МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2019 Т. 10 № 2 С. 169–180

УДК 519.719.2 DOI https://doi.org/10.4213/mvk294

New classes of 8-bit permutations based on a butterfly structure

D. B. Fomin

Technical Committee for Standardization “Cryptography and security mechanisms” (TC 26), Moscow, Russia

Получено 06.II.2018

Abstract. New classes of 8-bit permutation based on a butterfly structure are introduced. These classes set up a new way for generating $2n$-bit permutation from n-bit ones. We introduce some classes that contain permutations with good cryptographic properties and could be efficiently implemented for hardware and software applications.

Key words: Boolean function, S-box, butterfly structure, bent function

Новые классы 8-битовых подстановок, построенных с использованием конструкции «бабочка»

Д. Б. Фомин

Технический комитет по стандартизации «Криптографическая защита информации», Москва, Россия

Аннотация. Описаны новые классы 8-битовых подстановок, построенных с использованием конструкции типа «бабочка». Эти классы дают новый способ построения $2n$-битовых подстановок по n-битовым. Введены классы подстановок, которые обладают хорошими криптографическими свойствами и могут быть эффективно реализованы как программно, так и аппаратно.

Ключевые слова: булева функция, подстановка, конструкция типа «бабочка», бент-функция

Citation: *Mathematical Aspects of Cryptography*, 2019, v. 10, № 2, pp. 169–180 (Russian)

1. Introduction

Permutations are essential part of huge classes of cryptographic functions. These functions are used to construct symmetric encryption functions such as stream ciphers, block ciphers and hash functions. According to Shannon's criteria [1] every strong cryptographic function should provide confusion and diffusion. One of the well studied way to hide the relationship between the key and plaintext (or provide confusion) is using a substitutional-box — S-Box. Today, after decades of cryptanalysis of modern cryptographic functions there are several known properties for S-Box to be a part of secure cryptographic function.

There are a lot of reasons to compose S-Boxes from smaller ones: good software implementation with precomputed tables, better bit-sliced implementation, implementation for lightweight cryptography with smaller tables or lower gate count, efficient masking in hardware [2, 3]. Permutations which are composed from smaller ones are more secure against cache timing attacks than those relying on general 8-bit S-boxes, which require table lookups in memory [4]. There are known a lot of ways to construct large S-Box from smaller one: constructions based on Feistel network [5–7], Misty network [8, 5, 9], SPN network [10–12] or other constructions [13].

In this work we will study how to compose 8-bit S-box using a butterfly structure that was suggested in [4] and was obtained while studying decomposition of the Dillon APN permutation [14].

2. Definitions and Notation

We will use the following notation and definitions. Let $\mathbb{F}_{2^n}$ be a finite field of size 2^n. Every $a \in \mathbb{F}_{2^n}$ may be considered as a n-bit vector $a = (a_0, a_1, \ldots, a_{n-1})$, $a_i \in \mathbb{F}_2$, $i \in \overline{0, n-1}$. For any $a, b \in \mathbb{F}_{2^n}$ the operation $\langle a, b \rangle$ is a dot product: $\sum_{i=0}^{n-1} a_i \cdot b_i$.

S-Box S is any nonlinear function $S : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$. In this work we construct nonlinear bijective S-Boxes. These S-Boxes may be parts of a huge class of cryptographic functions based on block ciphers like SPN-network, Feistel network and etc. For every nonlinear function we can evaluate several measures of resistance against known methods of cryptanalysis. These measures are called properties of nonlinear function. Some of them are defined as follows.

Definition 1. The Walsh–Hadamard Transform (WHT) of an S-Box S for $a \in \mathbb{F}_{2^n}$, $b \in \mathbb{F}_{2^m}$ is defined as

$$W_S(a, b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\langle a, x \rangle + \langle b, S(x) \rangle}.$$

This function measures the correlation between the Boolean $\langle b, S(x)\rangle$ and linear $\langle a, x\rangle$ functions.

Definition 2. The nonlinearity N_S of an S-Box S is a measure that is defined as follows:

$$N_S = 2^{n-1} - \frac{1}{2}\max_{a,b\neq 0}\left|W_S(a,b)\right|.$$

S-Box with larger nonlinearity has better resistance against linear cryptanalysis. As an example, for $\mathbb{F}_{2^8}$ the permutation with the largest nonlinearity is the finite field inversion x^{-1} with $N_{x^{-1}} = 112$.

Definition 3. A nonlinear function $S\colon \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ is called a bent function if its nonlinearity is equal to $2^{n-1} - 2^{n/2-1}$. Let $n = 2m,\ x, y \in \mathbb{F}_{2^m}$. The Maiorana–McFarland construction [15] is the way to construct $2n$-bit bent-function from n-bit functions and finite field multiplication: every function $g\colon V_m \times V_m \mapsto V_n$ that has the following form is a bent function:

$$g(x, y) = \pi(x)\cdot l(y) + f(x),$$

where $\pi : \mathbb{F}_{2^m} \mapsto \mathbb{F}_{2^m}$ is a permutation, $l : \mathbb{F}_{2^m} \mapsto \mathbb{F}_{2^m}$ is a linear permutation and $f : \mathbb{F}_{2^m} \mapsto \mathbb{F}_{2^m}$ is a function.

Definition 4. The algebraic degree $\deg(S)$ of the S-Box S is the minimum among all maximum numbers of variables of the terms in the algebraic normal form (ANF) of $\langle a, S(x)\rangle$ for all possible values x and $a \neq 0$:

$$\deg(S) = \min_{a\in\mathbb{F}_{2^m}\setminus 0} \deg\left(\langle a, S(x)\rangle\right).$$

For any permutation on $\mathbb{F}_{2^n}$ the maximum value of the algebraic degree is $n-1$.

Definition 5. For a given $a \in \mathbb{F}_{2^m}\setminus 0, b \in \mathbb{F}_{2^m}$ we consider

$$\delta_S(a, b) = \#\left\{x \in \mathbb{F}_{2_n} | S(x + a) + S(x) = b\right\}.$$

The differential uniformity of an S-Box S is

$$\delta_S = \max_{a\in\mathbb{F}_{2^m}\setminus\{0,b\}} \delta_S(a, b).$$

The S-Box with smaller differential uniformity has the better resistance against differential cryptanalysis. For $\mathbb{F}_{2^8}$, permutation with the smallest known differential uniformity is the finite field inversion x^{-1} with $\delta_{x^{-1}} = 4$.

We will say that two permutation S_1 and S_2 are linear equivalent if there exist two linear permutations L_1 and L_2 : $S_1 = L_1 \circ S_2 \circ L_2$. We will also say that two permutations are affine equivalent if there exist two affine permutations A_1 and A_2 : $S_1 = A_1 \circ S_2 \circ A_2$.

3. Possible constructions

In this paper we study the butterfly structure that has been introduced in [4].

Definition 6. Let $n = 2m$. We will call function $F : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$ with input $x_i \| y_i$ and output $x_o \| y_o$ ($x_i, y_i, x_o, y_o \in \mathbb{F}_{2^m}$) a generalized butterfly structure if there exist two functions

$$F_1, F_2 : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \mapsto \mathbb{F}_{2^m}$$

such that:

- y_o depends on x_i, y_i according to the equation $y_o = F_1(x_i, y_i)$,
- y_i depends on x_o, y_o according to the equation $y_i = F_2(x_o, y_o)$.

When $F_1 = F_2$ function F is a butterfly structure presented in [4].

Proposition 1. *A generalized butterfly structure F is a permutation if and only if for every fixed value $y \in \mathbb{F}_{2^m}$ functions $F_1(x, y)$ and $F_2(x, y)$ are permutations.*

Proof. Let F be a permutation and $y \in \mathbb{F}_{2^m}$. Without loss of generality we'll prove it for function F_1 which defines the least significant bits of the output. If F_1 is not a permutation for a fixed value y, then there exist x_1 and x_2 such that

$$F_1(x_1, y) = F_1(x_2, y)$$

and

$$\# \{y_o \,|y_o = F_1(x, y),\ x \in \mathbb{F}_{2^m}\} \leqslant 2^m - 1,$$

and this is a contradiction with the statement that F is a permutation.

If F_i, $i \in \{1, 2\}$, are permutations, then there exists only one pair x_o, y_o for every x_i and y_i. $\square$

In [4] there was revealed that only one known 6-bit APN permutation is CCZ equivalent to the so-called non bijective butterfly structure and that in our terms F_1, F_2 are bent functions. We want to construct a permutation with good cryptographic properties that were mentioned in section 2. In contrast with [5] we will focus on the nonlinearity because we can choose F_1 and F_2 separately and independently.

In this paper we will consider the case $m = 4$. The core idea of this paper is as follows:

- Choose functions F_1, F_2 that correspond to Proposition 1.
- These functions may be based on Maiorana–McFarland construction and [16]:

$$F'_i(x,y) = \begin{cases} \pi_i(x) \cdot l_i(y) + f_i(x), & l_i(y) \neq 0, \\ \widehat{\pi}_i(x), & l_i(y) = 0, \end{cases} \tag{1}$$

$$F''_i(x,y) = \begin{cases} \pi_i(y) \cdot l_i(x) + f_i(y), & \pi_i(y) \neq 0, \\ \widehat{\pi}_i(x), & \pi_i(y) = 0, \end{cases} \tag{2}$$

  where $\pi_i, \widehat{\pi}_i$ are m-bit permutations, l_i is an m-bit linear permutation and f_i is an m-bit function.

- Make a generalized butterfly structure F based on F_1 and F_2 and evaluate its cryptographic properties.

3.1. Construction based on F' function

Proposition 2. *The function $F'_i(x,y)$ from equation* (1) *is a bijective function for any fixed value y if and only if $f(x)$ is a constant function.*

Proof. If $l_i(y)$ is equal to 0 then $F'_i(x,y) = \widehat{\pi}_i(x)$ and is a permutation.

If $l_i(y)$ is not equal to 0, then we consider the function $\pi_i(x) \cdot l_i(y) + f_i(x)$. This function is a permutation for a fixed value y if there are no $x_1, x_2 \in \mathbb{F}_{2^m}$ such that

$$\pi_i(x_1) \cdot l_i(y) + f_i(x_1) = \pi_i(x_2) \cdot l_i(y) + f_i(x_2).$$

Let us consider the following equations:

$$\pi_i(x_1) \cdot l_i(y) + f_i(x_1) \neq \pi_i(x_2) \cdot l_i(y) + f_i(x_2) \Leftrightarrow \\ \Leftrightarrow (\pi_i(x_1) + \pi_i(x_2))\, l_i(y) \neq (f_i(x_1) + f_i(x_2)). \tag{3}$$

Only a constant function $f_i(x)$ could satisfy equation (3) for every pair $x_1, x_2 \in \mathbb{F}_{2^m}$ because the set $\{(\pi_i(x_1) + \pi_i(x_2))\, l_i(y)\, | y \in \mathbb{F}_{2^m}\}$ is equal to the set of all nonzero elements of a finite field $\mathbb{F}_{2^m}$. □

There is another possible construction:

$$\widehat{F_i'}(x,y)=\begin{cases}\pi_i(x)\cdot l_i(y)+a\cdot\pi(x), & (l_i(y)+a)\neq 0,\\ \widehat{\pi}_i(x), & (l_i(y)+a)=0,\end{cases} \tag{4}$$

where $a\in\mathbb{F}_{2^m}$. It is obvious that equations (1) and (4) provide affine equivalent constructions. Moreover they provide constructions affine equivalent to the following one:

$$F_i'(x,y)=\begin{cases}\pi_i(x)\cdot y, & y\neq 0,\\ \widehat{\pi}_i(x), & y=0.\end{cases} \tag{5}$$

Let us denote

$$x\otimes_i y=\begin{cases}\pi_i(x)\cdot y, & y\neq 0,\\ \widehat{\pi}_i'(x), & y=0.\end{cases} \tag{6}$$

We will use new $\otimes_i$ operation [1] to represent the construction on the Fig. 1.We will call this construction "A".

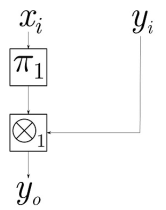

Fig. 1. Construction "A"

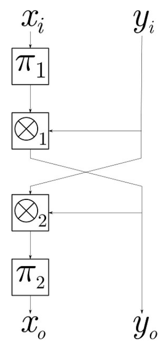

Fig. 2. Permutation based on two "A" constructions

The following proposition tells us that at least a part of all WHT of S-Box based on selected construction will have a good nonlinearity.

Proposition 3. *For all* $\alpha,\beta,\gamma\in\mathbb{F}_{2^m}$ *:*

$$\left|W_{F_i'(x,y)}(\alpha\,\|\,\beta,\gamma)\right|\leqslant\left|W_{\pi_i(x)\cdot y}(\alpha\,\|\,\beta,\gamma)\right|+2^m.$$

[1] The permutation $\widehat{\pi}_i'(x)$ in the equation (6) is different from $\widehat{\pi}_i(x)$ in the equation (5) only for construction "A" . For this construction $\widehat{\pi}_i'(x)=\widehat{\pi}_i\left(\pi^{-1}(x)\right)$. For other constructions $\widehat{\pi}_i'(x)=\widehat{\pi}_i(x)$.

Proof. We have

$$\left|W_{F_i'(x,y)}(\alpha\,\|\,\beta,\gamma)\right| = \left|\sum_{x,y\in\mathbb{F}_{2^m}}(-1)^{\langle\alpha,x\rangle+\langle\beta,y\rangle+\langle\gamma,F_i'(x,y)\rangle}\right| =$$

$$= \left|\sum_{x,y\in\mathbb{F}_{2^m},y\neq 0}(-1)^{\langle\alpha,x\rangle+\langle\beta,y\rangle+\langle\gamma,\pi_i(x)\cdot y\rangle} + \sum_{x\in\mathbb{F}_{2^m}}(-1)^{\langle\alpha,x\rangle+\langle\gamma,\widehat{\pi}_i(x)\rangle}\right| =$$

$$= \left|\sum_{x,y\in\mathbb{F}_{2^m},y\neq 0}(-1)^{\langle\alpha,x\rangle+\langle\beta,y\rangle+\langle\gamma,\pi_i(x)\cdot y\rangle} \pm \sum_{x\in\mathbb{F}_{2^m}}(-1)^{\langle\alpha,x\rangle} + \sum_{x\in\mathbb{F}_{2^m}}(-1)^{\langle\alpha,x\rangle+\langle\gamma,\widehat{\pi}_i(x)\rangle}\right| \leqslant$$

$$\leqslant \left|W_{\pi_i(x)\cdot y}\right| + \left|-\sum_{x\in\mathbb{F}_{2^m}}(-1)^{\langle\alpha,x\rangle} + \sum_{x\in\mathbb{F}_{2^m}}(-1)^{\langle\alpha,x\rangle+\langle\gamma,\widehat{\pi}_i(x)\rangle}\right|.$$

If $\alpha \neq 0$, then the last summand is equal to $\left|W_{\widehat{\pi}_i(\alpha,\gamma)}\right| \leqslant 2^{m-1}$. If $\alpha = 0$, $\gamma \neq 0$, then

$$\left|-\sum_{x\in\mathbb{F}_{2^m}}(-1)^{\langle\alpha,x\rangle} + \sum_{x\in\mathbb{F}_{2^m}}(-1)^{\langle\gamma,\widehat{\pi}_i(x)\rangle}\right| = 2^m,$$

because $\#\{x\,|\langle\gamma,\widehat{\pi}_i(x)\rangle = 0\} = 2^{m-1}$. If $\alpha = 0$, $\gamma = 0$, then

$$\left|-\sum_{x\in\mathbb{F}_{2^m}}(-1)^{\langle\alpha,x\rangle} + \sum_{x\in\mathbb{F}_{2^m}}(-1)^{\langle\gamma,\widehat{\pi}_i(x)\rangle}\right| = 0.$$

The function $\pi_i(x)\cdot y$ is a bent one, so $\left|W_{\pi_i(x)\cdot y}\right| = 2^{m-1}$. □

Let us make a butterfly permutation based on the following construction (see Fig. 2):

$$y_o = \begin{cases}\pi_1(x_i)\cdot y_i, & y_i \neq 0,\\ \widehat{\pi}_1(x_i), & y_i = 0,\end{cases} \tag{7}$$

$$x_o = \begin{cases}\pi_2(y_i\cdot y_o), & y_o \neq 0,\\ \widehat{\pi}_2(y_i), & y_o = 0.\end{cases} \tag{8}$$

To make evaluations easier we suppose that π_1, π_2 are some monomial permutations of $\mathbb{F}_{2^m}$ from the set

$$z^1, z^2, z^4, z^7, z^8, z^{11}, z^{13}, z^{14}.$$

We have implemented this construction (presented in Fig. 2) and have used a simple version of an evolutionary algorithm [17] to execute a search among all permutations $\widehat{\pi}_1$, $\widehat{\pi}_2$ for all possible fixed monomial permutations π_1, π_2. Let us list some results that we have obtained.

1. We found 32 constructions that provide the way to construct permutations with semi-optimal cryptographic properties:
   - the nonlinearity is equal to 108,
   - the differential uniformity is equal to 6,
   - the algebraic degree is equal to 7.
2. In these constructions $\pi_1(x)$ is any monomial function, $\pi_2(x) = x^\alpha$, $\alpha \in \{7, 11, 13, 14\}$.
3. For other pairs $\pi_1(x)$ and $\pi_2(x)$ permutations have the differential uniformity larger than 12.
4. These properties may be obtained with equal permutations $\widehat{\pi}_1(x)$, $\widehat{\pi}_2(x)$; note that semi-optimal cryptographic properties are obtained for all proposed constructions with $\widehat{\pi}_1(x) = \widehat{\pi}_2(x) = x^{-1}$.
5. These properties may be obtained for $\widehat{\pi}_1(x) \neq \widehat{\pi}_2(x)$.
6. Semi-optimal cryptographic properties may be obtained even for non monomial permutation $\pi_1(x)$ and $\pi_2(x)$. Let $\mathbb{F}_{2^{2m}} = \mathbb{F}_2(x)/\,(x^4 + x + 1)$. An example of such a permutation is:

$$\begin{aligned}
\widehat{\pi}_1 = \widehat{\pi}_2 &= \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 0 & 9 & 10 & 15 & 3 & 11 & 13 & 4 & 2 & 6 & 14 & 12 & 1 & 7 & 8 & 5 \end{pmatrix}, \\
\pi_1 &= \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 0 & 8 & 9 & 1 & 13 & 5 & 4 & 12 & 7 & 15 & 14 & 6 & 10 & 2 & 3 & 11 \end{pmatrix}, \\
\pi_2 &= \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 0 & 14 & 11 & 4 & 2 & 3 & 15 & 1 & 10 & 8 & 12 & 7 & 13 & 9 & 6 & 5 \end{pmatrix}.
\end{aligned}$$

3.2. Construction based on F'' function

Let us consider $F_i''(x,y)$ function. Three constructions could be implemented with such function (see Figs. 3–5). These constructions have absolutely the same output function $y_o = F_1''(x_i, y_i)$, but constructions "C" and "D" change y_i correspondingly by permutation π_1 and by composition of permutations π_1 and π_{f1}. Actually, constructions "C" and "D" are not even possible functions for generalized butterfly construction because in term of our definition y_i is an output of $F_2''(x,y)$ and it can't be changed by $F_1''(x,y)$.

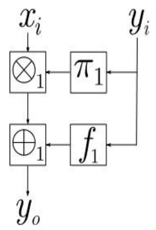

Fig. 3. Construction "B"

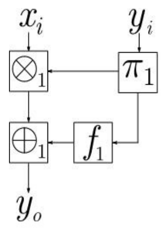

Fig. 4. Construction "C"

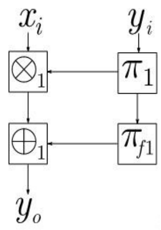

Fig. 5. Construction "D"

At the same time all these constructions are bijective for any fixed value y and for any function f_i. And output functions have the same nonlinearity as construction "A".

In this work we will study permutation based on two "B" constructions with $f_i = 0$ (see Fig. 6). In this construction $y_o = x_i \otimes_1 \pi_1(y_i)$ and $x_o = y_i \otimes_2 \pi_2\left(x_i \otimes_1 \pi_1(y_i)\right)$. If both $\pi_1(y_i)$ and $\pi_2(y_0)$ are not equal to 0, then $x_o = y_i \cdot \pi_2\left(x_i \cdot \pi_1(y_i)\right)$. We suppose that $\pi_2(x)$ is linear equivalent to x^α and $\pi_1(x)$ is linear equivalent to x^β, so x_o is linear equivalent to $x_i^\alpha \cdot y_i^{\alpha\beta+1}$.

We've implemented this construction and have used an evolutionary algorithm to execute a search among all permutations $\widehat{\pi}_1$, $\widehat{\pi}_2$ for all fixed monomial permutations π_1, π_2. We found four possible constructions with semi-optimal cryptographic properties:

1. $\pi_1(x) = x$, $\pi_2(x) = x^{13}$,
2. $\pi_1(x) = x^2$, $\pi_2(x) = x^{14}$,
3. $\pi_1(x) = x^4$, $\pi_2(x) = x^7$,
4. $\pi_1(x) = x^8$, $\pi_2(x) = x^{11}$.

Constructions 2 and 4 are inverse permutations for corresponding 1 and 3 constructions.

4. Comparison with other constructions

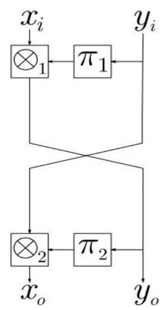

Fig. 6. Permutation based on two “B” constructions

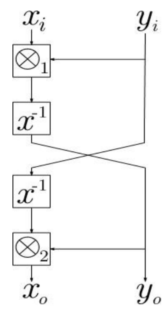

Fig. 7. Permutation from [18]

In [18] the following construction was presented (see Fig. 7) (in terms of our work):

$$x_o = \begin{cases} (x_i \cdot y_i)^{-1}, & y_i \neq 0, \\ \widehat{\pi}_1(x_i), & y_i = 0, \end{cases} \qquad y_o = \begin{cases} x_o \cdot y_i^{-1}, & x_o \neq 0, \\ \widehat{\pi}_2(x_i), & x_o = 0. \end{cases}$$

Permutations with following properties were also found in [18]:

- the nonlinearity is equal to 108,
- the differential uniformity is equal to 6,
- the algebraic degree is equal to 7.

Except these properties two additional one were considered in the work:

- absence of fixed points,
- maximum graph algebraic immunity.

Our construction based on two “A” constructions with $\pi_1(x) = \pi_2(x) = x^{-1}$ looks similar with construction presented in [18] (see Fig. 2 and Fig. 7) but was found independently. There were no theoretical foundation and principles of choosing this particular construction in [18] and we have no chance to compare it with one presented in our work. At the same time it was shown in [18] that the value of graph algebraic immunity of a constructed permutation depends on permutations $\widehat{\pi}_i$ and that for $\widehat{\pi}_i(x) = x^{-1}$ the permutation has almost optimal cryptographic properties except the value of graph algebraic immunity. We have found that for some our constructions with $\widehat{\pi}_i(x) = x^{-1}$ the value of graph algebraic immunity is equal to 2. But permutation $\widehat{\pi}_i(x)$ choosed by means of our search algorithm doesn’t have simple algebraic structure and this permutation has cryptographic properties like in [18], where it was also stressed that permutations with such properties have almost optimal cryptographic characteristics. Comparison with other results could also be found in [18].

We've generalized that construction on Fig. 7 and replace x^{-1} by monomial functions π_1 and π_2. We have searched among permutations $\widehat{\pi}_1$, $\widehat{\pi}_2$ for all fixed monomial permutations π_1, π_2 and found the following:

- for the following 12 constructions almost optimal cryptographic properties are obtained:
$$(\pi_1,\pi_2) \in \big\{(x^7,x),(x^7,x^4),(x^7,x^7),(x^{11},x^2),(x^{11},x^8),(x^{11},x^{11}), (x^{13},x),(x^{13},x^4),(x^{13},x^{13}),(x^{14},x^2),(x^{14},x^8),(x^{14},x^{14})\big\},$$
- for 4 constructions the differential uniformity is up to 8 and the nonlinearity is up to 104:
$$(\pi_1,\pi_2) \in \big\{(x^7,x^2),(x^{11},x),(x^{13},x^8),(x^{14},x^4)\big\},$$
- for 8 constructions the differential uniformity is up to 8 and the nonlinearity is up to 100:
$$(\pi_1,\pi_2) \in \big\{(x^7,x^{11}),(x^7,x^{14}),(x^{11},x^7),(x^{11},x^{13}),(x^{13},x^{11}),(x^{13},x^{14}), (x^{14},x^7),(x^{14},x^{13})\big\}.$$

5. Future work

In this paper we have presented several new classes of constructions that may be used to find permutations with rather good cryptographic properties. But at the same time there remains a lot of questions that should be solved. Among them:

- How many possibilities there exist to choose F_1 and F_2 to construct a permutation with good cryptographic properties?
- How many possibilities there exist to choose π_i and f_i in all these constructions?
- Can we choose permutations $\widehat{\pi}_i$ for our constructions to obtain good cryptographic properties without a search algorithm?
- Can we find a construction that will be an involution?
- Can we use mixed construction for butterfly structure (as example permutation based on "A" and "B" constructions) to find a permutation with rather good cryptographic properties?
- How to find permutations with good hardware, FPGA or bit-sliced implementations?

6. Conclusion

In this paper some new constructions of permutation $\mathbb{F}_{2^{2m}} \mapsto \mathbb{F}_{2^{2m}}$, $m = 4$, based on butterfly structure are suggested. There are at least 36 new constructions for permutations that have the nonlinearity 108, differential uniformity 6, algebraic degree 7 and the value of graph algebraic immunity 3.

References

[1] Shannon C., “Communication theory of secrecy systems”, *Bell Syst. Techn. J.*, **28** (1949), 656–715.

[2] Boss E., Grosso V., Gëneysu T., Leander G., Moradi A., Schneider T., “Strong 8-bit s-boxes with efficient masking in hardware extended version”, *J. Cryptogr. Eng.*, **7**:2 (2017), 149–165.

[3] Kutzner S., Nguyen P., Poschmann A., “Enabling 3-share threshold implementations for all 4-bit s-boxes”, ICISC 2013, Lect. Notes Comput. Sci., **8565**, 2013, 91–108.

[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] Canteaut A., Duval S., Leurent G., “Construction of lightweight s-boxes using Feistel and MISTY structures (full version)”, Cryptology ePrint Archive. Report 2015/711, http://eprint.iacr.org/2015/711.

[6] Lim C. H., “CRYPTON: A new 128-bit Block Cipher – Specification and Analysis” (1998), http://citeseerx.ist.psu.edu/.

[7] 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.

[8] Matsui M., “New block encryption algorithm MISTY”, FSE 1997, Lect. Notes Comput. Sci., **1267**, 1997, 54–68.

[9] Grosso V., Leurent G., Standaert F.-X., Varici K., “Ls-designs: Bitslice encryption for efficient masked software implementations”, FSE 2014, Lect. Notes Comput. Sci., **8540**, 2014, 18–37.

[10] Standaert F.-X., Piret G., Rouvroy G., Quisquater J.-J., Legat J.-D., “ICEBERG: An involutional cipher efficient for block encryption in reconfigurable hardware”, FSE 2004, Lect. Notes Comput. Sci., **3017**, 2004, 279–299.

[11] Rijmen V., Barreto P., “The KHAZAD legacy-level block cipher”, Primitive submitted to NESSIE 97 (2000).

[12] Lim C. H., “A revised version of Crypton – Crypton v1.0”, FSE’99, Lect. Notes Comput. Sci., **1636**, 1999, 31–45.

[13] Stallings W., “The Whirlpool secure hash function”, *Cryptologia*, **30**:1 (2006), 55–67.

[14] Browning K. A., Dillon J. F., McQuistan M. T., Wolfe A. J., “An APN permutation in dimension six”, 9th Int. Conf. Finite Fields Appl. 2009, Contemp. Math., **518**, 2010, 33–42.

[15] McFarland R. L., “A family of difference sets in non-cyclic groups”, *J. Comb. Theory, Ser. A*, **15**:1 (1973), 1–10.

[16] Dobbertin H., “Construction of bent functions and balanced boolean functions with high nonlinearity”, FSE 1994, Lect. Notes Comput. Sci., **1008**, 1994, 61–74.

[17] Olariu S., Zomaya A. Y., *Handbook of Bioinspired Algorithms and Applications*, Boca Raton, FL: Chapman and Hall/CRC, 2005.

[18] 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”, www.cs.haifa.ac.il/orrd/LC17/paper60.pdf.