МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2022 Т. 13 № 2 С. 37–52

УДК 519.719.2 DOI https://doi.org/10.4213/mvk407

On differential uniformity of permutations derived using a generalized construction

D. B. Fomin, M. A. Kovrizhnykh

National Research University "Higher School of Economics", *Moscow*

Получено 10.XI.2021

Abstract. The work is dedicated to the theoretical substantiation of a directed search for 8-bit permutations with given cryptographic properties: differential uniformity and nonlinearity. The statements on the partition of the set of vectorial Boolean functions derived using generalized construction into equivalence classes are proved. The statements that allow one to reject functions from equivalence classes either by a high differential uniformity or by nonbijectivity are justified. The results of this work may be used to construct permutations with specified cryptographic properties, ensuring the resistance of encryption algorithms against the linear and differential methods of cryptographic analysis.

Keywords: vectorial Boolean function, permutation, differential uniformity

О дифференциальной равномерности подстановок, построенных с использованием обобщенной конструкции

Д. Б. Фомин, М. А. Коврижных

Национальный исследовательский университет «Высшая школа экономики», *Москва*

Аннотация. Работа посвящена теоретическому обоснованию направленного поиска 8-битовых подстановок с заданными криптографическими характеристиками: дифференциальной δ-равномерностью и нелинейностью. Сформулированы и доказаны утверждения о разбиении на классы эквивалентности множества векторных булевых функций, построенных с помощью обобщенной конструкции. Обоснованы утверждения, позволяющие отбраковывать функции из классов эквивалентности либо по высокому показателю дифференциальной δ-равномерности, либо вследствие того, что они не являются подстановками. Результаты работы могут быть использованы для конструирования подстановок с заданными криптографическими свойствами, обеспечивающими стойкость алгоритмов шифрования к линейному и разностному методам криптографического анализа.

Citation: Matematicheskie Voprosy Kriptografii, 2022, v. 13, № 2, pp. 37–52 (Russian)

Ключевые слова: векторная булева функция, подстановка, дифференциальная δ-равномерность

Introduction

Vectorial Boolean functions (S-boxes) are among the main primitives of modern symmetric ciphers that provide Shannon's confusion principle [1]. S-boxes must have cryptographic properties that guarantee the impossibility of using differential and linear methods of cryptographic analysis. Thus, S-boxes with high nonlinearity can ensure the cipher resistance to linear cryptographic analysis, since they can not be effectively replaced by a linear analog of the same or less dimension. Moreover, S-boxes with the minimum possible differential uniformity are used for constructing cryptographic algorithms that are resistant to differential analysis.

Construction of n-bits permutations with given cryptographic properties for $n \geqslant 8$ is a difficult and urgent problem; this is confirmed by a large number of scientific publications and reports at all-Russian and international cryptographic conferences (e.g. [2–10]). The known approaches to constructing permutations may be divided into explicit algebraic methods, pseudo-random generation, and heuristic algorithms (see, e.g., an overview in [2]).

The idea of a combination of the above approaches seems promising, in particular, the use of functional circuits to derive permutations using functions of lower dimension (see, e.g., an overview in [9]). Moreover, such schemes usually have some parameters which may be used to optimize the cryptographic properties of constructed permutations.

Thus, in [4] a new construction of 8-bit S-boxes with nonlinearity up to 108, differential uniformity 6 or 8, algebraic degree 7, and algebraic immunity 3 was proposed. It uses the inversion in the field $\mathbb{F}_{2^4}$ and two arbitrary permutations of the space V_4.

In [5, 6] new schemes based on the well-known Feistel and Lai – Massey structures for generating permutations of dimension $n = 2k$, $k > 2$, are presented. The proposed constructions use inversion in the field $\mathbb{F}_{2^k}$, an arbitrary k-bit non-bijective function (which has no pre-image for 0), and any k-bit permutation. New 8-bit permutations without fixed points, which have the same strong combination of cryptographic properties as in [4] are introduced.

In [7] new classes of 8-bit permutations based on the butterfly structure were proposed. It was shown that there are at least 36 new constructions for permutations that have the nonlinearity 108, differential uniformity 6, algebraic degree 7, and graph algebraic immunity 3.

The papers [9, 10] extend the methods of constructing permutations from [7] to the case of an arbitrary vector space V_{2m} and theoretically substantiate the experimental results obtained in [7]. TU-decomposition described in [11, 12] is used as a functional circuit. Necessary and, in some cases, sufficient conditions for the resulting permutation to have given nonlinearity, algebraic degree, and differential uniformity are proved. Also, new generalized construction of vector functions is described. It utilizes monomial permutations as the basic constituent elements. In the case $m = 4$, 768 tuples of parameters of the generalized construction were experimentally found, using which, with the correct choice of auxiliary 4-bit permutations, 8-bit permutations with nonlinearity 108, differential uniformity 6, and algebraic degree 7 may be obtained.

The purpose of this paper is the theoretical substantiation of a directed search for 8-bit permutations with given cryptographic properties: differential uniformity and nonlinearity, among vectorial Boolean functions obtained using a generalized construction that admits TU-decomposition.

This paper is structured as follows. Section 1 contains the main definitions and notations used in the work. In Section 2 we consider a generalized construction of $(2m, 2m)$-function and show that this construction admits TU-decomposition. In Section 3 we introduce an equivalence relation on the set of all vector Boolean functions defined by generalized construction. Each equivalence class is determined by a tuple of exponents of monomial permutations. In Section 4, we prove several statements that allow us to reject the equivalence classes of 8-bit S-boxes that do not contain permutations with a low differential uniformity. Non-rejected classes may be used to generate 6-uniform 8-bit permutations with nonlinearity equal to 108.

1. Definitions and Notation

Let V_n be n-dimensional vector space over the field of two elements $\mathbb{F}_2$, $V_n^\times = V_n \setminus \{0\}$. The finite field of 2^n elements is denoted by $\mathbb{F}_{2^n}$, where $\mathbb{F}_{2^n} = \mathbb{F}_2[x]/g(x)$, $g(x)$ is an irreducible polynomial of degree n over the field $\mathbb{F}_2$. We denote by $\mathbb{Z}/2^n$ the ring of the integers modulo 2^n. There is a bijective mapping $\mathbb{Z}/2^n \to V_n$ that associates an element of the ring $\mathbb{Z}/2^n$ with its binary representation, and a bijective mapping $V_n \to \mathbb{F}_{2^n}$ that assigns a binary string to an element of the field $\mathbb{F}_{2^n}$. The operations of addition and multiplication in the field $\mathbb{F}_{2^n}$ are denoted by the signs “$+$” and “$\cdot$”, respectively.

It is well known [13] that there are only three irreducible polynomials of degree 4 over the field $\mathbb{F}_2$. For definiteness, we will further work in the field $\mathbb{F}_{2^4} = \mathbb{F}_2[x]/x^4 + x + 1$.

Concatenation of the vectors $a \in V_n$, $b \in V_m$ is denoted by $a\|b \in V_{n+m}$. The *dot product* of two vectors $a, b \in V_n$ is an element of the field $\mathbb{F}_2$ calculated by the formula $\langle a, b\rangle = a_{n-1}b_{n-1} + \ldots + a_0b_0$, where addition and multiplication are carried out in the field $\mathbb{F}_2$. Note that the direct product of vector spaces $V_m \times V_m$ may be associated with V_{2m}.

Definition 1. The vectorial Boolean (n, m)-function is a mapping $V_n \to V_m$. Permutation over V_n is a bijective (n, n)-function.

The symmetric group of all permutations of the space V_n is denoted by $S(V_n)$.

Monomial permutations of the field $\mathbb{F}_{2^m}$ are permutations of the form x^d, where d is a positive integer such that $\gcd(d, 2^m - 1) = 1$. In this case, only the values $d < 2^m - 1$ may be considered. In particular, for $m = 4$, monomial permutations are obtained for $d \in \{1, 2, 4, 7, 8, 11, 13, 14\}$. Moreover, linear monomial permutations of the field $\mathbb{F}_{2^4}$ are x^d for $d \in \{1, 2, 4, 8\}$ [13].

Definition 2. Let F be (n, m)-function, $1 \leqslant t \leqslant \min(n, m)$, $x_1, y_1 \in V_t$, $x_2 \in V_{n-t}$, $y_2 \in V_{m-t}$, $x = x_1\|x_2$, and $y = y_1\|y_2$. Let $T(x_1, x_2)$ be (n, t)-function such that when fixing an arbitrary x_2 the function T be a bijection with respect to the variable x_1, and U be $(n, m - t)$-function. Then if the function F may represented as

$$F(x) = F(x_1\|x_2) = (T(x_1, x_2), U(x_2, T(x_1, x_2))), \tag{1}$$

then such a representation of the function F will be called TU-decomposition [12].

Definition 3. The differential uniformity of (n, m)-function F is defined as

$$\delta_F = \max_{a \in V_n^{\times}, b \in V_m} \delta_F(a, b),$$

where $\delta_F(a, b) = |\{x \in V_n \mid F(x + a) + F(x) = b\}|$.

The use of functions with a lower differential uniformity in the synthesis of cryptographic algorithms makes it possible to guarantee resistance against the differential method of cryptographic analysis. For vectorial (n, n)-functions, the smallest value of δ_F is equal to 2. For even n, only one example (up to CCZ-equivalence) of a one-to-one 2-uniform function is known so far — the Dillon 6-bit permutation [14]. We can assume that $\delta_F > 8$ is a large value of the differential uniformity for the case $n = 8$ since 8-bit permutation with $\delta_F = 8$ may be obtained by pseudo-random search [2, 15, 16].

2. Generalized construction of $(2m, 2m)$-functions

Let $(2m, 2m)$-function $F(x_1, x_2) = y_1 \| y_2$, where $x_1, x_2, y_1, y_2 \in V_m$, be given by the following *generalized construction*, first introduced in [8],

$$\begin{aligned} y_1 = G_1(x_1, x_2) &= \begin{cases} x_1^{\alpha} \cdot x_2^{\beta}, & x_2 \neq 0, \\ \widehat{\pi}_1(x_1), & x_2 = 0, \end{cases} \\ y_2 = G_2(x_1, x_2) &= \begin{cases} x_1^{\gamma} \cdot x_2^{\delta}, & x_1 \neq 0, \\ \widehat{\pi}_2(x_2), & x_1 = 0. \end{cases} \end{aligned} \tag{2}$$

Hereinafter, one should pass from vectors of the space V_m to the corresponding elements of the field $\mathbb{F}_{2^m}$ and perform exponentiation and multiplication in the field $\mathbb{F}_{2^m}$. Moreover, in (2), $\widehat{\pi}_1$, $\widehat{\pi}_2$ are permutations over V_m. Without loss of generality, we assume that the following equalities hold

$$\widehat{\pi}_1(0) = 0, \quad \widehat{\pi}_2(0) = 0. \tag{3}$$

The parameters of the function (2) are permutations $\widehat{\pi}_1$, $\widehat{\pi}_2$ and the tuple of indexes $(\alpha, \beta, \gamma, \delta)$ of monomial permutations.

For the system (2) to specify a bijective mapping under the condition (3) it is sufficient that the system

$$\begin{cases} G_1(x_1, x_2) &= b_1, \\ G_2(x_1, x_2) &= b_2, \end{cases}$$

has solutions for arbitrary $b_1, b_2 \in V_m$.

Statement 1. *The construction* (2) *admits the TU-decomposition* (1).

Proof. Indeed, put $T(x_1, x_2) = G_1(x_1, x_2)$, note that for a fixed arbitrary x_2 the function T is a bijection with respect to the variable x_1, then

$$U(x_2, T(x_1, x_2)) = \begin{cases} (T(x_1, x_2))^{\lambda} \cdot x_2^{\mu}, & x_2 \neq 0,\ x_1 \neq 0, \\ \widehat{\pi}_2(x_2), & x_1 = 0, \\ 0, & x_2 = 0, \end{cases}$$

where $\alpha\lambda = \gamma \bmod (2^m - 1)$, $\mu = \delta - \beta\lambda \bmod (2^m - 1)$. □

Note that the GOST 34.12-2018 (Kuznyechik) permutation and the only known (up to CCZ-equivalence) 2-uniform permutation of the space V_n for even n also allow the TU-decomposition. The study of constructions that allow the TU-decomposition seems to be important.

3. On equivalence of functions derived using a generalized construction

In this section, we propose the principle of partitioning the set of functions derived using a generalized construction into disjoint equivalence classes. The corresponding statement is proved. It is shown how to obtain the entire equivalence class from one of its representatives.

Let us state a lemma [10, Lemma 1] for the case of functions that are obtained using the construction (2).

Lemma 1. *Let $(2m, 2m)$-function F be obtained using the construction (2), and $a_1, a_2, b_1, b_2 \in V_m$, then $\delta_F(a_1\|a_2, b_1\|b_2)$ is larger than or equal to the number of solutions to the system of equations*

$$\begin{cases} (x_1+a_1)^\alpha \cdot (x_2+a_2)^\beta + x_1^\alpha \cdot x_2^\beta &= b_1, \\ (x_1+a_1)^\gamma \cdot (x_2+a_2)^\delta + x_1^\gamma \cdot x_2^\delta &= b_2, \end{cases} \tag{4}$$

with the following constraints on the values of the variables x_1 and x_2:

$$x_1 \neq 0, \quad x_2 \neq 0, \quad x_1 \neq a_1, \quad x_2 \neq a_2. \tag{5}$$

Proof of the lemma is obvious since under the constraints (5) the equations defining the function have the form (4). □

The following statement is a generalization of the corresponding statement from [10].

Statement 2. *Let us consider the system (4) under constraints (5) with a tuple of parameters $(\alpha, \beta, \gamma, \delta)$, where x^α, x^β, x^γ, and x^δ define monomial permutations over the field $\mathbb{F}_{2^m}$. Let also the maximal number of its solutions (x_1, x_2), $x_1, x_2 \in \mathbb{F}_{2^m}$, for $a_1, a_2, b_1, b_2 \in \mathbb{F}_{2^m}$, where a_1 and a_2 do not vanish simultaneously, be known.*

Then the systems obtained from (4) by changing the parameters to

$$(\alpha \cdot d_1,\ \beta \cdot d_1,\ \gamma \cdot d_2,\ \delta \cdot d_2) \bmod (2^m-1), \quad \textit{or to}$$

$$(\alpha \cdot d_1,\ \beta \cdot d_2,\ \gamma \cdot d_1,\ \delta \cdot d_2) \bmod (2^m-1), \quad \textit{or to}$$

$$(\gamma,\ \delta,\ \alpha,\ \beta), \quad \textit{or to} \quad (\beta,\ \alpha,\ \delta,\ \gamma), \quad \textit{or to} \quad (\delta,\ \gamma,\ \beta,\ \alpha),$$

where the mappings x^{d_1} and x^{d_2} define linear permutations over the field $\mathbb{F}_{2^m}$, have the same maximal number of solutions satisfying the conditions (5)*.*

Proof. Let us consider the system

$$\begin{cases} (x_1+a_1)^{d_1\cdot\alpha}\cdot(x_2+a_2)^{d_1\cdot\beta}+x_1^{d_1\cdot\alpha}\cdot x_2^{d_1\cdot\beta} & = & b_1^{d_1}, \\ (x_1+a_1)^{d_2\cdot\gamma}\cdot(x_2+a_2)^{d_2\cdot\delta}+x_1^{d_2\cdot\gamma}\cdot x_2^{d_2\cdot\delta} & = & b_2^{d_2}, \end{cases} \tag{6}$$

where $a_1, a_2, b_1, b_2 \in \mathbb{F}_{2^m}$ and a_1, a_2 do not vanish simultaneously. Note that, because of x^{d_1} and x^{d_2} are the bijective mappings, if b_1 and b_2 take all values from the field $\mathbb{F}_{2^m}$, then $b_1^{d_1}$, $b_2^{d_2}$ also take all values from this field. Taking into account the linearity of the mappings x^{d_1} and x^{d_2}, we write the system (6) in the form

$$\begin{cases} ((x_1+a_1)^{\alpha}\cdot(x_2+a_2)^{\beta}+x_1^{\alpha}\cdot x_2^{\beta})^{d_1} & = & b_1^{d_1}, \\ ((x_1+a_1)^{\gamma}\cdot(x_2+a_2)^{\delta}+x_1^{\gamma}\cdot x_2^{\delta})^{d_2} & = & b_2^{d_2}. \end{cases}$$

Again, due to the bijectivity of the functions x^{d_1} and x^{d_2}, this system is equivalent to the system (4). Thus, a system with a tuple of parameters $(\alpha\cdot d_1,\ \beta\cdot d_1,\ \gamma\cdot d_2,\ \delta\cdot d_2) \bmod (2^m-1)$ has the maximal number of solutions that satisfy the conditions (5), which coincides with the maximal number of solutions of the system (4).

Further, consider the system

$$\begin{cases} (x_1+a_1)^{d_1\cdot\alpha}\cdot(x_2+a_2)^{d_2\cdot\beta}+x_1^{d_1\cdot\alpha}\cdot x_2^{d_2\cdot\beta} & = & b_1, \\ (x_1+a_1)^{d_1\cdot\gamma}\cdot(x_2+a_2)^{d_2\cdot\delta}+x_1^{d_1\cdot\gamma}\cdot x_2^{d_2\cdot\delta} & = & b_2, \end{cases} \tag{7}$$

where $a_1, a_2, b_1, b_2 \in \mathbb{F}_{2^m}$ and a_1, a_2 do not vanish simultaneously. Taking into account the linearity of the mappings x^{d_1} and x^{d_2}, we write the system (7) in the form

$$\begin{cases} (x_1^{d_1}+a_1^{d_1})^{\alpha}\cdot(x_2^{d_2}+a_2^{d_2})^{\beta}+(x_1^{d_1})^{\alpha}\cdot(x_2^{d_2})^{\beta} & = & b_1, \\ (x_1^{d_1}+a_1^{d_1})^{\gamma}\cdot(x_2^{d_2}+a_2^{d_2})^{\delta}+(x_1^{d_1})^{\gamma}\cdot(x_2^{d_2})^{\delta} & = & b_2. \end{cases}$$

Making the replacement $x_1^{d_1}=y_1$, $x_2^{d_2}=y_2$, $a_1^{d_1}=\overline{a}_1$, and $a_2^{d_2}=\overline{a}_2$, we get a system of the form (4)

$$\begin{cases} (y_1+\overline{a}_1)^{\alpha}\cdot(y_2+\overline{a}_2)^{\beta}+y_1^{\alpha}\cdot y_2^{\beta} & = & b_1, \\ (y_1+\overline{a}_1)^{\gamma}\cdot(y_2+\overline{a}_2)^{\delta}+y_1^{\gamma}\cdot y_2^{\delta} & = & b_2. \end{cases}$$

Thus a system with a tuple of parameters $(\alpha{\cdot}d_1, \beta{\cdot}d_2, \gamma{\cdot}d_1, \delta{\cdot}d_2) \mod 2^m{-}1$ has the maximal number of solutions that satisfy the conditions (5), which coincides with the maximal number of solutions of the system (4).

The systems of the form (4) with tuples of parameters $(\alpha, \beta, \gamma, \delta)$, $(\gamma, \delta, \alpha, \beta)$, $(\beta, \alpha, \delta, \gamma)$, and $(\delta, \gamma, \beta, \alpha)$ coincide up to a change in the order of writing equations or renaming variables. □

Further, throughout this section, we will consider the case $m = 4$.

Remark 1. Note that the sets $\{1, 2, 4, 8\}$ and $\{7, 11, 13, 14\}$ are closed under multiplication by $d \in \{1, 2, 4, 8\}$ modulo 15. Then, by virtue of Statement 2, we obtain that $8^4 = 2^{12} = 4096$ of all possible parameter tuples $(\alpha, \beta, \gamma, \delta)$ of the functions from the family (2) are split into disjoint equivalence classes with the same maximal number of solutions of the system (4) under the constraints (5) in each class. A distinct equivalence class can be obtained from one of its representatives $(\alpha, \beta, \gamma, \delta)$, by composing different tuples from the following ones

$$(\alpha \cdot d_1 \cdot d_3, \quad \beta \cdot d_1 \cdot d_4, \quad \gamma \cdot d_2 \cdot d_3, \quad \delta \cdot d_2 \cdot d_4) \mod 15, \tag{8a}$$

$$(\gamma \cdot d_1 \cdot d_3, \quad \delta \cdot d_1 \cdot d_4, \quad \alpha \cdot d_2 \cdot d_3, \quad \beta \cdot d_2 \cdot d_4) \mod 15, \tag{8b}$$

$$(\beta \cdot d_1 \cdot d_3, \quad \alpha \cdot d_1 \cdot d_4, \quad \delta \cdot d_2 \cdot d_3, \quad \gamma \cdot d_2 \cdot d_4) \mod 15, \tag{8c}$$

$$(\delta \cdot d_1 \cdot d_3, \quad \gamma \cdot d_1 \cdot d_4, \quad \beta \cdot d_2 \cdot d_3, \quad \alpha \cdot d_2 \cdot d_4) \mod 15, \tag{8d}$$

where $d_1, d_2, d_3, d_4 \in \{1, 2, 4, 8\}$.

Statement 3. *There are* 64 *different tuples of the form*

$$(d_1 \cdot d_3, \quad d_1 \cdot d_4, \quad d_2 \cdot d_3, \quad d_2 \cdot d_4) \mod 15,$$

where $d_1, d_2, d_3, d_4 \in \{1, 2, 4, 8\}$.

Proof. At the beginning, let us put $d_1 \cdot d_3 = 1$, this is possible in four cases: $d_1 = d_3 = 1$, or $d_1 = d_3 = 4$, or $d_1 = 2$, $d_3 = 8$, or $d_1 = 8$, $d_3 = 2$. Note that in the first case tuples of the form $(1,\ d_4,\ d_2,\ d_2 \cdot d_4) \mod 15$ are specified. Taking into account that $d_2, d_4 \in \{1, 2, 4, 8\}$, we get 16 different tuples. In the remaining three cases the values d_1 and d_3 generate tuples that coincide with these 16 already considered ones. Similarly, we obtain 16 different tuples for the cases $d_1 \cdot d_3 = 2$, $d_1 \cdot d_3 = 4$, $d_1 \cdot d_3 = 8$. This implies the validity of the statement. □

Thus, by virtue of Statement 2, the set of $(8, 8)$-functions derived using the generalized construction (2) is divided into equivalence classes corresponding to the tuples of parameters $(\alpha, \beta, \gamma, \delta)$ with the same maximal number of solutions to (4), (5) for functions from the same class. Moreover, due to Lemma 1, functions from the same class have the same lower bound for differential uniformity. The auxiliary Statement 3 that is proven in this section we will use to calculate the cardinality of each equivalence class.

4. Justification of criteria for rejection of vectorial Boolean functions derived using a generalized construction

In this section, we prove statements that allow us to reject functions given by the construction (2), either by the high differential uniformity or by the nonbijectivity. The statements of the previous and present sections permit to make the conclusion for all functions from the equivalence class basing on the analysis of only one of its representatives.

4.1. On differential uniformity

This subsection is devoted to rejection of $(2m, 2m)$-functions (2) in the case of $m = 4$, by differential uniformity $2^m - 2 = 14$ and higher. Moreover, some of the statements below (Propositions 1, 2) are also true in the general case (without restriction $m = 4$).

Proposition 1. *Let F be a $(2m, 2m)$-function given by the construction* (2)*. If the mappings x^α and x^γ define linear permutations over the field $\mathbb{F}_{2^m}$, then $\delta_F \geqslant 2^m - 2$.*

Proof. Let $x_1 \neq 0$, $x_2 \neq 0$. Consider the case $a_2 = 0$, then the system of equations (4) may be written in the form

$$\begin{cases} x_2^\beta((x_1 + a_1)^\alpha + x_1^\alpha) &= b_1, \\ x_2^\delta((x_1 + a_1)^\gamma + x_1^\gamma) &= b_2. \end{cases}$$

Since the permutations x^α and x^γ are linear, we obtain

$$\begin{cases} x_2^\beta(x_1^\alpha + a_1^\alpha + x_1^\alpha) &= b_1, \\ x_2^\delta(x_1^\gamma + a_1^\gamma + x_1^\gamma) &= b_2, \end{cases}$$

$$\begin{cases} x_2^\beta \cdot a_1^\alpha &= b_1, \\ x_2^\delta \cdot a_1^\gamma &= b_2. \end{cases} \tag{9}$$

Further, we fix arbitrarily $a_1, b_1 \in \mathbb{F}_{2^m}$, $a_1 \neq 0$, $b_1 \neq 0$. Because of the bijectivity of the mapping x^β from the first equation of the system (9) we find unique $x_2 \neq 0$ and substitute it into the second equation, thereby defining b_2. Thus, for fixed permissible values of a_1, b_1, b_2, the system (9) is solvable with respect to x_2, while x_1 may take any admissible values. Therefore, taking into account the constraints $x_1 \neq 0$, $x_1 \neq a_1$, we obtain that the number of solutions of the system is at least $2^m - 2$. Using Lemma 1, we find that $\delta_F \geqslant 2^m - 2$. □

Remark 2. In view of Proposition 1 and Statement 2 in the case $m = 4$ we have $2 \cdot 4^2 \cdot 8^2 - 4^4 = 1792$ tuples of parameters $(\alpha, \beta, \gamma, \delta)$ corresponding to $(8, 8)$-functions from the family (2) with a large differential uniformity.

Proposition 2. *Let F be a $(2m, 2m)$-function given by the construction* (2)*. If $\alpha = \beta = \gamma = \delta$, then $\delta_F \geqslant 2^m - 2$.*

Proof. Let $x_1 \neq 0$, $x_2 \neq 0$. Let $a_2 = 0$, $b_1 = b_2 = 1$, then the system of equations (4) is reduced to one equation

$$x_2^{\alpha}((x_1 + a_1)^{\alpha} + x_1^{\alpha}) = 1. \qquad (10)$$

Since the mapping x^{α} is bijective, if x_2 runs through all $2^m - 1$ values from the multiplicative group of the field $\mathbb{F}_{2^m}$, then the inverse element to x_2^{α}, which we denote c, also takes all values from the multiplicative group. Thus, the equation (10) may be written as

$$(x_1 + a_1)^{\alpha} + x_1^{\alpha} = c, \qquad (11)$$

where $c \in \mathbb{F}_{2^m} \setminus \{0\}$. It is known [17, Sec. 4] that the total number of solutions to the equation (11) is equal to 2^m, where $a_1 \neq 0$ is a fixed value and c takes all $2^m - 1$ values from the multiplicative group of the field $\mathbb{F}_{2^m}$. Therefore, taking into account the constraints $x_1 \neq 0$, $x_1 \neq a_1$ (5), the number of solutions of the original system is no less than $2^m - 2$. In view of the Lemma 1 the same estimate is true for δ_F. □

Remark 3. According to Proposition 2 and Statements 2, 3 in the case $m = 4$ we have 64 tuples of parameters $(\alpha, \beta, \gamma, \delta)$ that were not previously considered in Proposition 1. These tuples define $(8, 8)$-functions from the family (2) with a large differential uniformity. The representative of this equivalence class is $(7, 7, 7, 7)$.

Proposition 3. *Let F be a $(8, 8)$-function given by the construction* (2)*. If $\alpha = 11$, $\beta = \gamma = 1$, $\delta = 13$, then $\delta_F \geqslant 14$.*

Proof. Let $a_1 = a_2 = x \in \mathbb{F}_{2^4}$, $b_1 = 0$, $b_2 = x^3 + 1 \in \mathbb{F}_{2^4}$, where x is a primitive element of the field. Then the system of equations (4) may be written in the form

$$\left\{ \begin{array}{lcl} (x_1 + x)^{11} \cdot (x_2 + x) + x_1^{11} \cdot x_2 & = & 0, \\ (x_1 + x) \cdot (x_2 + x)^{13} + x_1 \cdot x_2^{13} & = & x^3 + 1. \end{array} \right. \tag{12}$$

From the first equation in (12) it follows that $x_1 \neq 0$, $x_2 \neq 0$, $x_1 \neq x = a_1$, $x_2 \neq x = a_2$, therefore, $x_1 + x$ and x_1 are elements of the multiplicative group of the field $\mathbb{F}_{2^4}$, hence they are some powers of x, in addition, $(x_1 + x)^{11} \cdot (x_2 + x) = x_1^{11} \cdot x_2$. Therefore, raising both sides of the last equality to the 11th power and using the fact that $x^{15} = 1$, we get

$$(x_1 + x) \cdot (x_2 + x)^{11} = x_1 \cdot x_2^{11}. \tag{13}$$

Substituting the expression in the left-hand side of (13) into the second equation of the system (12), we obtain the chain of equations

$$x_1 \cdot x_2^{11} \cdot (x_2 + x)^2 + x_1 \cdot x_2^{13} = x^3 + 1 \Leftrightarrow x_1 \cdot x_2^{11} \cdot (x_2^2 + x^2 + x_2^2) = x^3 + 1$$
$$\Leftrightarrow x_1 \cdot x_2^{11} \cdot x^2 = x^3 + 1 \Leftrightarrow x_1 \cdot x_2^{11} = (x^3 + 1) \cdot x^{13} \Leftrightarrow x_1 \cdot x_2^{11} = x^{12}.$$

Hence, taking into account the conditions $x_1 \neq x$, $x_2 \neq x$, we get 14 solutions (x_1, x_2). By Lemma 1, we find that $\delta_F \geqslant 14$. □

Remark 4. For the representative $(\alpha, \beta, \gamma, \delta) = (11, 1, 1, 13)$ all different tuples of its equivalence class may be obtained by formulas (8a) and (8b), since formulas (8c) and (8d) give the same tuples. Indeed, the tuple of parameters $(13, 1, 1, 11)$ in (8d) is obtained from $(11, 1, 1, 13)$ in (8a) for $d_1 = 2$, $d_2 = d_3 = 4$, $d_4 = 8$, the tuple $(1, 11, 13, 1)$ in (8c) is produced from $(1, 13, 11, 1)$ in (8b) for $d_1 = 2$, $d_2 = d_4 = 1$, $d_3 = 8$. Hence, by means of Proposition 3 and Statements 2, 3 we obtain 128 tuples of parameters $(\alpha, \beta, \gamma, \delta)$ corresponding to $(8, 8)$-functions from the family (2) with a large differential uniformity.

Proposition 4. *Let F be a $(8, 8)$-function given by the construction* (2). *If $\alpha = 7$, $\beta = \gamma = 1$, $\delta = 7$, then $\delta_F \geqslant 14$.*

Proof. Let $a_1 = a_2 = a \in \mathbb{F}_{2^4}$, $a \neq 0$, $b_1 = b_2 = b \in \mathbb{F}_{2^4}$, $b \neq 0$, $x_1 = x_2 \neq 0$, then the system of equations (4) may be written in the form

$$\left\{ \begin{array}{lcl} (x_1 + a)^7 \cdot (x_1 + a) + x_1^7 \cdot x_1 & = & b, \\ (x_1 + a) \cdot (x_1 + a)^7 + x_1 \cdot x_1^7 & = & b. \end{array} \right. \tag{14}$$

The system (14) is reduced to equation $(x_1+a)^8+x_1^8=b$, or

$$a^8=b. \tag{15}$$

Let us choose $a,b\in\mathbb{F}_{2^4}$ satisfying the equality (15). Then, taking into account the conditions (5) we obtain 14 solutions (x_1,x_1). By Lemma 1, we find that $\delta_F\geqslant 14$. □

Remark 5. For the representative $(\alpha,\beta,\gamma,\delta)=(7,1,1,7)$ all different tuples of its equivalence class may be obtained by formulas (8a) and (8b), since the tuples $(\beta,\alpha,\delta,\gamma)$ and $(\delta,\gamma,\beta,\alpha)$ in formulas (8c) and (8d) are identical to tuples $(\gamma,\delta,\alpha,\beta)$ and $(\alpha,\beta,\gamma,\delta)$ in (8b) and (8a) respectively. Hence, using Proposition 4 and Statements 2, 3 we find 128 tuples of parameters $(\alpha,\beta,\gamma,\delta)$ corresponding to $(8,8)$-functions from the family (2) with a large differential uniformity.

4.2. On the functions that are not permutations

This section is devoted to rejecting such $(2m,2m)$-functions (2), which can not be used to construct a permutation. The possibility of rejecting the entire equivalence class by one of its representatives, which is not a bijection for any values of auxiliary permutations $\widehat{\pi}_1$, $\widehat{\pi}_2$, is justified. Further, in the case $m=4$, a proposition to discard representatives of seven equivalence classes by the indicated condition is proved.

Statement 4. *Let F be a $(2m,2m)$-function given by the construction (2) with a tuple of parameters $(\alpha,\beta,\gamma,\delta)$, where x^α, x^β, x^γ, and x^δ define monomial permutations. If F is not a bijection for any values of the permutations $\widehat{\pi}_i(x_i)$, $i\in\{0,1\}$, then any $(2m,2m)$-function from the family (2) with the following tuples of parameters*

$$(\alpha\cdot d_1,\ \beta\cdot d_1,\ \gamma\cdot d_2,\ \delta\cdot d_2) \mod 2^m-1,$$
$$(\alpha\cdot d_1,\ \beta\cdot d_2,\ \gamma\cdot d_1,\ \delta\cdot d_2) \mod 2^m-1,$$
$$(\gamma,\ \delta,\ \alpha,\ \beta),\qquad (\beta,\ \alpha,\ \delta,\ \gamma),\qquad (\delta,\ \gamma,\ \beta,\ \alpha)$$

such that the mappings x^{d_1} and x^{d_2} define linear permutations over the field $\mathbb{F}_{2^m}$, also is not a bijection for any values of the permutations $\widehat{\pi}_i(x_i)$, $i\in\{0,1\}$.

Proof. By the condition of the statement, the $(2m,2m)$-function F from the family (2) with parameters $(\alpha,\beta,\gamma,\delta)$ is not a bijection for any values of permutations $\widehat{\pi}_i(x_i)$, $i \in \{0,1\}$, that is, there are such values $x_1, x_2, \widetilde{x}_1$, $\widetilde{x}_2 \in \mathbb{F}_{2^m} \backslash \{0\}$, $x_1 \neq \widetilde{x}_1$ or $x_2 \neq \widetilde{x}_2$, that the following equalities hold:

$$y_1 = G_1(x_1,x_2) = x_1^{\alpha} \cdot x_2^{\beta} = \widetilde{x}_1^{\alpha} \cdot \widetilde{x}_2^{\beta} = G_1(\widetilde{x}_1,\widetilde{x}_2) = \widetilde{y}_1,$$
$$y_2 = G_2(x_1,x_2) = x_1^{\gamma} \cdot x_2^{\delta} = \widetilde{x}_1^{\gamma} \cdot \widetilde{x}_2^{\delta} = G_2(\widetilde{x}_1,\widetilde{x}_2) = \widetilde{y}_2.$$

Then for the same values of $x_1, x_2, \widetilde{x}_1, \widetilde{x}_2$ for the tuples $(\alpha \cdot d_1, \beta \cdot d_1, \gamma \cdot d_2, \delta \cdot d_2) \bmod (2^m - 1)$ we have $G_1(x_1,x_2) = x_1^{d_1\alpha} \cdot x_2^{d_1\beta} = (x_1^{\alpha} \cdot x_2^{\beta})^{d_1} = (\widetilde{x}_1^{\alpha} \cdot \widetilde{x}_2^{\beta})^{d_1} = \widetilde{x}_1^{d_1\alpha} \cdot \widetilde{x}_2^{d_1\beta} = G_1(\widetilde{x}_1,\widetilde{x}_2)$, and similarly $G_2(x_1,x_2) = G_2(\widetilde{x}_1,\widetilde{x}_2)$.

Based on the bijectivity of the mappings x^{d_1}, x^{d_2}, which define linear permutations, for the tuples $(\alpha \cdot d_1,\ \beta \cdot d_2,\ \gamma \cdot d_1,\ \delta \cdot d_2) \bmod (2^m - 1)$ we uniquely find values $v_1, v_2, \widetilde{v}_1, \widetilde{v}_2 \in \mathbb{F}_{2^m} \backslash \{0\}$, such that $v_1^{d_1} = x_1$, $v_2^{d_2} = x_2$, $\widetilde{v}_1^{d_1} = \widetilde{x}_1$, $\widetilde{v}_2^{d_2} = \widetilde{x}_2$. Then $G_1(v_1,v_2) = v_1^{d_1\alpha} \cdot v_2^{d_2\beta} = x_1^{\alpha} \cdot x_2^{\beta} = \widetilde{x}_1^{\alpha} \cdot \widetilde{x}_2^{\beta} = \widetilde{v}_1^{d_1\alpha} \cdot \widetilde{v}_2^{d_2\beta} = G_1(\widetilde{v}_1,\widetilde{v}_2)$, and similarly $G_2(v_1,v_2) = G_2(\widetilde{v}_1,\widetilde{v}_2)$.

For tuples of parameters $(\gamma,\delta,\alpha,\beta)$, $(\beta,\alpha,\delta,\gamma)$, $(\delta,\gamma,\beta,\alpha)$ the equal values $y_1 = \widetilde{y}_1$ and $y_2 = \widetilde{y}_2$ are obtained by the corresponding transposition of arguments $x_1, x_2, \widetilde{x}_1, \widetilde{x}_2$. □

Proposition 5. $(8,8)$-*function* F *given by the construction* (2) *with the parameters* $(\alpha,\beta,\gamma,\delta)$ *from the list below* 1) $(7,7,7,13)$, 2) $(1,7,7,7)$, 3) $(4,7,7,7)$, 4) $(7,7,2,2)$, 5) $(1,1,7,13)$, 6) $(2,7,7,7)$, 7) $(7,2,2,7)$, *is not a bijection for any values of the permutations* $\widehat{\pi}_i(x_i)$, $i \in \{0,1\}$.

Proof. For the construction (2) with each of the seven specified tuples of parameters from the condition of the proposition, it suffices to indicate the values $x_1, x_2, \widetilde{x}_1, \widetilde{x}_2 \in \mathbb{F}_{2^4} \backslash \{0\}$, $x_1 \neq \widetilde{x}_1$ or $x_2 \neq \widetilde{x}_2$, such that $y_1 = G_1(x_1,x_2) = x_1^{\alpha} \cdot x_2^{\beta} = \widetilde{x}_1^{\alpha} \cdot \widetilde{x}_2^{\beta} = G_1(\widetilde{x}_1,\widetilde{x}_2) = \widetilde{y}_1$ and $y_2 = G_2(x_1,x_2) = x_1^{\gamma} \cdot x_2^{\delta} = \widetilde{x}_1^{\gamma} \cdot \widetilde{x}_2^{\delta} = G_2(\widetilde{x}_1,\widetilde{x}_2) = \widetilde{y}_2$.

1. Let $x_1 = x \in \mathbb{F}_{2^4}$, $x_2 = x^3 + x^2 = x^6 \in \mathbb{F}_{2^4}$, $\widetilde{x}_1 = \widetilde{x}_2 = x^3 + x^2 + x = x^{11} \in \mathbb{F}_{2^4}$. Then $y_1 = x_1^7 \cdot x_2^7 = x^7 \cdot (x^6)^7 = x^4$, $y_2 = x_1^7 \cdot x_2^{13} = x^7 \cdot (x^6)^{13} = x^{10}$, $\widetilde{y}_1 = \widetilde{x}_1^7 \cdot \widetilde{x}_2^7 = (x^{11})^7 \cdot (x^{11})^7 = x^4$, $\widetilde{y}_2 = \widetilde{x}_1^7 \cdot \widetilde{x}_2^{13} = (x^{11})^7 \cdot (x^{11})^{13} = x^{10}$.

For the other tuples, the proof may be carried out similarly; therefore, we present only sets of appropriate values $x_1, x_2, \widetilde{x}_1, \widetilde{x}_2$.

2. $x_1 = 1$, $x_2 = x^2 + x$, $\widetilde{x}_1 = x^3 + x^2 + x$, $\widetilde{x}_2 = x^2 + x + 1$.
3. $x_1 = x^3 + x^2 + x$, $x_2 = x$, $\widetilde{x}_1 = x$, $\widetilde{x}_2 = x^3 + x^2 + x$.
4. $x_1 = x_2 = 1$, $\widetilde{x}_1 = x^3 + x^2 + x + 1$, $\widetilde{x}_2 = x^3$.
5. $x_1 = x$, $x_2 = x^3$, $\widetilde{x}_1 = x^3 + x^2 + x$, $\widetilde{x}_2 = x^2 + 1$.
6. $x_1 = 1$, $x_2 = x^3 + x$, $\widetilde{x}_1 = \widetilde{x}_2 = x^3 + x^2 + x + 1$.
7. $x_1 = 1$, $x_2 = x^3 + x^2$, $\widetilde{x}_1 = x^3 + x^2 + x + 1$, $\widetilde{x}_2 = x^3 + x$. □

Corollary 1. $(8,8)$*-functions F from the family* (2) *with parameters* $(\alpha,\beta,\gamma,\delta)$ *from the equivalence classes generated by the tuples of parameters indicated in Proposition* 5, *are not bijections for any values of permutations* $\widehat{\pi}_i(x_i)$, $i\in\{0,1\}$.

Taking into account the Corollary 1, we reject all tuples of parameters from the equivalence classes with representatives specified in the Proposition 5.

Remark 6. For the representative $(\alpha,\beta,\gamma,\delta)=(7,7,7,13)$ all different tuples of its equivalence class may be obtained by the formula (8a), since formulas (8b), (8c), and (8d) will give the same tuples. Therefore, in the equivalence class generated by the representative $(7,7,7,13)$, there are 64 tuples of parameters. Further, the representatives of $(4,7,7,7)$, $(1,7,7,7)$ and $(2,7,7,7)$ generate three classes with 256 tuples in each one (768 tuples in total). Reasoning similarly to the Remark 5, we can show that the representatives of $(1,1,7,13)$, $(7,7,2,2)$ and $(7,2,2,7)$ generate equivalence classes of 128 tuples in each one (384 tuples in total).

In Table 1 we show the representatives of the equivalence classes and the reasons for rejection.

Table 1. Summary table of the equivalence classes for $m=4$

№	The representative of the equivalence class	The number of elements	The reason for rejection
1	Generalized representative: $(\alpha,\beta,\gamma,\delta)$, where $\alpha,\gamma\in\{1,2,4,8\}$	1792	$\delta_F\geqslant 14$, according to Statement 1
2	(7,7,7,7)	64	$\delta_F\geqslant 14$, according to Statement 2
3	(11,1,1,13)	128	$\delta_F\geqslant 14$, according to Statement 3
4	(7,1,1,7)	128	$\delta_F\geqslant 14$, according to Statement 4
5	(7,7,7,13)	64	are not permutations, according to Statement 5
6	(1,7,7,7)	256	
7	(4,7,7,7)	256	
8	(7,7,2,2)	128	
9	(1,1,7,13)	128	
10	(2,7,7,7)	256	
11	(7,2,2,7)	128	
12	(1,1,7,11)	256	are not rejected
13	(1,7,7,11)	256	
14	(1,7,7,2)	128	
15	(7,7,7,11)	128	

Conclusion

The statements proved in this paper justify the rejection of 3328 tuples of parameters $(\alpha, \beta, \gamma, \delta)$ of $(8, 8)$-functions F defined by the construction (2) due to the value $\delta_F \geqslant 14$ or because F is not a bijection. The 768 tuples of parameters $(\alpha, \beta, \gamma, \delta)$ remained unrejected, which are split by Statement 2 and Remark 1 into 4 equivalence classes with representatives $(1, 1, 7, 11)$, $(1, 7, 7, 11)$ with 256 tuples in each class, $(1, 7, 7, 2)$, $(7, 7, 7, 11)$ with 128 tuples in each class (see Table 1). In [8, 10] it was indicated that using these tuples of parameters with the correct choice of permutations $\widehat{\pi}_i(x_i)$, $i \in \{0, 1\}$, 6-uniform permutations with nonlinearity 108 can be obtained. Experimental results on receiving permutations with given cryptographic properties and an algebraic degree that is equal to 7 are presented in [18].

References

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

[2] 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, https://doi.org/10.4213/mvk227.

[3] Fomin D., “On the way of constructing 2n-bit permutations from n-bit ones”, The VIIIth Workshop on Current Trends in Cryptology (CTCrypt 2019), 2019, https://ctcrypt.ru/files/files/2019/materials/07_Fomin.pdf.

[4] 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**, 2019, 191–206.

[5] De la Cruz Jiménez R.A., “On some methods for constructing almost optimal S-Boxes and their resilience against side-channel attacks”, Cryptology ePrint Archive, Report 2018/618, https://eprint.iacr.org/2018/618.

[6] De la Cruz Jiménez R.A., “A method for constructing permutations, involutions and orthomorphisms with strong cryptographic properties”, *Prikl. discr. matem. Prilozheniye*, **12** (2019), 145–151, https://doi.org/10.17223/2226308X/12/42.

[7] Fomin D.B., “New classes of 8-bit permutations based on a butterfly structure”, *Matematicheskie voprosy kriptografii*, **10**:2 (2019), 169–180, https://doi.org/10.4213/mvk294.

[8] Fomin D.B., “On approaches to constructing low-resource nonlinear transformations”, *Obozr. prikl. promyshl. matem.*, **25**:4 (2018), 379–381 (In Russian).

[9] Fomin D.B., “Constructing permutations of the space V_{2m} using $(2m, m)$-functions”, *Matematicheskie voprosy kriptografii*, **11**:3 (2020), 121–138 (In Russian).

[10] Fomin D.B., “On algebraic degree and differential uniformity of permutations of the space V_{2m}, constructed using $(2m, m)$-functions”, *Matematicheskie voprosy kriptografii*, **11**:4 (2020), 133–149 (In Russian).

[11] Biryukov A., Perrin L., Udovenko A., “Reverse-engineering the s-box of streebog, kuznyechik and stribobr1”, *Lect. Notes Comput. Sci.*, EUROCRYPT (1), **9665**, 2016, 372–402.

[12] Canteaut A., Perrin L., Cryptology ePrint Archive, Report 2018/713, https://eprint.iacr.org/2018/713.

[13] Lidl R., Niederreiter H., *Finite Fields*, 2nd ed., Cambridge Univ. Press, 1997, 755 pp.

[14] Browning K.A., Dillon J.F., McQuistan M.T., Wolfe A.J., “An APN permutation in dimension six”, *Contemp. Math.*, **518** (2010), 33–42.

[15] Knuth D., *Art of Computer Programming.* V. 2: *Seminumerical Algorithms*, 3rd, Addison-Wesley Prof., 1997, 784 pp.

[16] Kazymyrov O.V., *Methods and tools for generating nonlinear replacement nodes for symmetric cryptographic algorithms*, Diss. kand. tekhn. nauk. Khar’kov, 2013 (In Russian), 190 pp.

[17] Heys H., *A Tutorial on Linear and Differential Cryptanalysis*, 2002, `http://www.engr.mun.ca/~howard/PAPERS/ldc_tutorial.pdf`.

[18] Kovrizhnykh M.A., Fomin D.B., “On a heuristic approach to constructing bijective vector Boolean functions with given cryptographic properties”, *Prikl. Diskr. Mat. Priloz.*, **14** (2021), 181–184 (In Russian).

МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ