

we define the following sets:

$$D(\Phi, p_1) = \{(a, b) \in V_n^* \times V_n^* | \mathsf{DDT}_\Phi[a, b] = p_1\}$$

and

$$L(\Phi, p_1) = \{(a, b) \in V_n^* \times V_n^* \big| |\mathsf{LAT}_\Phi[a, b]| = p_2\}.$$

Definition 13 ([34])**.** The differential spectrum of S-box $\Phi \in S(V_n)$ is defined as

$$D(\Phi) = \{(p_1, \#D(\Phi, p_1))|p_1 \in P_{n-1}\},\ \#D(\Phi) = 2^{n-1} - 1. \tag{18}$$

Definition 14 ([34])**.** The linear spectrum of an S-box $\Phi \in S(V_n)$ is defined as

$$L(\Phi) = \{(p_2, \#L(\Phi, p_1))|p_2 \in P_{n-2}\},\ \#L(\Phi) = 2^{n-2} - 1. \tag{19}$$

For a natural number $n = 2k$, let $\ell \leqslant 2^k \cdot (2^k - 2) \in \mathbb{N}$ be the size of some list L. The algorithm for improving the differential properties is presented below.

Making appropriate changes in Algorithm 1 we can obtain the algorithm for optimizing the (non)linear properties of π, which is omitted due to space limitations. It should be pointed that in these algorithms we always assume that the multiplication table of $\mathbb{F}_{2^k}$ is given.

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

Proposition 5. *For $n \to \infty$ we have*

$$t_1 = O(n^2 \cdot 2^{5n}).$$

Proof. The proof is divided in two stages. In the first stage we compute the maximum number of of step 4 iterations of the algorithm and in the second stage we find the complexity of step 4.

1) Let $\pi_\psi \in S(V_{2k})$. For element of a differential spectrum $D(\pi_\psi)$ we have $\#D(\pi_\psi, p_1) \leqslant (2^n - 1) \cdot \frac{1}{p_1}$. Thus, we obtain the following expressions:

$$\sum_{p_1 \in P_{n-1} \setminus \{0\}} (2^n - 1) \cdot \frac{1}{p_1} = (2^n - 1) \sum_{p_1 \in P_{n-1} \setminus \{0\}} \frac{1}{p_1} = (2^n - 1) \sum_{i=1}^{2^{n-1}} \frac{2^{n-1}}{i}$$
$$= (2^n - 1) \cdot 2^{n-1} \sum_{1=1}^{2^{n-1}} \frac{1}{i} \leqslant 2^{n-1} \cdot (2^n - 1) \cdot (\ln 2^{n-1} + 1)$$
$$\leqslant 2^{n-1} \cdot (2^n - 1) \cdot (\log_2 2^{n-1} + 1) = n \cdot 2^{n-1} \cdot (2^n - 1).$$

2) The estimate of complexity of Step 4 is the product of the following values:

Algorithm 1: Optimizing the differential properties of π_ψ

Input: Permutation $\mathcal{I}(x) = x^{2^k-2}$ over $\mathbb{F}_{2^k}$, function $\psi : V_k \to V_k^*$ and parameter $\ell \in \mathbb{N}$.

1 Construct $\pi_\psi = (\mathcal{I}(l) \otimes \psi(l \otimes r))\big\|\mathcal{I}(r \otimes \psi(l \otimes r)) \in S(V_{2k})$.

2 For permutation $\pi_\psi \in S(V_{2k})$ calculate the values $\delta_{\pi_\psi}, D(\pi_\psi), \mathcal{NL}(\pi_\psi)$ and set $\psi^{(-1)} = \psi$.

3 Initialize the list L:

$\mathsf{L} = \Big\{\Big(\pi_{\psi^{(-1)}}, \delta_{\pi_{\psi^{(-1)}}}, \#D\Big(\pi_{\psi^{(-1)}}, \delta_{\pi_{\psi^{(-1)}}}\Big), \mathcal{NL}\Big(\pi_{\psi^{(-1)}}\Big), \psi^{(-1)}\Big)\Big\}$, where $\#\mathsf{L} = 1$.

4 Using the list

$\mathsf{L} = \Big\{\Big(\pi_{\psi^{(i)}}, \delta_{\pi_{\psi^{(i)}}}, \#D\Big(\pi_{\psi^{(i)}}, \delta_{\pi_{\psi^{(i)}}}\Big), \mathcal{NL}\big(\pi_{\psi^{(i)}}\big), \psi^{(i)}\Big)\Big|\, i = -1, 0, \ldots, \#\mathsf{L} - 2\Big\}$

construct the new list

$$\widetilde{\mathsf{L}} = \Big\{\Big(\pi_{\psi'^{(i)}_{j,t}}, \delta_{\pi_{\psi'^{(i)}_{j,t}}}, \#D\Big(\pi_{\psi'^{(i)}_{j,t}}, \delta_{\pi_{\psi'^{(i)}_{j,t}}}\Big), \mathcal{NL}\Big(\pi_{\psi'^{(i)}_{j,t}}\Big), \psi'^{(i)}_{j,t}\Big)\Big\},$$

where for each $i = -1, 0, \ldots, \#\mathsf{L} - 2$, $j = 0, \ldots, 2^k - 1$, $t = 0, \ldots 2^k - 3$, functions $\pi_{\psi'^{(i)}_{j,t}} \in S(V_{2k})$ for which $\chi\Big(\pi_{\psi^{(i)}}, \pi_{\psi'^{(i)}_{j,t}}\Big) \in \{2^k - 1, 2 \cdot (2^k - 1)\}$, $\delta_{\pi_{\psi'^{(i)}_{j,t}}} \leqslant \delta_{\pi_{\psi^{(i)}}}, \mathcal{NL}(\pi_{\psi^{(i)}}) \leqslant \mathcal{NL}(\pi_{\psi'^{(i)}_{j,t}})$, functions $\psi^{(i)}, \psi'^{(i)}_{j,t} : V_k \to V_k^*$ have $\chi\Big(\psi^{(i)}, \psi'^{(i)}_{j,t}\Big) = 1$ and $\#D\Big(\pi_{\psi'^{(i)}_{j,t}}, \delta_{\pi_{\psi'^{(i)}_{j,t}}}\Big) < \#D\Big(\pi_{\psi^{(i)}}, \delta_{\pi_{\psi^{(i)}}}\Big)$ if $\delta_{\pi_{\psi'^{(i)}_{j,t}}} = \delta_{\pi_{\psi'^{(i)}}}$.

5 For the list $\widetilde{\mathsf{L}}$ do the following:

(I) Calculate the size $\#\widetilde{\mathsf{L}}$.

(II) Sort the elements of $\widetilde{\mathsf{L}}$ in the ascending order according to relation (17).

(III) Numerate the sorted list element by indexes $i = 0, \ldots, \#\widetilde{\mathsf{L}} - 1$.

(IV) Calculate values $m_1 = \min\{\#\mathsf{L} - 1, \#\widetilde{\mathsf{L}} - 1\}, m_2 = \min\{\ell - 1, \#\widetilde{\mathsf{L}} - 1\}$.

6 Compare the first elements of lists L and $\widetilde{\mathsf{L}}$:

– If $\displaystyle\sum_{i=0}^{m_1} \delta_{\pi_{\psi'^{(i)}}} < \sum_{i=0}^{m_1} \delta_{\pi_{\psi^{(i)}}}$ or

$\displaystyle\sum_{i=0}^{m_1} \delta_{\pi_{\psi'^{(i)}}} = \sum_{i=0}^{m_1} \delta_{\pi_{\psi^{(i)}}}$ and $\displaystyle\sum_{i=0}^{m_1} \#D\Big(\pi_{\psi'^{(i)}}, \delta_{\pi_{\psi'^{(i)}}}\Big) < \sum_{i=0}^{m_1} \#D\Big(\pi_{\psi^{(i)}}, \delta_{\pi_{\psi^{(i)}}}\Big)$,

then

(I) Clean the list L.

(II) Copy the elements from the list $\widetilde{\mathsf{L}}$ with indexes $i = 0, \ldots, m_2$ to L.

(III) Assign $\#\mathsf{L} = m_2 + 1$.

(IV) Go to step 4.

– Otherwise, the algorithm stops.

Output: The list

$\widetilde{\mathsf{L}} = \Big\{\Big(\pi_{\psi^{(i)}}, \delta_{\pi_{\psi^{(i)}}}, \#D\Big(\pi_{\psi^{(i)}}, \delta_{\pi_{\psi^{(i)}}}\Big), \mathcal{NL}\Big(\pi_{\psi^{(i)}}\Big), \psi^{(i)}\Big)\Big|\, i = -1, 0, \ldots, \#\mathsf{L} - 2\Big\}$,

where $\#\widetilde{\mathsf{L}} \leqslant \ell$.

- the parameter ℓ,
- the estimate of the number of all functions $\psi^{(i)}, \psi'^{(i)}_{j,t}\colon V_k \to V_k^*$ having $\chi\Big(\psi^{(i)}, \psi'^{(i)}_{j,t}\Big) = 1$ contained in $\widetilde{\mathsf{L}}$, which obviously cannot exceed $2^k \cdot (2^k - 2) = 2^n - 2^{\frac{n}{2}+1}$,
- the complexity of computing $\mathcal{NL}\big(\pi_{\psi^{(i)}}\big)$, which is equal to $c\cdot 2^{2n}\cdot n$, where $c = \mathrm{const}$.

The computation of remaining parameters is not so difficult as just described. Thus, the complexity of step 4 is smaller than

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

In this way, the total complexity of the algorithm is upper bounded by

$$t_1 \leqslant \ell \cdot c \cdot n^2 \cdot (2^{5n} - 2^{4n+\frac{n}{2}+1} - 2^{4n} + 2^{3n+\frac{n}{2}+1}) \leqslant \ell \cdot c \cdot n^2 \cdot 2^{5n}.$$

$\square$

As stated before, the Algorithm 1 is a slightly modified version of the algorithm for implementing the spectral-differential method given in [34, p. 102], the only essential difference with the latter is the last coordinate of elements belonging to L and $\widetilde{\mathsf{L}}$ respectively and we have reproduced the proof of Proposition 5 (borrowed from [34]) here only for the sake of completeness.

Analogously, using the results given in [34, p. 106] we can find the computational complexity t_2 of the algorithm similar to Algorithm 1 for optimizing the (non)linear properties of π_ψ, which in this case is equal to $t_2 = O(n \cdot 2^{6n})$.

Comparing the computational complexities of algorithms implementing spectral-differential and the spectral-linear methods, which are equal to $t_{\mathsf{spect/diff}} = O(n^2 \cdot 2^{6n-1})$ and $t_{\mathsf{spect/lin}} = O(n \cdot 2^{7n-4})$ respectively [34], we can see that Algorithm 1 is approximately 2^{n-1} times faster than the algorithm for implementing spectral-differential method, while our algorithm for optimizing the (non)linear properties is 2^{n-4} times faster than the algorithm for implementing spectral-linear method. However, both algorithms developed in [34] are universal, and to the best of our knowledge may optimize any S-box except those based on finite field inversion and affine equivalent to it. Algorithms presented in this section may optimize only S-boxes having the form $\pi_\psi = (\mathcal{I}(l) \otimes \psi(l \otimes r))\big|\big|\mathcal{I}(r \otimes \psi(l \otimes r))$ and affine equivalent to π_ψ.

3.4. Invariant subspaces with respect to the action of π_ψ

Let $\Phi\colon V_n \to V_n$ be any nonlinear bijective transformation. For any $\mathsf{W} \subseteq V_n$ we denote by $\Phi(\mathsf{W})$ the set containing all images of the elements from W, that is

$$\Phi(\mathsf{W}) = \{\Phi(x) \mid x \in \mathsf{W}\}.$$

Definition 15. We say that $\mathsf{W} \subseteq V_n$ is an invariant set with respect to the action of $\Phi : V_n \to V_n$, if $\Phi(\mathsf{W}) \subseteq \mathsf{W}$ or $\Phi(\mathsf{W}) \subseteq V_n \setminus \mathsf{W}$.

In this section, we study the question about the existence of subsets $\mathsf{W} \subseteq V_n$ such that $\pi_\psi(\mathsf{W}) \subseteq \mathsf{W}$. When these subsets are subspaces of V_n and $\pi_\psi(\mathsf{W} \oplus a) = \mathsf{W} \oplus b$ for some fixed elements $a, b \in V_n$, then they are called invariant subspaces.

Invariant subspaces are used in recent cryptanalytic approaches when mounting structural attacks on block ciphers (for example, in the so-called invariant subspaces attacks [32]). The existence of such structures may significantly decrease the cryptographic security of block ciphers. In [2, 44] were described some approaches for designing cryptographic primitives having a structure, knowledge of which allows to find the encryption key with a time complexity, significantly lower than the brute force method. Such structure is called a backdoor, and the whole encryption algorithm — backdoored encryption algorithm.

Another fundamental cryptanalytic method for block ciphers is the homomorphism attack. The effectiveness of this approach is highly dependent on how close the encryption function may be approximated by permutations having the partition-preserving property. The authors of [42] studied the possibility to approximate permutations by permutations from the wreath product of symmetric groups in an imprimitive action, where the so-called W-intersection matrix was proposed as a parameter characterizing the approximability of permutations by permutations from the wreath group. The W-intersection matrix for a permutation Φ of $S(V_n)$ is defined as follows

$$\mathcal{M}_{\mathsf{W}}(\Phi) = \left\| c^{\mathsf{W}}_{\alpha,\beta}(\Phi) \right\|_{\alpha,\beta \in \mathcal{R}_{\mathsf{W}}},$$

where $c^{\mathsf{W}}_{\alpha,\beta}(\Phi) = \#\left\{ x \in \mathsf{W} \oplus \alpha \,\middle|\, \Phi(x) \in \mathsf{W} \oplus \beta \right\}$, $\mathsf{W} < V_n$, $\dim \mathsf{W} = d \in \{1, 2, \ldots, n-1\}$ and $\mathcal{R}_{\mathsf{W}}$ is the set of coset representatives for the subspace $\mathsf{W} < V_n$.

The W-intersection matrix is a very useful tool to automatically verify the invariance of a fixed subspace W with respect to the action of given nonlinear bijective transformation.

Proposition 6. *Let* $\mathsf{W}_1 = \{(l\|0) | l \in V_k\}, \mathsf{W}_2 = \{(0\|r) | r \in V_k\}$ *be two* k*-dimensional subspaces of the vector space* V_{2k}*. Then*

$$c^{\mathsf{W}_1}_{0,0}(\pi_\psi) = c^{\mathsf{W}_2}_{0,0}(\pi_\psi) = 2^k. \tag{20}$$

Proof. The relations written in (20) are a direct consequence of the equality (10) for $h = \mathcal{I}$. □

Example 1. Let $n = 2k = 2 \cdot 4$ and $\mathbb{F}_{2^4} = \mathbb{F}_2[\xi]/\xi^4 \oplus \xi \oplus 1$, the 4-bit components[a] $\psi, \mathcal{I}$ be given as follows

$$\psi = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 7 & 12 & 3 & 12 & 12 & 9 & 13 & 13 & 8 & 2 & 2 & 11 & 9 & 15 & 2 & 3 \end{pmatrix},$$

$$\mathcal{I} = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 0 & 1 & 9 & 14 & 13 & 11 & 7 & 6 & 15 & 2 & 12 & 5 & 10 & 4 & 3 & 8 \end{pmatrix}.$$

The resulting permutation $\pi_\psi(l\|r) = (\mathcal{I}(l) \otimes \psi(l \otimes r))\|\mathcal{I}(r \otimes \psi(l \otimes r)) \in S(V_8)$ and its cryptographic parameters are compiled in the Table 1.

Table 1. The constructed permutation $\pi_\psi \in S(V_8)$

S-box π_ψ															
$\mathcal{NL}(\pi_\psi) = 104, \delta_{\pi_\psi} = 6, d_{min}(\pi_\psi) = 7, r_{\pi_\psi} = 3, r^{(3)}_{\pi_\psi} = 441.$															
0x0	0x6	0x3	0x2	0x8	0xf	0x1	0x7	0x4	0xc	0xe	0xd	0x9	0xb	0xa	0x5
0x70	0xca	0x37	0xc6	0xcb	0x95	0xdf	0xdb	0x8a	0x21	0x26	0xb2	0x97	0xf6	0x28	0x39
0xa0	0x8e	0x65	0xfd	0x47	0x1c	0xde	0x13	0x6c	0x67	0xf5	0xda	0xc4	0x12	0x81	0xec
0xc0	0x4a	0xa2	0x7f	0x79	0x18	0xfa	0xf3	0x86	0x9d	0x5a	0xfb	0xae	0x4e	0x4d	0x19
0x50	0x3a	0x2e	0xff	0x3b	0xea	0x68	0x42	0xe9	0x4f	0x96	0x9b	0xf7	0x3e	0x7b	0x94
0x40	0xc2	0x5d	0xeb	0x61	0xe8	0x3d	0x74	0x5e	0x9a	0xd1	0xd4	0x55	0xc8	0xdd	0x66
0x60	0x54	0xa1	0xe7	0x4c	0xb7	0x5f	0x29	0xad	0x27	0xe6	0x93	0xe5	0xd9	0x91	0x2f
0x10	0x84	0xcd	0xc7	0xaa	0x53	0xe3	0x8b	0x41	0xc1	0xe1	0xe4	0xa6	0x38	0x36	0xfe
0xb0	0x1f	0x85	0x33	0x71	0xdc	0xee	0xa5	0xed	0x87	0x24	0x77	0xd5	0x2d	0xd8	0x8f
0xe0	0x49	0xb5	0x35	0x6a	0x51	0xb3	0x43	0xbc	0xd3	0x1b	0x1a	0x9e	0x6d	0x9c	0x44
0x20	0xb9	0x32	0x89	0xbf	0xf2	0xba	0xf9	0x75	0x64	0xa8	0x73	0xf8	0xd7	0x3c	0x63
0x80	0x15	0xb1	0xa7	0xaf	0x92	0xfc	0x99	0xc9	0xb4	0xf4	0xab	0x6f	0xc3	0xe2	0x9f
0x30	0x52	0x2b	0xbd	0x59	0x7c	0x7a	0xd2	0x7e	0xb8	0x11	0xce	0xd6	0x1e	0x1d	0xf1
0xf0	0x98	0x8d	0x56	0x5b	0x25	0x6b	0x2c	0xc5	0xcf	0xa9	0x17	0x58	0x82	0x88	0x16
0x90	0x69	0x57	0x76	0x22	0x72	0x5c	0x8c	0x6e	0x48	0x45	0xb6	0x78	0x62	0xef	0x83
0xd0	0xbe	0x14	0xbb	0x3f	0x2a	0xa3	0x7d	0xac	0x31	0x4b	0xa4	0xcc	0x23	0x46	0x34

From Table 1 we can see that the nonlinear bijective transformation $\pi_\psi \in S(V_8)$ exhibit high values of its basic cryptographic parameters and it does not have polynomial relations of low degree.

[a]The component ψ has been found using the algoritmhs described in Section 3.2.

Let us now verify the existence of some invariant subspaces with respect to the action of the constructed permutation $\pi_\psi \in S(V_8)$. The W-intersection matrices $\mathcal{M}_{\mathsf{W}_i}(\pi_\psi) = \left\| c_{\alpha,\beta}^{\mathsf{W}_i}(\pi_\psi) \right\|_{\alpha,\beta\in\mathcal{R}_{\mathsf{W}_i}}$ given by

$$\mathcal{M}_{\mathsf{W}_1}(\pi_\psi)=\begin{pmatrix} \boxed{16} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 2 & 1 & 1 & 0 & 1 & 3 & 3 & 0 & 0 & 0 & 2 & 1 \\ 0 & 2 & 2 & 1 & 1 & 3 & 0 & 2 & 0 & 0 & 0 & 1 & 0 & 3 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 3 & 3 & 0 & 1 & 0 & 2 & 0 & 2 & 0 & 2 \\ 0 & 2 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 2 & 2 & 3 & 1 & 0 & 0 & 3 \\ 0 & 1 & 3 & 1 & 0 & 2 & 0 & 1 & 2 & 0 & 2 & 0 & 3 & 0 & 0 & 1 \\ 0 & 1 & 0 & 3 & 0 & 0 & 0 & 0 & 1 & 0 & 3 & 1 & 2 & 1 & 2 & 2 \\ 0 & 0 & 2 & 3 & 1 & 1 & 0 & 1 & 0 & 3 & 0 & 2 & 2 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 2 & 1 & 0 & 0 & 2 & 1 & 0 & 3 & 2 & 3 & 0 \\ 0 & 3 & 0 & 1 & 2 & 0 & 0 & 3 & 2 & 0 & 1 & 0 & 1 & 1 & 0 & 2 \\ 0 & 3 & 0 & 0 & 2 & 2 & 3 & 0 & 1 & 1 & 1 & 2 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 2 & 3 & 0 & 1 & 2 & 0 & 0 & 2 & 3 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 3 & 2 & 2 & 3 & 1 & 0 & 0 & 1 & 0 & 2 & 1 \\ 0 & 0 & 3 & 2 & 0 & 0 & 1 & 1 & 2 & 1 & 0 & 1 & 0 & 2 & 3 & 0 \\ 0 & 2 & 1 & 0 & 0 & 0 & 2 & 0 & 3 & 0 & 1 & 1 & 2 & 3 & 0 & 1 \\ 0 & 1 & 0 & 2 & 3 & 1 & 2 & 0 & 0 & 2 & 0 & 0 & 1 & 0 & 1 & 3 \end{pmatrix}, \mathcal{M}_{\mathsf{W}_2}(\pi_\psi)=\begin{pmatrix} \boxed{16} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 3 & 2 & 0 & 0 & 0 & 1 & 1 & 2 & 0 & 1 & 3 & 2 & 0 & 1 \\ 0 & 3 & 0 & 0 & 1 & 0 & 3 & 0 & 2 & 0 & 1 & 0 & 1 & 2 & 1 & 2 \\ 0 & 2 & 0 & 0 & 3 & 1 & 0 & 2 & 1 & 1 & 2 & 0 & 1 & 0 & 0 & 3 \\ 0 & 0 & 1 & 3 & 2 & 1 & 1 & 1 & 0 & 3 & 0 & 0 & 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 1 & 1 & 3 & 2 & 1 & 0 & 1 & 0 & 0 & 2 & 3 & 2 & 0 \\ 0 & 0 & 3 & 0 & 1 & 2 & 1 & 0 & 0 & 2 & 2 & 1 & 0 & 1 & 3 & 0 \\ 0 & 1 & 0 & 2 & 1 & 1 & 0 & 0 & 2 & 0 & 2 & 0 & 3 & 0 & 3 & 1 \\ 0 & 1 & 2 & 1 & 0 & 0 & 0 & 2 & 3 & 0 & 1 & 1 & 0 & 3 & 2 & 0 \\ 0 & 2 & 0 & 1 & 3 & 1 & 2 & 0 & 0 & 2 & 0 & 3 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 2 & 0 & 0 & 2 & 2 & 1 & 0 & 1 & 3 & 0 & 1 & 0 & 3 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 3 & 3 & 2 & 2 & 0 & 1 & 2 \\ 0 & 3 & 1 & 1 & 0 & 2 & 0 & 3 & 0 & 0 & 0 & 2 & 1 & 2 & 0 & 1 \\ 0 & 2 & 2 & 0 & 0 & 3 & 1 & 0 & 3 & 1 & 1 & 0 & 2 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 2 & 2 & 3 & 3 & 2 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 2 & 3 & 2 & 0 & 0 & 1 & 0 & 0 & 3 & 2 & 1 & 1 & 0 & 0 \end{pmatrix}, \quad (21)$$

for subspaces $\mathsf{W}_1 = \{(l\|0) | l \in V_4\}$, $\mathsf{W}_2 = \{(0\|r) | r \in V_4\}$ of the vector space V_8 were found by computer calculations using SAGE [45].

From (21) we can see that $c_{0,0}^{\mathsf{W}_1}(\pi_\psi) = c_{0,0}^{\mathsf{W}_2}(\pi_\psi) = 16$, which means that $\pi_\psi(\mathsf{W}_i) = \mathsf{W}_i$. Hence the subspaces W_1 and W_2 are invariant under the action of the constructed permutation $\pi_\psi \in S(V_8)$.

So, despite the fact that permutation $\pi_\psi \in S(V_8)$ exhibit a low value of δ-uniformity, high nonlinearity and may be described by a system of 441 polynomials equations of degree 3, it has a weakness: the existence of some structures (subspaces W_1 and W_2) which are invariant with respect to the action of this nonlinear bijective transformation. If this permutation is used as a nonlinear layer in XSL-network, then these structures should be taken into account when designing the linear layer and the key-expansion algorithm to avoid the existence of a large number of weak keys of the encryption function. However, this weakness may be eliminated by choosing appropriate linear (respectively, affine) layers $\mathcal{L}_1$ and $\mathcal{L}_2$ from $\mathsf{GL}_8(\mathbb{F}_2)$.

When looking at the TU-decomposition (see, e.g., [4]) of the 8-bit S-box $\hat{\pi}_{\mathsf{Kuz}} = \alpha \circ \pi_{\mathsf{Kuz}} \circ \omega$ used in the block cipher Kuznyechik [17], where $\alpha, \omega \in \mathsf{GL}_8(\mathbb{F}_2)$ and π_{Kuz} is a permutation based on a Feistel-like structure, we have found by using the W-intersection matrix that the subspace $\mathsf{W}_1 = \{(l\|0) | l \in V_4\}$ is invariant with respect to the action of the nonlinear bijective transformation $\pi_{\mathsf{Kuz}} = \omega^{-1} \circ \hat{\pi}_{\mathsf{Kuz}} \circ \alpha^{-1}$, i.e., $\pi_{\mathsf{Kuz}}(\mathsf{W}_1 \oplus 0\mathrm{x}c) = \mathsf{W}_1$. However, by computing $\mathcal{M}_{\mathsf{W}_i}(\hat{\pi}_{\mathsf{Kuz}}), i = 1, 2$, we have checked the absence of invariant subspaces such as W_1 and W_2 in the permutation $\hat{\pi}_{\mathsf{Kuz}}$.

In the above cases we have seen the important role played by the linear layers used in those constructions, which also explain why we have inserted these matrices into the original construction of $\hat{\pi}$. Its purposes are not only to break the cycle structure and eliminate the existence of fixed points, but also circumvent the existence of invariant subspaces such as W_1 and W_2.

3.5. Constructing highly-nonlinear involutions

In this section we will study how to build a particular kind of permutations with strong cryptographic properties using the construction presented in the previous section as building blocks.

Definition 16. Let ε be the identity permutation of $S(V_n)$. A permutation $\Phi \in S(V_n)$ is called an involution if $\Phi \circ \Phi = \varepsilon$.

Involutions are of particular interest in cryptography, because in the case of lightweight block ciphers these components are used to decrease the implementation cost of decryption process.

Even when the function $\mathcal{I}$ is an involution on $S(V_k)$ and the permutaion $h \in S(V_k)$ may be chosen to be involution too, the permutaions generated by π are not always involutions. Taking $h = \mathcal{I}$, in order to achieve the property $\pi_\psi \circ \pi_\psi = \varepsilon$ we have performed a search algorithm. The algorithm take as input a randomly generated non-bijective 4-bit function ψ, and for this ψ the resulting permutation π_ψ was constructed. Then the Hamming distance $\chi(\varepsilon, \pi_\psi \circ \pi_\psi)$ was calculated. If $\chi(\varepsilon, \pi_\psi \circ \pi_\psi) = 0$ and π_ψ satisfy the set of cryptographic criteria (listed in Section 2), the algorithm stops and as output we get a nonlinear involution. Otherwise, in an iterative process ψ is changed randomly (in an arbitrary number of positions) until $\chi(\varepsilon, \pi_\psi \circ \pi_\psi)$ became to be equal to zero, which means that an involution is founded. We repeated the above procedure until an involution π_ψ with the properties listed in the set of cryptographic criteria has been founded.

We have implemented this algorithm in SAGE [45] obtaining some 8-bit involutions π_ψ with $\#\mathsf{FixP}(\pi_\psi) = 16$ and the following cryptographic properties:

- $d_{min}(\pi_\psi) = 7$,
- $\delta_{\pi_\psi} \in \{6, 8\}$,
- $r_\pi = 3$ with $r^{(3)}_{\pi_\psi} = 441$,
- $100 \leqslant \mathcal{NL}(\pi_\psi) \leqslant 104$.

From a cryptographic point of view one need to minimize the number of fixed points of a permutation as much as possible [25]. Moreover, it is well-known that any involution may be easily distinguished from a random permutation by the number of its fixed points [6]. The results of the following propositions may help to develop a simple method allowing to minimize the size of $\mathsf{FixP}(\Phi)$, if the involution Φ has more than two fixed points.

Proposition 7. *Let Φ_1, Φ_2 be two involutions of $S(V_n)$ having the property $\Phi_1 \circ \Phi_2 = \Phi_2 \circ \Phi_1$. Then $\Phi_1 \circ \Phi_2$ is also an involution of $S(V_n)$.*

Proof. If Φ_1, Φ_2 are two involutions of $S(V_n)$ such that $\Phi_1 \circ \Phi_2 = \Phi_2 \circ \Phi_1$, then we have $(\Phi_1 \circ \Phi_2) \circ (\Phi_1 \circ \Phi_2) = \Phi_1 \circ (\Phi_2 \circ \Phi_2) \circ \Phi_1 = \Phi_1 \circ \Phi_1 = \varepsilon$. □

Proposition 8. *Let Φ be an involution of $S(V_n)$ having $\#\mathsf{FixP}(\Phi) \geqslant 2$. Then for any transposition $\tau = (\alpha, \beta) \in S(V_n)$, where $\alpha, \beta \in \mathsf{FixP}(\Phi)$, the permutation $\Phi \circ \tau$ is also an involution of $S(V_n)$.*

Proof. It is clear that any transposition is an involution. So for any involution $\tau = (\alpha, \beta) \in S(V_n)$ such that $\alpha, \beta \in \mathsf{FixP}(\Phi)$ the folowing relation holds:

$$\{x \in V_n \,|\, \Phi(x) \neq x\} \cap \{x \in V_n \,|\, \tau(x) \neq x\} = \varnothing, \tag{22}$$

i. e., permutations τ and Φ are independent[b]. It is well-known that for independent permutations the following equality holds: $\Phi \circ \tau = \tau \circ \Phi$ (see [16, Proposition 26, p. 227]), thus by Proposition 7 we conclude that permutation $\Phi \circ \tau$ is an involution in $S(V_n)$. □

Although by applying Proposition 8 to 8-bit involutions π_ψ with $\#\mathsf{FixP}(\pi) = 16$ we can remove all fixed points, the cryptographic properties related to linear and differential cryptanalysis of the new involutions slightly decrease in comparison with those generated by π_ψ. However, still by using this Proposition we can find almost optimal involutions without fixed points.

Also, we have tried to design directly involutions using our scheme as building block. To achieve the fulfillment of condition $\Phi \circ \Phi = \varepsilon$, our strategy was to combine our constructions into two or more rounds. Choosing two arbitrary k-bit involutions h_1, h_2, the following construction is able to produce $2k$-bit involutions.

Figure 2 shows that the construction of $\hat{\pi}^{(invol)}$ is a composition of three functions π_3, π_2 and π_1, where π_3 and π_1 have similarities with 1-round Lai – Massey scheme. The involution property of the whole construction may be derived from the well-known fact that if M is an involution over

[b] Permutations $h_1, h_2 \in S(V_n)$ are independent if $\{x \in V_n \mid h_1(x) \neq x\} \cap \{x \in V_n \mid h_2(x) \neq x\} = \varnothing$.

Construction of $\hat{\pi}^{(invol)}$

For the input value $(l\|r) \in V_{2k}$ we define the corresponding output value as follows
$\hat{\pi}^{(invol)}(l\|r) = \big(\pi_3 \circ \pi_2 \circ \pi_1\big)(l\|r) = l_1\|r_1$, where

$$\pi_1(l\|r) = (l \otimes \mathcal{I}(\psi(l \otimes r)))\Big\|(r \otimes \psi(l \otimes r)),$$

$$\pi_2(l\|r) = h_1(l)\Big\|h_2(r),$$

$$\pi_3(l\|r) = \Big(l \otimes \psi(l \otimes r)\Big)\Big\|\Big(r \otimes \mathcal{I}(\psi(l \otimes r))\Big).$$

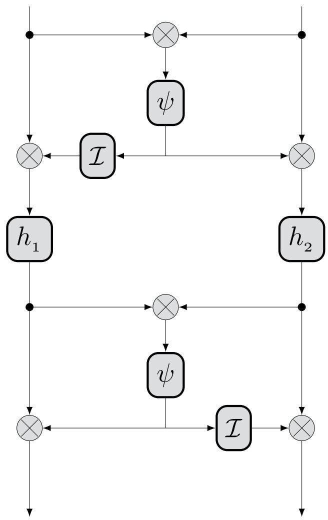

Fig. 2. Structure of $\hat{\pi}^{(invol)}$

V_n, then for any permutation $G \in V_n$ the resulting transformation $F = G^{-1} \circ M \circ G$ is an involution over V_n. Here
$F(l\|r) = \hat{\pi}_{invol}$, $G(l\|r) = \Big(l \otimes \mathcal{I}(\psi(l \otimes r))\Big\|(l \otimes \psi(l \otimes r))\Big)$,
$M(l\|r) = h_1(l)\|h_2(r)$ and $G^{-1}(l\|r) = \Big((l \otimes \psi(l \otimes r))\|(l \otimes \mathcal{I}(\psi(l \otimes r))\Big)$.

It is worth to note that, in the particular case of a construction of involution of the form $F = G^{-1} \circ M \circ G$, the nonlinear transformation F has exactly the same number of fixed points as the middle permutation M, and more general the same cycle structure (see [16, Theorem 34, p. 235]).

For sets $\mathsf{W}_*^{(1)} = \big\{(*\|r)\,\big|\, r \in V_k\big\}$, where $* \in \big\{\alpha, h_1(\alpha)\big\}$, and $\mathsf{W}_\star^{(2)} = \big\{(l\|\star)\,\big|\, l \in V_k\big\}$, where $\star \in \big\{\alpha, h_2(\alpha)\big\}$, the following relations hold:
$M\Big(\mathsf{W}_\alpha^{(1)}\Big) \subseteq \mathsf{W}_{h_1(\alpha)}^{(1)}, M\Big(\mathsf{W}_{h_1(\alpha)}^{(1)}\Big) \subseteq \mathsf{W}_\alpha^{(1)}, M\Big(\mathsf{W}_\alpha^{(2)}\Big) \subseteq \mathsf{W}_{h_2(\alpha)}^{(2)}, M\Big(\mathsf{W}_{h_2(\alpha)}^{(2)}\Big) \subseteq \mathsf{W}_\alpha^{(2)}$, which means that sets $\mathsf{W}_*^{(1)}, \mathsf{W}_\star^{(2)}$ are invariant with respect to the action of M and this is a weakness for permutation M. Moreover, some of these sets may be presented even after composition of π_3, π_2 and π_1. Indeed, if $h_1(0) = 0$, then for any $r \in V_k$ we have $\hat{\pi}^{(invol)}(0||r) = 0||r_1 \in \mathsf{W}_0^{(1)}$, and if $h_2(0) = 0$, then $\hat{\pi}^{(invol)}(l||0) = l_1||0 \in \mathsf{W}_0^{(2)}$, so in this case $\mathsf{W}_0^{(i)}, i = 1, 2$, are invariant subspaces with respect to $\hat{\pi}^{(invol)}$ and these structures should be taken into account when designing the linear layer and the key-expansion

algorithm of a block cipher to avoid the existence of a large number of weak keys for the encryption function. For this reason it is highly recommended to perform a search over the structure of $\hat{\pi}^{(invol)}$ using involutions h_1 and h_2 without fixed points.

Using the previous construction we have performed a search based on random generation of 4-bit involutions and 4-bit function $\psi\colon V_4 \to V_4^*$ aiming to find almost optimal involutions $\hat{\pi}^{(invol)}$ without fixed points (in contrast to those generated by the construction of π) with the parameters

- $d_{min}(\hat{\pi}^{(invol)}) = 7$,
- $\delta_{\hat{\pi}^{(invol)}} = 8$,
- $r_{\hat{\pi}^{(invol)}} = 3$ with $r^{(3)}_{\hat{\pi}^{(invol)}} = 441$,
- $100 \leqslant \mathcal{NL}(\hat{\pi}^{(invol)}) \leqslant 102$.

The possibility of having no fixed points in those involutions constructed under the $\hat{\pi}^{(invol)}$ scheme has some significances. In fact, the involutions produced by this construction have more finite field multiplications, this has an impact on the masking complexity of these kind of permutations in comparison with those involutions generated by π_ψ (see Section 5). Moreover, the cryptographic properties related to linear and differential cryptanalysis of involutions based on $\hat{\pi}^{(invol)}$-construction slightly decrease in comparison with those generated by π_ψ.

3.6. Searching of highly-nonlinear orthomorphisms

In this section we will study the possibility of using our algorithmic-algebraic scheme to find a special kind of the so-called complete mappings. Complete mapping were first introduced by Mann [33] and the term orthomorphisms was first used by Johnson, Dulmage and Mendelsohn [23] and were also studied in [13, 14, 34–40, 49]. Orthomorphisms are pertinent to the construction of mutually orthogonal Latin squares and may be used to design check digit systems.

In Cryptography, applications of orthomorphisms of the group $(V_n, \oplus)$ are found in the construction of block ciphers, stream ciphers and hash functions (in the Lai – Massey scheme, for example, in well-known FOX [47] family of block ciphers, Chinese stream cipher LOISS [22] and hash function EDON-R [21]). More recently, orthomorphisms have been used to strengthen the Even–Mansour block cipher against some cryptographic attacks [20].

Definition 17 ([37]). A permutation $\Phi \in S(V_n)$ is called ortomorphism on $(V_n, \oplus)$ if the mapping $\widetilde{\Phi}\colon V_n \to V_n$ defined as $\widetilde{\Phi}(x) = x \oplus \Phi(x)$ is a permutation of $S(V_n)$.

The set of all ortomorphisms of the group $(V_n, \oplus)$ is denoted by $\mathsf{Orth}(V_n)$. For any permutation $\Phi \in S(V_n)$ we define the set

$$\mathcal{D}_\Phi = \left\{\widetilde{\Phi}(x)\middle| x \in V_n\right\} = \left\{\Phi(x) \oplus x\middle| x \in V_n\right\}. \tag{23}$$

From (23) it follows that $\Phi \in \mathsf{Orth}(V_n)$ if and only if $\#\mathcal{D}_\Phi = 2^n$.

Proposition 9. *For any* $\Phi \in \mathsf{Orth}(V_n)$ *the following relations holds*: $\mathcal{W}_\Phi(a, b) = \mathcal{W}_{\widetilde{\Phi}}(a \oplus b, b)$ *and* $\Delta_\Phi(a, b) = \Delta_{\widetilde{\Phi}}(a, a \oplus b)$.

Proof. If the permutation $\Phi \in S(V_n)$ is an ortomorphism on V_n, then $\mathcal{W}_\Phi(a, b) = \sum\limits_{x \in V_n} (-1)^{\langle b, \Phi(x)\rangle \oplus \langle a, x\rangle} = \sum\limits_{x \in V_n} (-1)^{\left\langle b, \widetilde{\Phi}(x)\right\rangle \oplus \langle a \oplus b, x\rangle} = \mathcal{W}_{\widetilde{\Phi}}(a \oplus b, b)$ for all $a, b \in V_n$. Analogously, we can find that $\Delta_\Phi(a, b) = \Delta_{\widetilde{\Phi}}(a, a \oplus b)$ for all $a, b \in V_n$. □

The next proposition shows that regardless of the choice of the function ψ we can not construct orthomorphisms over $(V_n, \oplus)$ using the construction of π_ψ.

Proposition 10. *Let* $\psi\colon V_k \to V_k^*$ *be an arbitrary* k*-bit function. Then for permutation* $\pi_\psi\colon V_{2k} \to V_{2k}$, $\pi_\psi(l\|r) = (\mathcal{I}(l) \otimes \psi(l \otimes r))\|\mathcal{I}(r \otimes \psi(l \otimes r))$, *the following inequality holds*:

$$\#\mathcal{D}_{\pi_\psi} < 2^{2k}. \tag{24}$$

Proof. Let us fix an arbitrary k-bit function $\psi\colon V_k \to V_k^*$ and construct the permutation $\pi_\psi = (\mathcal{I}(l) \otimes \psi(l \otimes r))\|\mathcal{I}(r \otimes \psi(l \otimes r))$. As for any $a, b \in \mathbb{F}_{2^k} \setminus \{0\}$ the equation $a \otimes x = b$ has a unique solution, then for any $i \in \{0, 1, \ldots, 2^k - 1\}$ and some primitive element $c \in \mathbb{F}_{2^k}$ we have

$$\begin{aligned} \mathsf{ord}\, c &= 2^k - 1 \Rightarrow \mathsf{ord}\, c^{-2} = 2^k - 1 \Rightarrow \exists i : \psi(0) = c^{-2i} \\ &\Rightarrow \pi_\psi(0\|c^i) \oplus (0\|c^i) = \pi_\psi(0\|0) \oplus (0\|0) \Rightarrow \#\mathcal{D}_{\pi_\psi} < 2^{2k}. \end{aligned}$$

□

Let us now consider the class of permutations
$\dot{\pi}_\psi(l\|r) = \mathcal{I}(r \otimes \psi(l \otimes r))\|(\mathcal{I}(l) \otimes \psi(l \otimes r))$.

Proposition 11. *Let* $\psi, \psi'\colon V_k \to V_k^*$ *be two arbitrary mappings with* $\chi(\psi, \psi') = 1$. *Then for permutations* $\dot{\pi}_\psi, \dot{\pi}_{\psi'}$ *the following relations holds*:

1) $\left|\#\mathcal{D}_{\dot{\pi}_\psi} - \#\mathcal{D}_{\dot{\pi}_{\psi'}}\right| \leqslant 2\cdot(2^k-1)$, *if* $\psi(0)\neq\psi'(0)$,

2) $\left|\#\mathcal{D}_{\dot{\pi}_\psi} - \#\mathcal{D}_{\dot{\pi}_{\psi'}}\right| \leqslant 2^k-1$, *if* $\psi(i)\neq\psi'(i)$ *for some* $i\neq 0$.

Proof. Let prove the first item of the proposition. The set $\mathcal{D}_{\dot{\pi}_{\psi'}}$ may be written as

$$\begin{aligned}\mathcal{D}_{\dot{\pi}_{\psi'}} &= \left\{0\right\}\bigcup\left\{\mathcal{I}(r\otimes\psi'(0))\|r)\middle| r\in V_k^*\right\}\bigcup\left\{(l\|(\mathcal{I}(l)\otimes\psi'(0))\middle| l\in V_k^*\right\}\\ &\bigcup\left\{(\mathcal{I}(r\otimes\psi'(l\otimes r))\|(\mathcal{I}(l)\otimes\psi'(l\otimes r))\oplus(l\|r)\middle| l,r\in V_k^*\right\}.\end{aligned}$$

According the conditions of the proposition $\psi(0)\neq\psi'(0)$, and $\psi(j)=\psi'(j)$ for any $j\in V_k^*$. Then

$$\begin{aligned}\mathcal{D}_{\dot{\pi}_{\psi'}} &= \left\{0\right\}\bigcup\left\{\mathcal{I}(r\otimes\psi'(0))\|r)\middle| r\in V_k^*\right\}\bigcup\left\{(l\|(\mathcal{I}(l)\otimes\psi'(0))\middle| l\in V_k^*\right\}\\ &\bigcup\left\{(\mathcal{I}(r\otimes\psi(l\otimes r))\|(\mathcal{I}(l)\otimes\psi(l\otimes r))\oplus(l\|r)\middle| l,r\in V_k^*\right\},\end{aligned}$$

where $\#\left\{\mathcal{I}(r\otimes\psi'(0))\|r)\middle| r\in V_k^*\right\}=\#\left\{(l\|(\mathcal{I}(l)\otimes\psi'(0))\middle| l\in V_k^*\right\}=2^k-1$.

Since for the set $\mathcal{D}_{\dot{\pi}_\psi}$

$$\mathcal{D}_{\dot{\pi}_\psi}\supseteq\left\{0\right\}\bigcup\left\{(\mathcal{I}(r\otimes\psi(l\otimes r))\|(\mathcal{I}(l)\otimes\psi(l\otimes r))\oplus(l\|r)\middle| l\in V_k^*, r\in V_k^*\right\},$$

then

$$\mathcal{D}_{\dot{\pi}_{\psi'}}\subseteq\mathcal{D}_{\dot{\pi}_\psi}\bigcup\left\{\mathcal{I}(r\otimes\psi'(0))\|r)\middle| r\in V_k^*\right\}\bigcup\left\{(l\|(\mathcal{I}(l)\otimes\psi'(0))\middle| l\in V_k^*\right\}.$$

Hence

$$\#\mathcal{D}_{\dot{\pi}_{\psi'}}\leqslant\#\mathcal{D}_{\dot{\pi}_\psi}+2\cdot(2^k-1). \tag{25}$$

Analogously for $\mathcal{D}_{\dot{\pi}_\psi}$ the following inequality holds:

$$\#\mathcal{D}_{\dot{\pi}_\psi}\leqslant\#\mathcal{D}_{\dot{\pi}_{\psi'}}+2\cdot(2^k-1). \tag{26}$$

So, from (25),(26) we deduce that

$$\left|\#\mathcal{D}_{\dot{\pi}_\psi}-\#\mathcal{D}_{\dot{\pi}_{\psi'}}\right|\leqslant 2\cdot(2^k-1).$$

Let now prove the second item of the proposition. The set $\mathcal{D}_{\dot{\pi}_{\psi'}}$ may be decomposed into subsets as follows:

$$\begin{aligned}\mathcal{D}_{\dot{\pi}_{\psi'}} &= \left\{0\right\}\bigcup\left\{\mathcal{I}(r\otimes\psi'(0))\|r)\middle| r\in V_k^*\right\}\bigcup\left\{(l\|(\mathcal{I}(l)\otimes\psi'(0))\middle| l\in V_k^*\right\}\\ &\bigcup\left\{(\mathcal{I}(r\otimes\psi'(l\otimes r))\|(\mathcal{I}(l)\otimes\psi'(l\otimes r))\oplus(l\|r)\middle| l,r\in V_k^*\right\}.\end{aligned}$$

According the conditions of the proposition we have $\psi(i) \neq \psi'(i)$ for some $i \in V_k^*$, and $\psi(j) = \psi'(j)$ for any $j \in V_k \setminus \{i\}$. Then

$$\mathcal{D}_{\dot{\pi}_{\psi'}} = \Big\{0\Big\} \bigcup \Big\{\mathcal{I}(r \otimes \psi(0)) \| r) \Big| r \in V_k^*\Big\} \bigcup \Big\{(l \| (\mathcal{I}(l) \otimes \psi(0)) \Big| l \in V_k^*\Big\}$$
$$\bigcup \Big\{(\mathcal{I}(r \otimes \psi(l \otimes r)) \| (\mathcal{I}(l) \otimes \psi(l \otimes r)) \oplus (l \| r) \Big| l \in V_k^*, r \neq i \otimes l^{-1} \in V_k^*\Big\}$$
$$\bigcup \Big\{(\mathcal{I}(r \otimes \psi'(l \otimes r)) \| (\mathcal{I}(l) \otimes \psi'(l \otimes r)) \oplus (l \| r) \Big| l \in V_k^*, r = i \otimes l^{-1}\Big\},$$

and it is not difficult to see that
$\#\Big\{(\mathcal{I}(r \otimes \psi'(l \otimes r)) \| (\mathcal{I}(l) \otimes \psi'(l \otimes r)) \oplus (l \| r) \Big| l \in V_k^*, r = i \otimes l^{-1}\Big\} \leqslant 2^k - 1.$

Taking into account that

$$\mathcal{D}_{\dot{\pi}_{\psi}} \supseteq \Big\{0\Big\} \bigcup \Big\{\mathcal{I}(r \otimes \psi(0)) \| r) \Big| r \in V_k^*\Big\} \bigcup \Big\{(l \| (\mathcal{I}(l) \otimes \psi(0)) \Big| l \in V_k^*\Big\}$$
$$\bigcup \Big\{(\mathcal{I}(r \otimes \psi(l \otimes r)) \| (\mathcal{I}(l) \otimes \psi(l \otimes r)) \oplus (l \| r) \Big| l \in V_k^*, r \neq i \otimes l^{-1} \in V_k^*\Big\},$$

we find that

$$\mathcal{D}_{\dot{\pi}_{\psi'}} \subseteq \mathcal{D}_{\dot{\pi}_{\psi}} \bigcup \Big\{(\mathcal{I}(r \otimes \psi'(l \otimes r)) \| (\mathcal{I}(l) \otimes \psi'(l \otimes r)) \oplus (l \| r) \Big| l \in V_k^*, r = i \otimes l^{-1}\Big\},$$

which means

$$\#\mathcal{D}_{\dot{\pi}_{\psi'}} \leqslant \#\mathcal{D}_{\dot{\pi}_{\psi}} + 2^k - 1. \tag{27}$$

Analogously for $\mathcal{D}_{\dot{\pi}_{\psi}}$ the following inequality holds:

$$\#\mathcal{D}_{\dot{\pi}_{\psi}} \leqslant \#\mathcal{D}_{\dot{\pi}_{\psi'}} + 2^k - 1, \tag{28}$$

and thus from (27), (28) we obtain $\Big|\#\mathcal{D}_{\dot{\pi}_{\psi}} - \#\mathcal{D}_{\dot{\pi}_{\psi'}}\Big| \leqslant 2^k - 1.$

□

Proposition 11 may be used for searching highly-nonlinear orthomorphisms on $(V_{2k}, \oplus)$. In order to achieve the property $\#\mathcal{D}_{\dot{\pi}_{\psi}} = 2^{2k}$ we have performed a search algorithm similar to algorithm 1. The aim of this algorithm is to increase the value of $\#\mathcal{D}_{\dot{\pi}_{\psi}}$ up to 2^{2k}, which means that a nonlinear transformation of $\mathsf{Orth}(V_{2k})$ will be founded. At the same time, according to propositions 3 and 4 it is not difficult to see that the algorithm for searching this kind of permutations may also optimize the differential and (non)linear properties of the initial permutation $\dot{\pi}_{\psi}$. So, we have implemented this algorithm (which is omitted due to space limitations) in SAGE [45] obtaining some affine nonequivalent 8-bit nonlinear transformations $\dot{\pi}_{\psi} \in \mathsf{Orth}(V_8)$ having the following cryptographic parameters:

- $d_{min}(\dot{\pi}_\psi) = 7$,
- $\delta_{\dot{\pi}_\psi} = 8$,
- $r_{\dot{\pi}_\psi} = 3$ with $r^{(3)}_{\dot{\pi}_\psi} = 441$,
- $100 \leqslant \mathcal{NL}(\dot{\pi}_\psi) \leqslant 104$.

4. Some concrete S-boxes, its Pollock representations, column frequency tables and W-intersection matrices

We include in Table 2 some permutations generated by our method, one ordinary permutation with the best founded cryptographic parameters, two involutions and one of the best founded orthomophisms.

Table 2. Some constructed 8-bit S-boxes

S-box $\hat{\pi}_1$

$\mathcal{NL}(\hat{\pi}_1) = 104, \delta_{\hat{\pi}_1} = 6, d_{min}(\hat{\pi}_1) = 7, r_{\hat{\pi}_1} = 3, r^{(3)}_{\hat{\pi}_1} = 441.$

0x6e	0xe8	0x5f	0xa8	0x32	0x24	0xa7	0xe	0x1d	0x64	0x87	0x14	0xc3	0x6f	0x95	0x92
0xfb	0x4c	0x82	0x99	0x3d	0x19	0xac	0x45	0x9f	0xfe	0xde	0x15	0xb9	0xf9	0xe2	0x8a
0xec	0xf5	0xd	0xea	0x3a	0x77	0x47	0x12	0x11	0x1	0x97	0xc5	0x13	0x10	0x81	0x9d
0xed	0x75	0x88	0x68	0xfa	0xa4	0xc0	0xca	0xba	0xb2	0x3b	0x61	0xae	0xa	0x6c	0x65
0xd5	0x42	0x5d	0xdc	0xf2	0x85	0x9b	0xa6	0x67	0x50	0x63	0x91	0xc7	0x34	0x80	0xd7
0x96	0x1b	0x8e	0x5e	0x94	0x2f	0xb1	0xad	0xa0	0x93	0x2c	0x52	0xd0	0x29	0x7	0xc8
0x8d	0x7f	0x49	0x6b	0x36	0x2e	0xd9	0xe0	0x37	0xcd	0x83	0xaf	0x6d	0x57	0xce	0xb3
0x5c	0xc6	0x60	0xd8	0x3f	0xe4	0x4f	0xab	0x56	0xa1	0x72	0xe7	0x69	0xf1	0xdd	0x9c
0x84	0x90	0x25	0x4b	0x76	0x5a	0x6a	0xda	0xf0	0xe5	0x53	0x5b	0x7e	0x2a	0x2b	0xd3
0x35	0xa3	0x1c	0xa2	0x28	0x9e	0x30	0xa9	0xb4	0x6	0xb	0xef	0xaa	0x43	0xe9	0x7d
0xe1	0x3e	0x31	0x44	0x54	0xdb	0x79	0xc9	0x41	0xfc	0xf7	0x66	0x7a	0xb7	0x51	0x38
0xdf	0x62	0x40	0xbb	0x26	0x9	0xf3	0xcf	0xd2	0x1a	0x20	0xc	0x4	0x16	0x33	0x22
0x4e	0xa5	0x58	0x9a	0xd6	0x2	0xe6	0xcb	0xbe	0xeb	0x86	0x7b	0xbd	0xd1	0x3	0xf6
0xee	0x8f	0xf	0x55	0x8b	0x4a	0x7c	0x23	0x2d	0xb6	0x1f	0xc2	0x17	0xbf	0x73	0x8
0xcc	0x70	0x1e	0x59	0x46	0xe3	0x27	0xff	0x78	0xb8	0x18	0x21	0xd4	0xbc	0x98	0xf4
0xc1	0xc4	0x74	0x39	0x89	0xf8	0xfd	0x48	0x71	0x4d	0xb0	0x3c	0x0	0x8c	0xb5	0x5

Involution $\hat{\pi}_2$

$\mathcal{NL}(\hat{\pi}_2) = 104, \delta_{\hat{\pi}_2} = 6, d_{min}(\hat{\pi}_2) = 7, r_{\hat{\pi}_2} = 3, r^{(3)}_{\hat{\pi}_2} = 441.$

0x0	0x10	0x90	0xe0	0xd0	0xb0	0x70	0x60	0xf0	0x20	0xc0	0x50	0xa0	0x40	0x30	0x80
0x1	0x11	0x19	0x85	0x2f	0x2c	0x8b	0xf5	0x2e	0x12	0xfa	0x9a	0x8c	0x98	0xfb	0x93
0x9	0x2d	0x4e	0x3c	0x47	0xd5	0x36	0xdc	0x3b	0x29	0xdb	0x46	0x15	0x21	0x18	0x14
0xe	0xb3	0xb8	0x64	0xb4	0x81	0x26	0x3f	0x86	0x6b	0x89	0x28	0x23	0x65	0x3e	0x37
0xd	0x87	0x8a	0x63	0x6c	0x9c	0x2b	0x24	0x66	0x4f	0x96	0x9b	0x83	0x4d	0x22	0x49
0xb	0xad	0x62	0xbe	0x61	0x5c	0xb7	0xa8	0x69	0xb2	0xa3	0x5b	0x55	0xed	0xe1	0xe9
0x7	0x54	0x52	0x43	0x33	0x3d	0x48	0x67	0xc2	0x58	0x6e	0x39	0x44	0xcc	0x6a	0xcb
0x6	0xbd	0xbf	0x7c	0xaa	0xe2	0x76	0xdf	0xa5	0xb9	0xdd	0xe4	0x73	0xee	0xde	0xa9
0xf	0x35	0xc6	0x4c	0xc3	0x13	0x38	0x41	0xc8	0x3a	0x42	0x16	0x1c	0x8e	0x8d	0x8f
0x2	0x94	0x92	0x1f	0x91	0xd7	0x4a	0xe7	0x1d	0xd3	0x1b	0x4b	0x45	0xd6	0xea	0xe5
0xc	0xc1	0xc9	0x5a	0xcd	0x78	0xab	0xf9	0x57	0x7f	0x74	0xa6	0xac	0x51	0xfd	0xff
0x5	0xc4	0x59	0x31	0x34	0xb5	0xcf	0x56	0x32	0x79	0xbb	0xba	0xce	0x71	0x53	0x72
0xa	0xa1	0x68	0x84	0xb1	0xc7	0x82	0xc5	0x88	0xa2	0xca	0x6f	0x6d	0xa4	0xbc	0xb6
0x4	0xf6	0xd8	0x99	0xd4	0x25	0x9d	0x95	0xd2	0xfc	0xfe	0x2a	0x27	0x7a	0x7e	0x77
0x3	0x5e	0x75	0xe3	0x7b	0x9f	0xe8	0x97	0xe6	0x5f	0x9e	0xf1	0xf2	0x5d	0x7d	0xf7
0x8	0xeb	0xec	0xf4	0xf3	0x17	0xd1	0xef	0xf8	0xa7	0x1a	0x1e	0xd9	0xae	0xda	0xaf

Involution $\pi_3^{(invol)}$

$\mathcal{NL}(\pi_3^{(invol)}) = 100, \delta_{\pi_3^{(invol)}} = 8, d_{min}(\pi_3^{(invol)}) = 7, r_{\pi_3^{(invol)}} = 3, r^{(3)}_{\pi_3^{(invol)}} = 441.$

0x3e	0x37	0x56	0x45	0x53	0xc1	0xc8	0xe5	0x72	0x20	0xea	0xad	0xa9	0xc7	0xcf	0x5a
0xba	0x5b	0x73	0xf0	0x2f	0x83	0xdf	0xdb	0x9d	0x7c	0xb0	0x86	0xff	0x22	0xcd	0x93
0x9	0xa6	0x1d	0xe0	0xd9	0xe7	0xed	0x69	0x6c	0xb5	0xf5	0x46	0xa0	0xab	0xd6	0x14
0x6b	0x4a	0xa2	0x95	0x52	0x75	0x5d	0x1	0x9a	0x74	0xf6	0x44	0xae	0xf2	0x0	0xc5
0x8e	0x99	0xf1	0x79	0x3b	0x3	0x2b	0xfc	0xe9	0x5c	0x31	0x7e	0x50	0xca	0x98	0x55
0x4c	0x7f	0x34	0x4	0x61	0x4f	0x2	0xcc	0xdc	0x7d	0xf	0x11	0x49	0x36	0xdd	0x66
0xc6	0x54	0xb4	0xb9	0xd7	0xec	0x5f	0x8f	0xda	0x27	0x6e	0x30	0x28	0xa8	0x6a	0xe4
0xfa	0x84	0x8	0x12	0x39	0x35	0xd4	0x8b	0xce	0x43	0xe1	0x90	0x19	0x59	0x4b	0x51
0xcb	0xe2	0x85	0x15	0x71	0x82	0x1b	0xd3	0xa1	0xd1	0xeb	0x77	0xaf	0xbb	0x40	0x67
0x7b	0xe6	0xac	0x1f	0xe8	0x33	0xb3	0xd5	0x4e	0x41	0x38	0xde	0x9e	0x18	0x9c	0xbf
0x2c	0x88	0x32	0xb7	0xfb	0xbc	0x21	0xf9	0x6d	0xc	0xd0	0x2d	0x92	0xb	0x3c	0x8c
0x1a	0xef	0xee	0x96	0x62	0x29	0xbe	0xa3	0xc9	0x63	0x10	0x8d	0xa5	0xc3	0xb6	0x9f
0xfd	0x5	0xfe	0xbd	0xf7	0x3f	0x60	0xd	0x6	0xb8	0x4d	0x80	0x57	0x1e	0x78	0xe
0xaa	0x89	0xf3	0x87	0x76	0x97	0x2e	0x64	0xf4	0x24	0x68	0x17	0x58	0x5e	0x9b	0x16
0x23	0x7a	0x81	0xf8	0x6f	0x7	0x91	0x25	0x94	0x48	0xa	0x8a	0x65	0x26	0xb2	0xb1
0x13	0x42	0x3d	0xd2	0xd8	0x2a	0x3a	0xc4	0xe3	0xa7	0x70	0xa4	0x47	0xc0	0xc2	0x1c

Orthomorphism $\dot{\pi}_4$

$\mathcal{NL}(\dot{\pi}_4) = 104, \delta_{\dot{\pi}_4} = 8, d_{min}(\dot{\pi}_4) = 7, r_{\dot{\pi}_4} = 3, r^{(3)}_{\dot{\pi}_4} = 441.$

0xe1	0x3d	0x2d	0x17	0x51	0x71	0x9b	0x1a	0x96	0xfa	0x64	0x46	0x2f	0x1b	0xe3	0x40
0x1f	0xea	0x12	0xd1	0xa2	0x11	0x5d	0x44	0xb	0xa0	0xaa	0xc9	0x5f	0x58	0xf	0x15
0x5b	0xce	0x49	0x5c	0x7d	0x8a	0xb1	0x2	0x8c	0xcc	0xc8	0xaf	0x56	0xf7	0x4b	0x95
0xa3	0xab	0xcf	0x6f	0xeb	0xd9	0x37	0xdf	0xa8	0x3c	0xbd	0xa4	0x10	0xd7	0xed	0x24
0x29	0x7b	0xe9	0x27	0x22	0x57	0xb6	0xf6	0x79	0x45	0x55	0x82	0xb4	0xc5	0x97	0x69
0x48	0xda	0x2a	0x8f	0x6	0xe2	0x80	0xfe	0xc1	0xf5	0xff	0x3b	0x8d	0x6b	0x85	0xc3
0xdc	0x23	0xca	0x1e	0x5a	0xd	0xf3	0x0	0x81	0xe5	0xc4	0x52	0x32	0x3a	0x1d	0x6d
0x6a	0x77	0x75	0xbe	0xbb	0xb0	0xfc	0xc2	0xf8	0xb2	0x4a	0x9d	0x86	0x4	0x39	0x20
0xd4	0x8	0x4c	0x42	0x94	0xad	0x70	0xa5	0xd5	0x90	0xa7	0xe4	0x3f	0x53	0xde	0x9a
0x54	0xfd	0x2c	0x7	0x5	0x76	0xb8	0xdd	0x7f	0x87	0xa1	0x16	0xd2	0x3e	0xec	0x6e
0x63	0xc	0x50	0x3	0xe8	0x4e	0x73	0x26	0x13	0x4d	0x60	0xa6	0x2e	0xdb	0x8e	0x34
0x5e	0xe7	0xb9	0x1	0xf0	0x72	0xbf	0x25	0x93	0xae	0x62	0x83	0xf4	0xe6	0x47	0x19
0x89	0x7c	0x35	0xa9	0xb5	0x7a	0xf1	0x38	0xef	0x14	0xee	0x1c	0x74	0x31	0xe	0xfb
0xf9	0x91	0x78	0x33	0x18	0xd6	0xd8	0x41	0x9e	0x7e	0xa	0xd3	0x28	0xe0	0xb3	0x21
0x66	0x9f	0xba	0x2b	0x30	0x92	0xbc	0xc6	0x8b	0x6c	0x65	0x68	0x9c	0x4f	0xf2	0x61
0x36	0x84	0xcd	0xc0	0x88	0xc7	0xb7	0x43	0x59	0x98	0xd0	0x99	0x9	0xac	0xcb	0x67

In [4] the authors suggested looking at the visual representation of the LAT of an S-box with the goal to find some unexpected patterns, which may be used in some sense to distinguish it from a random one. The suggested representation is a heatmap of the LAT matrix and was called "a Jackson Pollock representation" of the LAT.

Similarly to [4], in [46] the author illustrate the usefulness of the "Jackson Pollock representation" of the LAT of an S-box, defining the so-called column frequency table, a tool which may be used to strengthen the effect of some unexpected patterns of a given S-box.

Definition 18 ([46]). Let $\mathcal{A}$ be an $n \times m$ matrix over $\mathbb{Z}$. The column frequency table of $\mathcal{A}$, denoted by $\mathsf{CF}(\mathcal{A})$, is defined as

$$\mathsf{CF}(\mathcal{A})[y,x] = \#\Big\{\hat{y} \in \{1,\ldots,n\} \,\Big|\, \mathcal{A}[\hat{y},x] = \mathcal{A}[y,x]\Big\}. \tag{29}$$

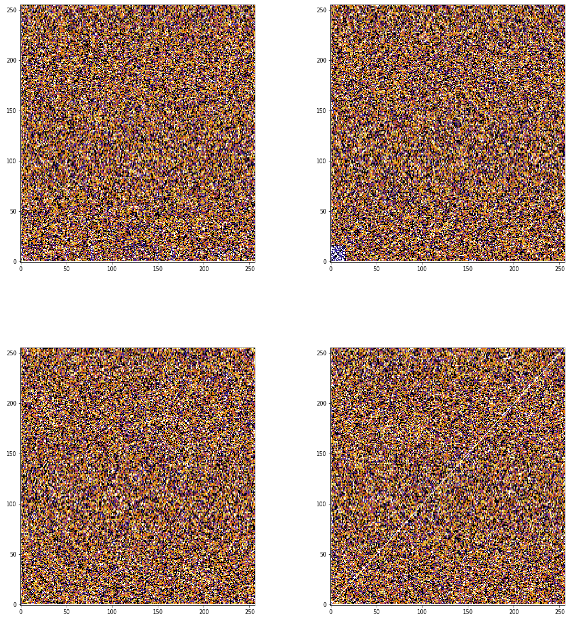

Fig. 3. Pollock representation of the LAT of S-boxes $\hat{\pi}_1$,$\hat{\pi}_2$,$\pi_3^{(invol)}$ and $\dot{\pi}_4$

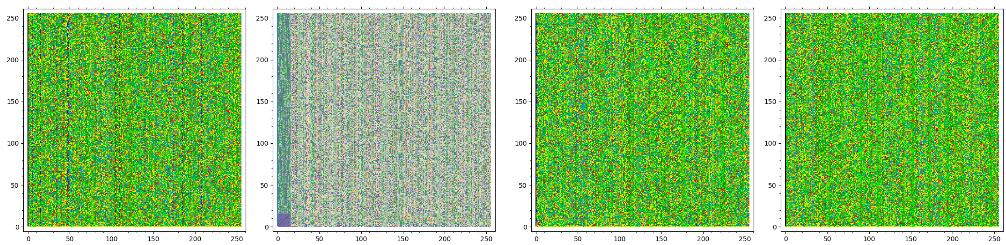

Fig. 4. Column Frequency Tables of the LAT of S-boxes $\hat{\pi}_1$,$\hat{\pi}_2$,$\pi_3^{(invol)}$ and $\dot{\pi}_4$

The Pollock representation and column frequency tables of the LAT of S-boxes $\hat{\pi}_1$,$\hat{\pi}_2$,$\pi_3^{(invol)}$ and $\dot{\pi}_4$ listed in Table 2 are shown in Fig. 3 and 4 respectively.

As may be observed, the existence of some visual patterns cannot be detected for the S-box $\hat{\pi}_1$, this is due to the use of some binary linear layers in construction of $\hat{\pi}_1$. If we remove these binary matrices, then some patterns appear in the S-box $\hat{\pi}_1$ similar to those detected for $\hat{\pi}_2$ (second image displayed in Fig. 3 and 4 respectively). When displaying the Pollock representation and column frequency tables of the LAT of $\pi_3^{(invol)}$ we don't find any patterns in these representations. The diagonal lines reflected in Fig. 3 and 4 respectively for the orthomorphism $\dot{\pi}_4$ is due to the fact that for any orthomorphism $\Phi \in \mathsf{Orth}(V_n)$ the relation $\mathcal{W}_{\Phi}(a, a) = \mathcal{W}_{\widehat{\Phi}}(0, a) = 0$ holds for all $a \in V_n$.

The W-intersection matrices (see Section 3.4) of nonlinear bijective transformations $\hat{\pi}_1$,$\hat{\pi}_2$,$\pi_3^{(invol)}$ and $\dot{\pi}_4$ for subspaces $\mathsf{W}_1 = \{(l\|0)|l \in V_4\}$, $\mathsf{W}_2 = \{(0\|r)|r \in V_4\}$ of the vector space V_8 are given below.

$$\mathcal{M}_{\mathsf{W}_1}(\hat{\pi}_1) = \begin{pmatrix}
1&2&1&1&0&1&3&0&1&2&2&0&1&0&1&0\\
0&2&0&1&2&0&0&0&2&2&1&1&0&1&1&3\\
2&4&0&1&1&0&0&1&1&2&0&0&1&0&2&1\\
1&0&0&1&0&0&4&1&1&0&2&2&2&0&1&1\\
0&0&0&1&1&2&2&0&2&2&1&0&1&3&0&1\\
1&1&3&0&0&2&0&0&1&3&2&1&1&1&0&0\\
0&0&1&2&1&1&2&1&2&0&1&1&2&1&1&0\\
0&0&0&1&1&2&2&1&0&1&2&0&1&2&2&1\\
0&0&3&0&1&3&1&2&1&1&0&0&0&2&1&1\\
2&1&1&2&1&0&0&1&0&1&4&1&0&0&2&0\\
0&0&0&3&2&2&1&2&0&0&0&1&1&1&1&2\\
3&2&3&1&1&0&1&0&0&0&0&1&1&2&0&1\\
2&0&0&0&1&1&0&1&1&1&1&2&1&2&2&1\\
2&2&2&0&1&1&0&2&2&0&0&2&1&0&1&0\\
0&2&2&0&1&1&0&2&0&1&0&2&1&1&1&2\\
2&0&0&2&2&0&0&2&2&0&0&2&2&0&0&2
\end{pmatrix}, \mathcal{M}_{\mathsf{W}_2}(\hat{\pi}_1) = \begin{pmatrix}
0&2&0&0&1&2&1&0&0&0&0&1&3&2&3&1\\
2&0&2&1&1&3&1&0&1&0&0&1&1&0&1&2\\
2&1&1&0&1&1&0&0&2&1&0&0&1&2&2&2\\
0&0&1&0&1&1&0&0&3&3&2&3&1&0&1&0\\
0&0&2&0&2&0&5&0&1&1&2&1&0&1&0&1\\
0&0&1&1&3&1&0&1&1&2&2&1&0&0&2&1\\
2&1&0&1&0&0&1&3&0&2&1&1&2&1&0&1\\
1&0&1&1&0&1&1&0&1&2&2&2&0&1&1&2\\
2&3&1&0&1&0&1&2&1&0&1&0&0&2&1&1\\
1&2&1&1&1&1&2&0&1&0&1&1&1&2&1&0\\
2&0&1&3&0&0&1&3&1&0&0&2&1&0&1&1\\
0&3&2&0&1&2&1&1&0&0&0&2&2&0&0&2\\
2&0&0&2&2&0&0&2&0&2&2&0&0&2&2&0\\
1&2&0&1&1&0&1&2&0&2&2&0&2&0&0&2\\
1&2&1&3&0&2&0&1&1&1&0&1&1&1&1&0\\
0&0&2&2&1&2&1&1&3&0&1&0&1&2&0&0
\end{pmatrix},$$

$$\mathcal{M}_{\mathsf{W}_1}(\hat{\pi}_2) = \begin{pmatrix}
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&3&3&0&0&0&0&0&3&3&0&0&0&0&0&3\\
1&3&3&3&3&0&0&0&0&0&0&0&0&3&0&0\\
1&0&3&3&0&0&3&0&3&0&0&3&0&0&0&0\\
1&0&3&0&3&0&3&0&3&3&0&0&0&0&0&0\\
1&0&0&0&0&3&3&0&0&0&3&3&0&0&3&0\\
1&0&0&3&3&3&3&0&0&0&0&0&3&0&0&0\\
1&0&0&0&0&0&0&3&0&0&3&3&0&3&3&0\\
1&3&0&3&3&0&0&0&3&0&0&0&3&0&0&0\\
1&3&0&0&3&0&0&0&0&3&0&0&0&3&3&0\\
1&0&0&0&0&3&0&3&0&0&3&0&3&0&0&3\\
1&0&0&3&0&3&0&3&0&0&0&3&3&0&0&0\\
1&0&0&0&0&0&3&0&3&0&3&3&3&0&0&0\\
1&0&3&0&0&0&0&3&0&3&0&0&0&3&0&3\\
1&0&0&0&0&3&0&3&0&3&0&0&0&0&3&3\\
1&3&0&0&0&0&0&0&0&0&3&0&0&3&3&3
\end{pmatrix}, \mathcal{M}_{\mathsf{W}_2}(\hat{\pi}_2) = \begin{pmatrix}
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&3&0&1&3&1&1&1&0&0&0&1&0&3&1&0\\
1&0&3&0&0&1&1&0&3&3&1&0&1&0&1&1\\
1&1&0&3&3&1&0&0&0&1&1&0&3&0&1&1\\
1&3&0&3&3&0&0&1&0&0&1&1&1&1&0&1\\
1&1&1&1&0&3&0&3&1&0&0&0&3&1&0&1\\
1&1&1&0&0&0&3&1&3&0&1&3&0&1&0&1\\
1&1&0&0&1&3&1&3&1&1&0&0&1&0&0&3\\
1&0&3&0&0&1&3&1&3&1&0&1&0&1&1&0\\
1&0&3&1&0&0&0&1&1&3&1&1&1&0&0&3\\
1&0&1&1&1&0&1&0&0&1&3&3&0&1&3&0\\
1&1&0&0&1&0&3&0&1&1&3&3&0&0&1&1\\
1&0&1&3&1&3&0&1&0&1&0&0&3&1&1&0\\
1&3&0&0&1&1&1&0&1&0&1&0&1&3&3&0\\
1&1&1&1&0&0&0&0&1&0&3&1&1&3&3&0\\
1&0&1&1&1&1&1&3&0&3&0&1&0&0&0&3
\end{pmatrix}$$

$$\mathcal{M}_{\mathsf{W}_1}(\pi_3^{(invol)}) = \begin{pmatrix}
0&0&0&2&0&0&1&0&0&1&4&3&2&1&2&0\\
0&0&2&0&2&1&2&1&1&2&2&1&0&0&0&2\\
0&2&2&2&2&1&1&0&1&0&0&0&1&2&2&0\\
2&0&2&0&1&3&1&2&1&2&0&0&0&1&0&1\\
0&2&2&1&0&0&1&2&2&2&0&2&0&0&0&2\\
0&1&1&3&0&2&0&3&0&1&1&0&2&0&0&2\\
1&2&1&1&1&0&0&0&1&0&1&2&0&2&2&2\\
0&1&0&2&2&3&0&0&0&2&0&2&2&1&0&1\\
0&1&1&1&2&0&1&0&0&2&2&0&2&2&2&0\\
1&2&0&2&2&1&0&2&2&0&0&0&3&1&0&0\\
4&2&0&0&0&1&1&0&2&0&2&1&0&1&1&1\\
3&1&0&0&2&0&2&2&0&0&1&0&0&3&2&0\\
2&0&1&0&0&2&0&2&2&3&0&0&0&0&2&2\\
1&0&2&1&0&0&2&1&2&1&1&3&0&0&2&0\\
2&0&2&0&0&0&2&0&2&0&1&2&2&2&0&1\\
0&2&0&1&2&2&2&1&0&0&1&0&2&0&1&2
\end{pmatrix}, \mathcal{M}_{\mathsf{W}_2}(\pi_3^{(invol)}) = \begin{pmatrix}
0&0&1&2&1&3&0&1&0&0&2&0&4&0&2&0\\
0&0&2&0&0&1&0&2&2&2&0&2&1&2&0&2\\
1&2&0&0&1&0&2&0&0&0&3&1&0&2&3&1\\
2&0&0&0&2&2&1&2&0&2&2&0&1&0&0&2\\
1&0&1&2&0&3&0&2&1&2&0&0&1&0&1&2\\
3&1&0&2&3&0&2&2&0&0&0&0&1&2&0&0\\
0&0&2&1&0&2&2&0&1&0&1&2&1&2&2&0\\
1&2&0&2&2&2&0&0&2&1&0&0&1&1&1&1\\
0&2&0&0&1&0&1&2&2&0&2&1&1&2&2&0\\
0&2&0&2&2&0&0&1&0&2&1&2&0&2&2&0\\
2&0&3&2&0&0&1&0&2&1&0&2&0&1&0&2\\
0&2&1&0&0&0&2&0&1&2&2&2&2&0&2&0\\
4&1&0&1&1&1&1&1&1&0&0&2&0&0&0&3\\
0&2&2&0&0&2&2&1&2&2&1&0&0&0&0&2\\
2&0&3&0&1&0&2&1&2&2&0&2&0&0&0&1\\
0&2&1&2&2&0&0&1&0&0&2&0&3&2&1&0
\end{pmatrix},$$

$$\mathcal{M}_{\mathsf{W}_1}(\dot{\pi}_4) = \begin{pmatrix}
0&3&2&1&2&1&1&1&0&2&0&0&0&0&2&1\\
2&4&0&0&1&3&0&0&0&0&3&0&1&1&1&0\\
1&0&0&0&2&3&0&1&2&1&1&1&3&0&0&1\\
0&1&1&2&0&0&1&0&0&0&4&1&1&3&2&0\\
0&0&3&0&1&2&1&2&1&1&0&2&1&0&1&1\\
1&0&1&1&1&0&1&0&4&0&0&0&2&1&1&3\\
2&2&1&2&0&2&1&0&1&0&0&0&2&1&1&1\\
1&0&1&1&1&0&1&2&1&1&0&4&1&0&0&2\\
1&0&0&1&2&1&0&1&0&3&3&0&0&3&1&0\\
2&1&1&1&0&1&1&2&1&0&1&1&0&2&1&1\\
2&1&2&1&2&1&2&1&1&0&1&0&0&1&1&0\\
1&1&1&0&1&1&1&1&1&1&1&2&0&0&2&2\\
1&2&0&3&0&0&0&3&1&0&1&1&0&0&2&2\\
1&1&2&1&1&0&0&2&0&2&0&1&0&3&1&1\\
0&0&1&1&1&0&5&0&1&3&0&2&1&0&0&1\\
1&0&0&1&1&1&1&0&2&2&1&1&4&1&0&0
\end{pmatrix}, \mathcal{M}_{\mathsf{W}_2}(\dot{\pi}_4) = \begin{pmatrix}
0&1&0&2&2&0&2&0&1&3&1&1&1&0&1&1\\
0&1&0&1&1&0&0&2&1&0&2&2&2&2&1&1\\
1&0&1&0&0&2&0&0&1&3&3&0&2&2&0&1\\
1&2&1&2&0&0&0&3&0&1&0&1&1&0&2&2\\
2&1&2&0&1&2&1&0&3&0&1&2&0&1&0&0\\
1&2&3&0&0&0&2&2&0&1&2&0&0&2&1&0\\
2&2&0&2&0&0&1&2&2&0&0&1&2&1&0&1\\
1&1&2&1&1&2&3&0&1&0&1&0&0&1&1&1\\
0&2&0&2&0&1&1&0&2&2&0&2&1&0&1&2\\
2&0&1&0&1&3&0&1&1&0&1&0&3&1&2&0\\
2&1&1&0&2&2&0&1&1&0&3&0&0&1&1&1\\
0&0&2&2&2&0&3&0&1&2&0&1&1&1&0&1\\
1&0&2&0&3&0&2&0&1&1&0&0&1&1&1&3\\
1&1&0&1&1&1&1&2&1&0&1&3&1&0&1&1\\
0&0&1&2&0&1&0&2&0&1&0&2&1&2&3&1\\
2&2&0&1&2&2&0&1&0&2&1&1&0&1&1&0
\end{pmatrix}.$$

As it may be seen, the matrices $\mathcal{M}_{\mathsf{W}_i}(s), i = 1, 2,$ where $s \in \{\hat{\pi}_1, \hat{\pi}_2, \pi_3^{(invol)}, \dot{\pi}_4\}$, do not have any element equal to 16, which confirms that subspaces $\mathsf{W}_1 = \{(l\|0)|l \in V_4\}$, $\mathsf{W}_2 = \{(0\|r)|r \in V_4\}$ of the vector space V_8 are not invariant with respect to the action of these nonlinear bijective transformations.

5. Masking complexity of 8-bit S-boxes obtained by the scheme of π_ψ and $\hat{\pi}^{(invol)}$

In this section we study the possibility to combine our 8-bit S-boxes with the classical masking countermeasure against SCAs in terms of its masking complexity. The polynomial representation of an S-box defined by relation (7) is based on four kinds of operations over $\mathbb{F}_{2^n}$: additions, multiplications by constants (scalar multiplications), squares, and nonlinear multiplications (i. e. multiplications of two different variables). Except for the latter, all these operations are linear (respectively, affine) over V_n. The processing of any S-box may then be performed as a sequence of functions which are linear (respectively, affine) over V_n (themselves composed of additions, squares and scalar multiplications) and of nonlinear multiplications. Hence, masking an S-box processing may be done by masking every operation mentioned above independently. We recall hereafter the concept of masking complexity defined as follows.

Definition 19 ([9]). The masking complexity of any n-bit S-box Φ, denoted by $\mathcal{MC}(\Phi)$, is the minimal number of nonlinear multiplications required to evaluate its polynomial representation over $\mathbb{F}_{2^n}$.

Denoting by $\mathcal{M}_k^n$ the class of exponents α such that X^α has a masking complexity equal to k we summarizes in Table 3 the results (obtained in [9]) for the cyclotomic classes $C_\alpha = \{\alpha \cdot 2^j \mod (15) \,|\, j = 0, 1, 2, 3\}$ in $\mathcal{M}_k^4$.

Table 3. Cyclotomic classes for $n = 4$ w.r.t. the masking complexity k

k	Cyclotomic classes in $\mathcal{M}_k^4$
0	$C_0 = \{0\}, C_1 = \{1, 2, 4, 8\}$
1	$C_3 = \{3, 6, 12, 9\}, C_5 = \{5, 10\}$
2	$C_7 = \{7, 11, 13, 14\}$

Taking into account that the number of field multiplications for any 4-bit permutation and any 4-bit non-bijective function is lower bounded by 0 and upper bounded by $3, 4$ respectively (see [9]), we obtain the following bounds for 8-bit S-boxes produced by our construction:

$$5 \leqslant \#\text{ nonlinear multiplications of } \pi_\psi \leqslant 12. \tag{30}$$

As we can see from (30), 8-bit S-boxes with only 5 nonlinear multiplications over $\mathbb{F}_{2^4}$ may be constructed using the proposed scheme.

The number of field multiplications for those involutions obtained by the $\pi^{(invol)}$ scheme is given by the following bound $10 \leqslant \#\text{ nonlinear multiplications of } \pi^{(invol)} \leqslant 24$. As we can see, masking these involutions is more expensive than ordinary S-boxes produced by the construction of π_ψ.

Finally, in Table 4 we compare our results with some candidates having a given level of masking. As we can see, our S-boxes based on π scheme

Table 4. Comparison of 8-bit S-boxes w.r.t. # nonl. multiplications

S-box class	# nonl. multiplications
AES's S-box [19] AES's S-box [26]	4 ($\mathbb{F}_{2^8}$) 5 ($\mathbb{F}_{2^4}$)
Clefia S-box [19]	10 ($\mathbb{F}_{2^8}$)
Iceberg S-box [19]	18 ($\mathbb{F}_{2^4}$)
Khazad S-box [19]	18 ($\mathbb{F}_{2^4}$)
Picaro S-box [41]	4 ($\mathbb{F}_{2^4}$)
Zorro S-box [19]	4 ($\mathbb{F}_{2^4}$)
S-boxes based on π_ψ scheme [this work]	$5 \leqslant$ # nonl. multiplications $\leqslant 12$
S-boxes based on $\pi^{(invol)}$ scheme [this work]	$10 \leqslant$ # nonl. multiplications $\leqslant 24$

exhibits better values of field multiplications than S-boxes of Clefia, Iceberg and Khazad respectively, having at the same time stronger cryptographic properties but at the cost of worse number of nonlinear multiplications compared with the AES [26], Picaro [41] and Zorro S-boxes [19].

6. Conclusion and Future Work

In this paper we have presented a new algorithmic-algebraic scheme based on the Lai – Massey structure for constructing permutations of dimension $n = 2k, k \geqslant 2$. Compared to the best nonlinearity (108 for $k = 4$) offered by the construction presented in [11] and latter generalized in [18], the nonlinearity of permutations obtained by our scheme is slightly smaller (equal to 104), but to the best of our knowledge the schemes presented in [11,18] cannot produce involutions and orthomorphisms with cryptographic properties close to the optimal ones, so we can conclude that the new structure presented in this paper is more powerful and attractive due to the diversity of permutations that may be constructed. Interestingly, the involutions and orthomorphisms founded in our paper have comparable classical cryptographic properties as those constructed by using spectral-linear and spectral-differential methods [34] and the limited deficit's method [36]. The main advantage of our 8-bit permutations is that they may be constructed using smaller 4-bit components which is useful for the implementation of the S-box in hardware or using a bit-sliced approach. There are several questions (more theoretical results, hardware and bit-sliced implementations, more efficient methods of masking) about the class of permutations suggested in this work which are left for future work.

Acknowledgement: The author is very grateful to Oleg V. Kamlovskii and the anonymous reviewers of CTCrypt'2020 and Mathematical Aspects of Cryptography for their useful comments and valuable observations, which helped to improve the final version of this article.

References

[1] Avanzi R.A., *A Salad of Block Ciphers. The State of the Art in Block Ciphers and their Analysis*, Cryptology ePrint Archive, Report 2017/1171 http://eprint.iacr.org/2017/1171.

[2] Bannier A., Bodin N., Filiol E., "Partition-based trapdoor ciphers", Cryptology ePrint Archive, Report 2016/493, http://eprint.iacr.org/2016/493.

[3] Bracken C., Leander G., "A highly nonlinear differentially 4 uniform power mapping that permutes fields of even degree", Finite Fields and Their Appl., **16**, 2010, 231–242.

[4] Biryukov A., Perrin L., Udovenko A., "Reverse engineering the S-box of Streebog, Kuznyechik and STRIBOBr1", EUROCRYPT 2016, Lect. Notes Comput. Sci., **9665**, 2016, 372–402.

[5] Boura C., Canteaut A., Jean J. et al., "Two notions of differential equivalence on S-boxes", *Designs, Codes and Cryptogr.*, **87**, 2019, 185–202.

[6] Boura C., Canteaut A., Knudsen L.R. et al., "Reflection ciphers", *Designs, Codes and Cryptogr.*, **82**, 2017, 3–25.

[7] Brier E., Clavier C., Olivier F., "Correlation power analysis with a leakage model", CHES 2004, Lect. Notes Comput. Sci., **3156**, 2004, 157–173.

[8] Carlet C., *Boolean Functions for Cryptography and Coding Theory*, Cambridge, Cambridge Univ. Press, 2021.

[9] Carlet C., Goubin L., Prouff E., Quisquater M., Rivain M., "Higher-order masking schemes for S-boxes", FSE 2012., Lect. Notes Comput. Sci., **7549**, 2012, 366–384.

[10] Courtois N. T., Pieprzyk J., "Cryptanalysis of block ciphers with overdefined systems of equations", Cryptology ePrint Archive, Report 2002/044, https://eprint.iacr.org/2002/044.

[11] De la Cruz Jiménez R.A., "Generation of 8-Bit S-boxes having almost optimal cryptographic properties using smaller 4-bit S-boxes and finite field multiplication", LATINCRYPT 2017, Lect. Notes Comput. Sci., **11368**, 2017, 191–206.

[12] Dinur A., Shamir A., "Cube attacks on tweakable black box polynomials", Cryptology ePrint Archive, Report 2008/385, https://eprint.iacr.org/2008/385.

[13] Evans A., "Applications of complete mappings and orthomorphisms of finite groups", *Quasigroups and Related System*, **23** (2015), 5–30.

[14] Evans A., *Orthomorphism graphs of groups*, Springer-Verlag, Berlin, Heidelberg, 1992, 116 pp.

[15] Gierlichs B., Batina L., Tuyls P., Preneel B., "Mutual information analysis", CHES 2008., Lect. Notes Comput. Sci., **5154**, 2008, 426-442.

[16] Glukhov M.M., Elizarov V.P., Nechaev A.A., *Algebra: Textbook. 2nd ed., revised and suppl.*, Lan', Sankt-Peterburg–Moskva–Krasnodar, 2015 (in Russian).

[17] *GOST R* 34.12-2015 *Information technology. Cryptographic protection of information. Block ciphers. Moscow, Standartinform*, 2015.

[18] Fomin D. B., "New classes of 8-bit permutations based on a butterfly structure", *Matematicheskie voprosy kriptografii*, **10**:2 (2019), 169–180.

[19] Gérard B., Grosso V., Naya-Plasencia M., Standaert F.X., "Block ciphers that are easier to mask: how far can we go?", CHES 2013., Lect. Notes Comput. Sci., **8086**, 2013, 383–399.

[20] Gérard G. Sh., Gueron Sh., *Balanced permutations Even–Mansour ciphers*, Cryptology ePrint Archive, Report 2014/642, 2014 https://eprint.iacr.org/2014/642.

[21] Gligoroski D., Odegard R.S., Mihova M., et al., "Cryptographic hash function Edon-R", IEEE, Proc. 1st Int. Workshop Security Communic. Networks, IWSCN, 2009, 1–9.

[22] Feng D., Feng X., Zhang W., Fan X., Wu C., "Loiss: a byte oriented stream cipher", IWCC 2011, Lect. Notes Comput. Sci., **6639**, 2011, 109–125.

[23] Johnson D.M., Dulmage A.L., Mendelsohn N.S., "Orthomorphisms of groups and orthogonal Latin squares. I.", *Canad. J. Math.*, **13**, 1961, 356–372.

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

[25] Kazymyrov O. V., Kazymyrova V. N., *Extended criterion for absence of fixed points*, Cryptology ePrint Archive, Report 2013/576, https://eprint.iacr.org/2013/576.

[26] Kim H., Hong S., Lim J., "A fast and provably secure higher-order masking of AES S-box", CHES 2011, Lect. Notes Comput. Sci., **6917**, 2011, 95–107.

[27] Kim J., *Combined differential, linear and related-key attacks on block ciphers and MAC algorithms*, Cryptology ePrint Archive, Report 2006/451, http://eprint.iacr.org/2006/451.pdf.

[28] Kocher P., Jaffe J., Jun B., *Introduction to Differential Power Analysis and Related Attacks. Techn. Rep.*, Cryptography Research Inc., 1998, http://www.cryptography.com/resources/whitepapers/DPA-technical.html.

[29] Kocher P., "Timing attacks on implementations of Diffie-Hellman,RSA, DSS and other systems", CRYPTO '96., Lect. Notes Comput. Sci., **1109**, 1996, 104–113.

[30] Knudsen L. R., "Truncated and higher order differentials", FSE 1994., Lect. Notes Comput. Sci., **1008**, 1994, 196–211.

[31] Lachaud G., Wolfmann J., "The weights of the orthogonals of the extended quadratic binary Goppa codes", *IEEE Trans. Inf. Theory*, **36**:3 (1990), 686–692.

[32] Leander G., Abdelraheem M., Alkhzaimi H., Zenner E., "A cryptanalysis of PRINTcipher: The invariant subspace attack", CRYPTO 2011, Lect. Notes Comput. Sci., **6841**, 20110, 206–221.

[33] Mann H.B., "On orthogonal Latin squares", *Bull. Amer. Math. Soc.*, **50** (1944), 249–257.

[34] Menyachikhin A. V., "Spectral-linear and spectral-differential methods for generating S-boxes having almost optimal cryptographic parameters", *Matematicheskie Voprosy Kriptografii*, **8**:2 (2017), 97–116.

[35] Menyachikhin A. V., *Method for generating S-boxes using the values of linear and differential spectra and device for its realization*, RU Patent № 2633132, Bull. № 29, 2017, https://patentdb.ru/patent/2633132 (in Russian).

[36] Menyachikhin A.V., "Orthomorphisms of Abelian groups with minimal pairwise distances", *Discrete Math. Appl.*, **30**:3 (2020), 177–186.

[37] Menyachikhin A.V., "The limited deficit's method and the construction problem of orthomorphisms and almost ortomorphisms of Abelian group", *Diskr. Matem.*, **31**:3 (2019), 58–77 (in Russian).

[38] Menyachikhin A. V., *Device for generating orthomorphisms using paired differences*, RU Patent № 2632119, Bull. № 28, 2017, https://patentdb.ru/patent/2632119 (in Russian).

[39] Niederreiter H., Robinson K., "Bol loops of order pq", *Math. Proc. Cambridge Phil. Soc.*, **89** (1981), 241–256.

[40] Niederreiter H., Robinson K., "Complete mappings of finite fields", *J. Australian Math. Soc.*, **33** (1982), 197–212.

[41] Piret G., Roche T., Carlet C., "PICARO – A block cipher allowing efficient higher-order side-channel resistance", ACNS 2012, Lect. Notes Comput. Sci., **7341**, 2012, 311–328.

[42] Pogorelov B. A., Pudovkina M. A., "On the distance from permutations to imprimitive groups for a fixed system of imprimitivity", *Discrete Math. Appl.*, **24**:2 (2014), 95–108.

[43] Pokrasenko D. P., “On the maximal component algebraic immunity of vectorial Boolean functions”, *J. Appl. Industr. Math.*, **10**:2 (2016), 257–263.

[44] Rijmen V., Preneel B., “A family of trapdoor ciphers”, FSE 1997., Lect. Notes Comput. Sci., **1267**, 1997, 139–148.

[45] *Sage Mathematics Software* (*Version* 8.1), 2018 http://www.sagemath.org.

[46] Udovenko A., *Design and Cryptanalysis of symmetric-key algorithms in black and white-box models*, PhD diss., Univ. Luxembourg, 2019, 268 pp.

[47] Vaudenay S., Junod P., *Device and method for encrypting and decrypting a block of data. United States Patent* (20040247117), 2004, https://patents.justia.com/patent/20040247117.

[48] Lai X., Massey J.L., “A proposal for a new block encryption standard”, EUROCRYPT’90, Lect. Notes Comput. Sci., **473**, 1991, 389–404.

[49] Yan T., Huanguo Zh., Haiqing H., “Using evolutionary computation in construction of orthomorphism”, 2009 *Int. Conf. Multimed. Inf. Netw. Security*, **2**, Hubei, China, 2009, 478–481.