УДК 519.7 DOI 10.17223/20710410/61/2

# NONLINEARITY OF APN FUNCTIONS: COMPARATIVE ANALYSIS AND ESTIMATES

V. G. Ryabov

*NP "GST", Moscow, Russia*

**E-mail:** 4vryabov@gmail.com

The main results of the paper relate to the nonlinearity of APN functions defined for a vectorial Boolean function as the Hamming distance from it to the set of affine mappings in the space of images of all vectorial Boolean functions in fixed dimension. For APN functions in dimension $n$, the lower nonlinearity bound of the form $2^n - \sqrt{2^{n+1} - 7 \cdot 2^{-2}} - 2^{-1}$ and the corresponding lower bound on the affinity order are obtained. The exact values of the nonlinearity of all APN functions up to dimension 5 are found, and also for one known APN 6-dimensional permutation and for all differentially 4-uniform permutations in dimension 4.

**Keywords:** *vectorial Boolean function, permutation, APN function, EA-equivalence, nonlinearity, differentially uniform.*

# НЕЛИНЕЙНОСТЬ APN-ФУНКЦИЙ: СРАВНИТЕЛЬНЫЙ АНАЛИЗ И ОЦЕНКИ

В. Г. Рябов

*НП «ГСТ», г. Москва, Россия*

Нелинейность APN-функции определяется как расстояние Хэмминга от неё до множества аффинных отображений в пространстве значений векторных булевых функций фиксированной размерности. Для APN-функций размерности $n$ получены нижняя граница нелинейности вида $2^n - \sqrt{2^{n+1} - 7 \cdot 2^{-2}} - 2^{-1}$ и соответствующая ей нижняя граница порядка аффинности. Найдены точные значения нелинейности всех APN-функций размерности, не превосходящей 5, а также для одной известной APN-подстановки размерности 6 и для всех дифференциально 4-равномерных подстановок размерности 4.

**Ключевые слова:** *векторная булева функция, подстановка, APN-функция, EA-эквивалентность, нелинейность, дифференциальная равномерность.*

## 1. Introduction

Denote by $\mathbb{F}_2^n$ the $n$-dimensional vector space over the two-element field $\mathbb{F}_2$, where $n$ is a natural number, and by $P_2^{n,k}$ the set of all mappings of the space $\mathbb{F}_2^n$ into the space $\mathbb{F}_2^k$. The mapping $F \in P_2^{n,k}$ is called a vectorial Boolean function or simply a vectorial function, implying the Boolean case, and in the case $k = 1$ we will use similar terms without the adjective "vectorial". The subset of one-to-one mappings from $P_2^{n,n}$, called permutations, is denoted by $S_2^n$.

Any vectorial Boolean function is uniquely determined by an ordered set of coordinate Boolean functions. In turn, each coordinate function can be represented by a polynomial

of $n$ variables over the field $\mathbb{F}_2$. For a vectorial function $F \in P_2^{n,k}$, the algebraic degree of nonlinearity $\deg F$ is usually defined as the maximum degree of the polynomials representing its coordinate functions. Under the condition $\deg F \leqslant 1$ the mapping $F$ is affine. Denote by $A_2^{n,k}$ the subset of all affine mappings from the set $P_2^{n,k}$.

As noted in [1], two approaches to the definition of the nonlinearity of vectorial functions have become widespread. The first approach is based on using the Hamming distance. The Hamming distance from the function $f \in P_2^{n,1}$ to the set $A_2^{n,1}$ in the space $\mathbb{F}_2^{2^n}$, called its nonlinearity, is denoted by $N_f$. In [2], with an orientation towards the linear method of cryptanalysis, the nonlinearity of the vectorial function $F \in P_2^{n,k}$ with a set of coordinate functions $\boldsymbol{f} = (f_1, \ldots, f_k)$ is defined by the formula

$$NL_F = \min_{\boldsymbol{w} \in \mathbb{F}_2^k \setminus \{\mathbf{0}\}} N_{\langle \boldsymbol{w}, \boldsymbol{f} \rangle}, \tag{1}$$

where $\langle \cdot, \cdot \rangle$ denotes the inner product of vectors, that is, it is the minimum of the nonlinearities of all nonzero linear combinations of coordinate functions of the mapping $F$. The Boolean case allows to give an equivalent definition of the nonlinearity of a vectorial function using the maximum absolute value of the Walsh — Hadamard transform coefficients of all nonzero linear combinations of its coordinate functions.

The second approach to determining the nonlinearity of the vectorial function $F$, associated with the differential method of cryptanalysis, is to compare for all possible $\alpha \in \mathbb{F}_2^n \setminus \{\mathbf{0}\}$ and $\beta \in \mathbb{F}_2^k$ the cardinalities of subsets of variables for which the directed derivative satisfies the condition

$$D_\alpha F(\boldsymbol{x}) = F(\boldsymbol{x} \oplus \alpha) \oplus F(\boldsymbol{x}) = \beta, \tag{2}$$

where $\oplus$ is the addition operation in the corresponding space. Since in the Boolean case the equality $D_\alpha F(\boldsymbol{x}) = D_\alpha F(\boldsymbol{x} \oplus \alpha)$ is true, all elements of this spectrum have an even value. For $F \in P_2^{n,k}$, the value

$$\triangle_F = \max_{\substack{\alpha \in \mathbb{F}_2^n \setminus \{\mathbf{0}\}, \\ \beta \in \mathbb{F}_2^k}} \big|\{\boldsymbol{x} : D_\alpha F(\boldsymbol{x}) = \beta\}\big|,$$

is considered in this approach as an indicator of nonlinearity. A mapping $F \in P_2^{n,k}$ for which the condition $\triangle_F \leqslant \delta$ is satisfied is called a differentially $\delta$-uniform [3], and in the case $k = n$ and $\delta = 2$ it is called almost perfect nonlinear or APN function [4].

At the same time, within the framework of the first approach, one more indicator of the nonlinearity of the vectorial function can be naturally determined. Taking into account the isomorphism of the Abelian groups of the vector space $\mathbb{F}_2^k$ and the field $\mathbb{F}_{2^k}$, the classical Hamming distance in space $\mathbb{F}_{2^k}^{2^n}$ can be used to measure the remoteness of the functions $F_1$ and $F_2$ from $P_2^{n,k}$. Let's denote this distance by $\rho(F_1, F_2)$. For a vectorial function $F \in P_2^{n,k}$ let's define the nonlinearity indicator $N_F$ using the formula

$$N_F = \min_{A \in A_2^{n,k}} \rho(F, A). \tag{3}$$

In [5–7] this indicator was called the second type of nonlinearity, and in [8] — the vectorial nonlinearity.

For $k = 1$, the nonlinearity indicators in the sense (1) and in the sense (3) are the same. However, starting from $k = 2$, they differ significantly. The indicator $N_F$ also plays

an important role in cryptography and coding [7]. In particular, it is more relevant for the analysis of methods using multi-dimensional affine approximations of Boolean vectorial functions. For example, it can be used to get the lower bound on the minimum number of affinity domains in an arbitrary piecewise affine representation of a vectorial Boolean function, which in the domestic cryptographic literature is referred to as the affinity order and denoted by $\operatorname{ard} F$. Indeed, it is easy to see that the affinity order of the vectorial function $F \in P_2^{n,k}$ satisfies the inequality

$$\operatorname{ard} F \geqslant \frac{2^n}{2^n - N_F}. \tag{4}$$

Moreover, unlike the characteristics $NL_F$ and $\triangle_F$, the indicator $N_F$ is a metric, which makes it possible to speak mathematically correctly about the remoteness of a vectorial function from affine ones. In this regard, in [9, 10], relating to the case of arbitrary finite fields, the indicator of the form $N_F$ was called the nonlinearity of the mapping $F$.

The nonlinearity in the sense (1) for APN functions has been studied by many authors. Here it is necessary to highlight the papers of C. Carlet (see, for example, [11–16]). For a vectorial function $F \in P_2^{n,n}$, the Sidelnikov — Chabaud — Vaudenay inequality implies an upper bound on the nonlinearity in the sense (1), namely

$$NL_F \leqslant 2^{n-1} - 2^{(n-1)/2}. \tag{5}$$

This bound is reached only for odd $n$ for the so-called almost bent or AB functions. All AB functions are APN functions. The converse is not true in general, but it is true in particular case of odd $n$ for quadratic functions. For other currently known APN functions, including the case of even $n$, the largest value of nonlinearity in the sense (1) is $2^{n-1} - 2^{n/2}$. Also of interest are the lower bounds given in [16], namely, $NL_F \geqslant 2^{n-1} - 2^{(3n-3)/4}$ for odd $n$ and $NL_F \geqslant 2^{n-1} - 2^{(3n-2)/4}$ for even $n$. At the same time, there are a number of open problems regarding nonlinearity in the sense (1) for APN functions [13].

The nonlinearity in the sense (3) for APN functions has been studied to a lesser extent. From the results of [7] for a vectorial function $F \in P_2^{n,k}$ follows a chain of inequalities of the form $0 \leqslant NL_F \leqslant N_F \leqslant 2^n - 2^{n-k} - 1$. In [15][1], another upper bound of the form

$$N_F \leqslant 2^n - n - 1 \tag{6}$$

is obtained (for $k \leqslant 2n - 5$ or $k = n = 4$, a strict inequality holds). Using estimates of the size of the image set, the lower bound on the indicator $N_F$ for differentially $\delta$-uniform vectorial functions from $P_2^{n,k}$ of the form

$$N_F \geqslant 2^n - \sqrt{2^n + \delta\ (2^n - 1)} \tag{7}$$

is also obtained there, from which the lower bound on this indicator follows for all APN functions in dimension $n$ of the form

$$N_F \geqslant 2^n - \sqrt{3 \cdot 2^n - 2}. \tag{8}$$

At the same time, the study of the behavior of nonlinearity in the sense (3) of vectorial Boolean functions, including APN functions, needs to be continued, which was, in particular, indicated in the open problem 11 of the eighth international Olympiad in cryptography

[1] In [15], as applied to the indicator $N_F$, the term nonlinearity is not used.

NSUCRYPTO2021 [17]. In the footsteps of solving this problem using estimates of the size of the Sidon set, G. P. Nagy at the end of 2022 posted material with new lower bounds on the Internet [8]. Its lower bound on the indicator $N_F$ for differentially $\delta$-uniform vectorial functions from $P_2^{n,k}$ has the form

$$N_F \geqslant 2^n - \sqrt{\delta \cdot 2^n} - 2^{-1},$$

from which the lower bound on this indicator follows for all APN functions in dimension $n$ of the form

$$N_F \geqslant 2^n - \sqrt{2^{n+1}} - 2^{-1}.$$

This paper is devoted to the study of the nonlinearity of APN functions in the sense (3). In what follows, unless otherwise stated, by the nonlinearity of a vectorial function we mean the indicator $N_F$. The main task is to refine the bounds on the nonlinearity of the APN functions and find its exact values for the APN functions in small dimension ($n \geqslant 5$), as well as to compare the behavior of $N_F$ with $\deg F$ and $NL_F$ for such mappings. In parallel and independently of the studies of G. P. Nagy, without resorting to estimates of the size of the Sidon set, the author has obtained a lower bound on the nonlinearity of APN functions, which is presented in Section 2. A lower bound on the affinity order that follows from it is also given. In Section 3, the exact values of the nonlinearity for all APN functions up to dimension 5, as well as for one known APN 6-dimensional permutation, are found. Since none of the 4-dimensional permutations is an APN, in Section 4 the case of differentially 4-uniform permutations in dimension 4 is considered. In Section 5, open problems and conjectures related to the behavior of the nonlinearity of APN functions are presented.

## 2. Boundaries on nonlinearity of APN functions

In [18], the following necessary and sufficient condition for a Boolean vectorial function to be an APN was first obtained.

**Proposition 1** [18]. Let a vectorial function $F \in P_2^{n,n}$. Then $F$ is APN if and only if there is no 2-dimensional linear manifold[2] in the space of the domain of $F$ on which the mapping $F$ coincides with some affine one.

In [19] this condition is used as an alternative definition of APN functions. There are other formulations of this condition, for example, for pairwise distinct variables $\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_3, \boldsymbol{x}_4 \in \mathbb{F}_2^n$, if the equality $\boldsymbol{x}_1 \oplus \boldsymbol{x}_2 \oplus \boldsymbol{x}_3 \oplus \boldsymbol{x}_4 = 0$ holds, then the inequality $F(\boldsymbol{x}_1) \oplus F(\boldsymbol{x}_2) \oplus F(\boldsymbol{x}_3) \oplus F(\boldsymbol{x}_4) \neq 0$ is true.

**Theorem 1.** Let $F$ be the APN function in dimension $n$. Then the following inequality is true for its nonlinearity:

$$N_F \geqslant 2^n - \sqrt{2^{n+1} - 7 \cdot 2^{-2}} - 2^{-1}. \tag{9}$$

***Proof.*** Let's prove the theorem by contradiction, assuming that the inequality

$$N_F < 2^n - \sqrt{2^{n+1} - 7 \cdot 2^{-2}} - 2^{-1} \tag{10}$$

is true. It follows from the definition of nonlinearity that there is at least one affine mapping $A \in A_2^{n,n}$ with which the vectorial function $F$ coincides on $2^n - N_F$ variables of the domain of $F$ and $A$. Let $\mathbf{C}_{F,A} = \{\boldsymbol{x} \in \mathbb{F}_2^n : F(\boldsymbol{x}) = A(\boldsymbol{x})\}$ and $C_{F,A} = |\mathbf{C}_{F,A}| = 2^n - N_F$. Then inequality (10) implies the inequality

$$C_{F,A} > \sqrt{2^{n+1} - 7 \cdot 2^{-2}} + 2^{-1}.$$

[2] In the original, a linear manifold is called an affine subspace.

The number of all possible unordered pairs of elements from the set $\mathbf{C}_{F,A}$ satisfies the chain of relations

$$\binom{C_{F,A}}{2} = \frac{C_{F,A}(C_{F,A}-1)}{2} > 2^n - 1.$$

Therefore, among nonzero vectors from the set $\{\boldsymbol{x}_1 \oplus \boldsymbol{x}_2 : \boldsymbol{x}_1, \boldsymbol{x}_2 \in \mathbf{C}_{F,A},\ \boldsymbol{x}_1 \neq \boldsymbol{x}_2\}$ there will definitely be the same. The vectors $\boldsymbol{x}_1 \oplus \boldsymbol{x}_2$ and $\boldsymbol{x}_1 \oplus \boldsymbol{x}_3$, where $\boldsymbol{x}_2 \neq \boldsymbol{x}_3$, obviously differ. Therefore, there are pairwise distinct vectors $\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_3, \boldsymbol{x}_4 \in \mathbf{C}_{F,A}$, for which the equality $\boldsymbol{x}_1 \oplus \boldsymbol{x}_2 = \boldsymbol{x}_3 \oplus \boldsymbol{x}_4$ is satisfied. These vectors form a 2-dimensional linear manifold on which $F$ coincides with $A$. In accordance with Proposition 1, the vectorial function $F$ is not APN. ■

It is easy to see that the lower bound on the nonlinearity of APN functions, obtained in Theorem 1, for $n > 4$ refines the estimate (8) from [15].

**Corollary 1.** Under the conditions of Theorem 1, for odd $n \geqslant 3$, the following inequality is true:

$$N_F \geqslant 2^n - 2^{(n+1)/2}. \tag{11}$$

Indeed, in the case of odd $n \geqslant 3$, for the difference of an integer $2^{(n+1)/2}$ and the root from expression (9), the chain of relations is valid

$$\sqrt{2^{n+1}} - \sqrt{2^{n+1} - 7 \cdot 2^{-2}} = \frac{7}{2^2(\sqrt{2^{n+1}} + \sqrt{2^{n+1} - 7 \cdot 2^{-2}})} < \frac{7}{30}.$$

**Corollary 2.** Under the conditions of Theorem 1, the following inequality is true:

$$\operatorname{ard} F \geqslant \frac{2^n}{\sqrt{2^{n+1} - 7 \cdot 2^{-2}} + 2^{-1}}; \tag{12}$$

and in the case of odd $n$

$$\operatorname{ard} F \geqslant 2^{(n-1)/2}. \tag{13}$$

Estimates (12) and (13) refine the lower bound on the affinity order from [20] for APN functions.

Inequality (6) can be used as the upper nonlinearity bound for APN functions.

## 3. Nonlinearity of APN functions up to dimension 5

Results on the nonlinearity of APN functions in small dimensions are given for classes of extended affine (EA) equivalence, since unordered sets of algebraic degrees of nonlinearity and absolute values of the Walsh — Hadamard coefficients for nonzero linear combinations of coordinate functions, cardinalities of subsets of variables satisfying condition (2), and also, Hamming distances to all affine mappings are invariants [9] for EA-equivalent vectorial Boolean functions (under CCZ-equivalence, only the spectrum of absolute Walsh — Hadamard values remains as an invariant). Accordingly, all the above nonlinearity indicators, including the algebraic degree, are also invariants in the case of EA-equivalence.

The results obtained in this section are based on results [21, 22], where all classes of EA-equivalent APN functions up to dimension 5 are presented through the canonical element, which is the representative of the class with the smallest truth table in the lexicographic sense. To shorten the notation, the $2^n$-ary number system will be used.

For $n = 1$, all Boolean functions are APN and simultaneously affine.

For $n = 2$, there is a single class of EA-equivalent APN functions presented in the Table 1. Along with the nonlinearity value $N_F$ found here, the values of the degree of nonlinearity $\deg F$ and the nonlinearity in the sense (1) $NL_F$ are also given.

Table 1

**Nonlinearity of APN functions in dimension** 2

| $\boldsymbol{x}$ | 0 | 1 | 2 | 3 | $\deg F$ | $NL_F$ | $N_F$ |
|---|---|---|---|---|---|---|---|
| $F(\boldsymbol{x})$ | 0 | 0 | 0 | 1 | 2 | 0 | 1 |

The value of the nonlinearity coincides with the lower bound (9) and the upper bound (6). The affinity order of all APN functions in dimension 2 is 2. There are no permutations in this EA-class and there is the APN function represented by the power function $x^3$ over a field $\mathbb{F}_4$. Vectorial functions in dimension $n$ over the field $\mathbb{F}_2$, represented by one-dimensional power functions of the form $x^d$ over the field $\mathbb{F}_{2^n}$, are commonly called power vectorial functions or simply power functions[3] with exponent $d$.

For $n = 3$, the class of EA-equivalent APN functions is also unique and is presented together with the nonlinearity indicators in the Table 2.

Table 2

**Nonlinearity of APN functions in dimension** 3

| $\boldsymbol{x}$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | $\deg F$ | $NL_F$ | $N_F$ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $F(\boldsymbol{x})$ | 0 | 0 | 0 | 1 | 0 | 2 | 4 | 7 | 2 | 2 | 4 |

In this case, according to (5), all APN functions are AB. The value of the nonlinearity coincides with the lower bound (11) and the upper bound (6). In accordance with (4), the affinity order of all such mappings is greater than or equal to 2. This class contains permutations, including power functions with exponents 3, 5, and 6.

For $n = 4$, there are 2 classes of EA-equivalent APN functions (these classes are CCZ-equivalent), presented in the Table 3.

Table 3

**Nonlinearity of APN functions in dimension** 4

| $\boldsymbol{x}$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | $\deg F$ | $NL_F$ | $N_F$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $F_1(\boldsymbol{x})$ | 0 | 0 | 0 | 1 | 0 | 2 | 4 | 7 | 0 | 4 | 6 | 3 | 8 | 14 | 10 | 13 | 2 | 4 | 10 |
| $F_2(\boldsymbol{x})$ | 0 | 0 | 0 | 1 | 0 | 2 | 4 | 7 | 0 | 4 | 6 | 3 | 8 | 14 | 11 | 12 | 3 | 4 | 10 |

The values of nonlinearity for both EA-classes coincides with the lower bound (9) and the upper bound (6). In accordance with (4), the affinity order of all APN functions in dimension 4 is greater than or equal to 3. There are no permutations in these classes. The first class contains power functions with exponents 3, 6, 9, and 12. In the second class, there are no power functions, but there are APN functions found in [23].

For $n = 5$, there are already 7 classes of EA-equivalent APN functions, presented in the Table 4 (the first, third and seventh classes, as well as the second, fourth and sixth classes are CCZ-equivalent).

[3]The term monomial functions is also used.

Table 4

**Nonlinearity of APN functions in dimension** 5

| $\boldsymbol{x}$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $F_1(\boldsymbol{x})$ | 0 | 0 | 0 | 1 | 0 | 2 | 4 | 7 | 0 | 4 | 8 | 13 | 16 | 22 | 28 | 27 | 0 | 8 | 16 | 25 |
| $F_2(\boldsymbol{x})$ | 0 | 0 | 0 | 1 | 0 | 2 | 4 | 7 | 0 | 4 | 8 | 13 | 16 | 22 | 28 | 27 | 0 | 8 | 16 | 25 |
| $F_3(\boldsymbol{x})$ | 0 | 0 | 0 | 1 | 0 | 2 | 4 | 7 | 0 | 4 | 8 | 13 | 16 | 22 | 29 | 26 | 0 | 8 | 16 | 25 |
| $F_4(\boldsymbol{x})$ | 0 | 0 | 0 | 1 | 0 | 2 | 4 | 7 | 0 | 4 | 8 | 13 | 16 | 22 | 29 | 26 | 0 | 8 | 16 | 25 |
| $F_5(\boldsymbol{x})$ | 0 | 0 | 0 | 1 | 0 | 2 | 4 | 8 | 0 | 3 | 6 | 12 | 7 | 16 | 25 | 23 | 0 | 7 | 3 | 22 |
| $F_6(\boldsymbol{x})$ | 0 | 0 | 0 | 1 | 0 | 2 | 4 | 8 | 0 | 3 | 6 | 16 | 8 | 21 | 26 | 29 | 0 | 5 | 12 | 27 |
| $F_7(\boldsymbol{x})$ | 0 | 0 | 0 | 1 | 0 | 2 | 4 | 8 | 0 | 3 | 6 | 16 | 8 | 21 | 26 | 29 | 0 | 6 | 15 | 24 |

| $\boldsymbol{x}$ *cont.* | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | $\deg F$ | $NL_F$ | $N_F$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $F_1(\boldsymbol{x})$ *cont.* | 5 | 15 | 17 | 26 | 22 | 26 | 14 | 3 | 3 | 13 | 31 | 16 | 2 | 12 | 25 |
| $F_2(\boldsymbol{x})$ *cont.* | 5 | 15 | 17 | 26 | 27 | 23 | 3 | 14 | 14 | 0 | 18 | 29 | 2 | 12 | 25 |
| $F_3(\boldsymbol{x})$ *cont.* | 5 | 15 | 19 | 24 | 7 | 11 | 27 | 22 | 26 | 20 | 1 | 14 | 3 | 12 | 25 |
| $F_4(\boldsymbol{x})$ *cont.* | 5 | 15 | 19 | 24 | 10 | 6 | 22 | 27 | 23 | 25 | 12 | 3 | 3 | 12 | 25 |
| $F_5(\boldsymbol{x})$ *cont.* | 28 | 19 | 9 | 0 | 19 | 8 | 15 | 28 | 21 | 9 | 29 | 2 | 4 | 10 | 25 |
| $F_6(\boldsymbol{x})$ *cont.* | 20 | 6 | 31 | 16 | 7 | 31 | 8 | 22 | 9 | 26 | 17 | 11 | 3 | 12 | 25 |
| $F_7(\boldsymbol{x})$ *cont.* | 18 | 3 | 17 | 30 | 2 | 29 | 14 | 20 | 25 | 13 | 9 | 23 | 3 | 12 | 25 |

The calculated values of nonlinearity for all 7 EA-classes are the same. The resulting value exceeds the lower bound (11) by 1 and coincides with the the upper bound (6). In accordance with (4), the affinity order of all APN functions in dimension 5 is greater than or equal to 5. All APN functions from the first, second, sixth and seventh classes are AB, and from the fifth class are not AB. These 5 classes contain permutations. The third and fourth classes don't contain any permutations, but contain the AB functions found in [23].

In this case, all power functions with exponents from 1 to 30 are permutations. In order to determine whether they are APN permutations and obtain the distribution of power APN permutations over the indicated 5 classes of EA-equivalence, which is absent in [21], let's recall known results. H. Dobbertin [24] conjectured that the six known infinite families of power APN functions presented in Table 5 exhaust the entire set of power APN functions (in accordance with later works, the Niho case for $n \equiv 3 \pmod 4$ was added to the original table from [24]).

Table 5

**Known infinite families of power APN functions**

| Name | Exponent | Conditions |
|---|---|---|
| Gold | $2^k+1$ | $(k,n)=1,\ 1 \leqslant k < n/2$ |
| Kasami | $2^{2k}-2^k+1$ | $(k,n)=1,\ 2 \leqslant k < n/2$ |
| Welch | $2^{(n-1)/2}+3$ | $n$ odd |
| Niho | $2^{(n-1)/2}+2^{(n-1)/4}-1$<br>$2^{(n-1)/2}+2^{(3n-1)/4}-1$ | $n \equiv 1 \pmod 4$<br>$n \equiv 3 \pmod 4$ |
| Dobbertin | $2^{4n/5}+2^{3n/5}+2^{2n/5}+2^{n/5}-1$ | $n \equiv 0 \pmod 5$ |
| Inverse | $2^n-2$ | $n$ odd |

The power functions from the Welch and Niho families, and also in the case of odd $n$ from the Gold and Kasami families, are AB functions. At the same time, the mappings from the Dobbertin and Inverse families are not AB. All power functions from the Gold family are quadratic.

The equivalence of exponents was also discussed in [24], which is defined as follows: if a power function $x^d$ is an APN, then a power function $x^h$ is also an APN, where for $0 \leqslant i < n$ modulo comparison $h \equiv 2^i d \pmod{(2^n-1)}$ is true, and also in the case when

$x^d$ is a permutation, one more comparison $hd \equiv 2^i \pmod{(2^n - 1)}$ is true. In this sense, each exponent presented above gives in fact an equivalence class of exponents for which the power function is the APN. Unfortunately, this equivalence is sometimes forgotten to be mentioned by some authors, which narrows the reader's understanding about possible exponents of power APN functions.

Dobbertin's conjecture has not yet been proven, but it has been checked for all values of $n$ up to 34. It was shown in [25–27] that the equivalence of exponents corresponds to the CCZ-equivalence of APN functions. It follows from [21] that the first and seventh classes, as well as the second and sixth classes are CCZ-equivalent. In addition, the first class contains $x^5$, the second class contains $x^3$, the fifth class contains $x^{15}$, the sixth class contains $x^{11}$, and the seventh class contains $x^7$. Then, after calculating the equivalent exponents for the CCZ-equivalent power APN functions and knowing their algebraic degrees, we obtain the following proposition.

**Proposition 2.** All non-affine power 5-dimensional permutations are APN and the following distribution of power APN permutations over 5 classes of EA-equivalence of APN functions in dimension 5 takes place:

— exponents 5 (Gold, Niho), 9, 10, 18, 20 correspond to the first class;
— exponents 3 (Gold), 6, 12, 17, 24 correspond to the second class;
— exponents 15, 23, 27, 29 (Dobbertin), 30 (Inverse) correspond to the fifth class;
— exponents 11, 13 (Kasami), 21, 22, 26 correspond to the sixth class;
— exponents 7 (Welch), 14, 19, 25, 28 correspond to the seventh class.

For $n \geqslant 6$, the situation with finding the nonlinearity of APN functions becomes much more complicated. Firstly, a complete partition of such functions into EA-equivalence classes is currently unknown, while the number of already known EA-classes even for $n = 6$ is measured in hundreds (the most advanced results in this direction are presented in [28, 29]). Second, the complexity of computing a nonlinearity for a mapping from $P_2^{n,n}$ is $O(2^{n^2+2n})$ additive operations in the field $\mathbb{F}_{2^n}$, and thus computing such a nonlinearity for $n$ greater than or equal to 6 is itself a difficult task.

Consider a special case of the APN 6-dimensional permutation $S$ presented in [30] (Table 6).

Table 6

**APN 6-dimensional permutation**

| $\boldsymbol{x}$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $S(\boldsymbol{x})$ | 0 | 54 | 48 | 13 | 15 | 18 | 53 | 35 | 25 | 63 | 45 | 52 | 3 | 20 | 41 | 33 |
| $\boldsymbol{x}$ *cont.*1 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
| $S(\boldsymbol{x})$ *cont.*1 | 59 | 36 | 2 | 34 | 10 | 8 | 57 | 37 | 60 | 19 | 42 | 14 | 50 | 26 | 58 | 24 |
| $\boldsymbol{x}$ *cont.*2 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 |
| $S(\boldsymbol{x})$ *cont.*2 | 39 | 27 | 21 | 17 | 16 | 29 | 1 | 62 | 47 | 40 | 51 | 56 | 7 | 43 | 44 | 38 |
| $\boldsymbol{x}$ *cont.*3 | 48 | 49 | 50 | 51 | 52 | 53 | 54 | 55 | 56 | 57 | 58 | 59 | 60 | 61 | 62 | 63 |
| $S(\boldsymbol{x})$ *cont.*3 | 31 | 11 | 4 | 28 | 61 | 46 | 5 | 49 | 9 | 6 | 23 | 32 | 30 | 12 | 55 | 22 |

Permutation $S$, like the majority of known APN functions in dimensional 6, has a relatively high nonlinearity in the sense (1) equal to 24. Computer calculation of its nonlinearity gives a value 55, which exceeds the lower bound (9) by 2 and is inferior to the upper bound (6) also by 1. In accordance with (4), the affinity order of permutation $S$ is greater than or equal to 8.

The obtained values of nonlinearity for APN functions in small dimensions allow us to assume that, in contrast to the nonlinearity in the sense (1), all APN functions have the same nonlinearity.

Since there are no APN 4-dimensional permutations, let's consider further the behavior of nonlinearity for differentially 4-uniform permutations in dimension 4.

## 4. Nonlinearity of differentially 4-uniform permutations in dimension 4

From the results [22], it follows that there are 13 EA-equivalent classes of differentially 4-uniform mappings from $P_2^{4,4}$ containing 4-dimensional permutations (the second and third, fourth and twelfth, fifth and sixth EA-classes in addition are pairwise CCZ-equivalent). As in the case of APN functions, we represent these classes in the Table 7 through their canonical elements in the hexadecimal notation, with three indicators for each of them, including the nonlinearity values found here.

Table 7

**Nonlinearity of differentially 4-uniform permutations in dimension 4**

| $\boldsymbol{x}$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | $\deg F$ | $NL_F$ | $N_F$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $F_1(\boldsymbol{x})$ | 0 | 0 | 0 | 0 | 0 | 1 | 2 | 3 | 0 | 2 | 4 | 8 | 0 | 12 | 5 | 7 | 3 | 2 | 9 |
| $F_2(\boldsymbol{x})$ | 0 | 0 | 0 | 0 | 0 | 1 | 2 | 3 | 0 | 4 | 8 | 13 | 0 | 5 | 14 | 10 | 3 | 4 | 9 |
| $F_3(\boldsymbol{x})$ | 0 | 0 | 0 | 0 | 0 | 1 | 2 | 3 | 0 | 4 | 8 | 13 | 0 | 6 | 11 | 12 | 3 | 4 | 9 |
| $F_4(\boldsymbol{x})$ | 0 | 0 | 0 | 0 | 0 | 1 | 2 | 3 | 0 | 4 | 8 | 13 | 0 | 6 | 12 | 11 | 3 | 4 | 9 |
| $F_5(\boldsymbol{x})$ | 0 | 0 | 0 | 0 | 0 | 1 | 2 | 4 | 0 | 1 | 3 | 6 | 2 | 8 | 6 | 15 | 3 | 2 | 9 |
| $F_6(\boldsymbol{x})$ | 0 | 0 | 0 | 0 | 0 | 1 | 2 | 4 | 0 | 1 | 3 | 6 | 3 | 8 | 7 | 15 | 3 | 2 | 9 |
| $F_7(\boldsymbol{x})$ | 0 | 0 | 0 | 0 | 0 | 1 | 2 | 4 | 0 | 1 | 3 | 8 | 2 | 7 | 13 | 5 | 3 | 2 | 9 |
| $F_8(\boldsymbol{x})$ | 0 | 0 | 0 | 0 | 0 | 1 | 2 | 4 | 0 | 1 | 3 | 8 | 4 | 11 | 12 | 14 | 3 | 4 | 9 |
| $F_9(\boldsymbol{x})$ | 0 | 0 | 0 | 0 | 0 | 1 | 2 | 4 | 0 | 1 | 3 | 8 | 4 | 13 | 10 | 14 | 3 | 4 | 9 |
| $F_{10}(\boldsymbol{x})$ | 0 | 0 | 0 | 0 | 0 | 1 | 2 | 4 | 0 | 1 | 3 | 8 | 4 | 13 | 14 | 10 | 3 | 4 | 9 |
| $F_{11}(\boldsymbol{x})$ | 0 | 0 | 0 | 0 | 0 | 1 | 2 | 4 | 0 | 1 | 6 | 8 | 2 | 9 | 13 | 14 | 3 | 4 | 9 |
| $F_{12}(\boldsymbol{x})$ | 0 | 0 | 0 | 0 | 0 | 1 | 2 | 4 | 0 | 1 | 6 | 8 | 2 | 13 | 8 | 15 | 3 | 4 | 9 |
| $F_{13}(\boldsymbol{x})$ | 0 | 0 | 0 | 0 | 0 | 1 | 2 | 4 | 0 | 2 | 8 | 15 | 1 | 10 | 15 | 6 | 3 | 4 | 9 |

Using the results [22], it can be shown based on the number of matches of canonical elements with zero function that all EA-classes containing 4-dimensional permutations with differential uniformity greater than or equal to 6 give nonlinearity less than or equal to 9. Since, as can be seen from the Table 7, the permutations of all 13 classes have the same nonlinearity equal to 9, we can say that differentially 4-uniform permutations have the maximum possible nonlinearity in the class $S_2^4$, which exceeds the lower bound (7) by 1 and is inferior to the upper bound (6) by 2. In accordance with (4), the affinity order of all differentially 4-uniform 4-dimensional permutations, as for APN functions in this dimension, is greater than or equal to 3.

At the same time, the nonlinearity in the sense (1) for permutations of the first, fifth, sixth, and seventh classes is inferior to that for permutations of the remaining nine classes, equal to 4. The latter, as is known, is the maximum possible nonlinearity in the sense (1) for 4-dimensional permutations. Thus, we obtain the following proposition.

**Proposition 3.** There are 9 pairwise not EA-equivalent (7 pairwise not CCZ-equivalent) classes of APN functions in dimension 4 containing permutations with three optimal nonlinearity indicators, namely: $\triangle_S = 4$, $NL_S = 4$ and $N_S = 9$.

In [31], all 4-dimensional permutations with two optimal nonlinearity indicators ($\triangle_S$=4, $NL_S = 4$) were divided into 16 affine equivalence classes. We represent this partition in

terms of canonical representatives within the extended affine equivalence classes in the Table 8. The left column shows the number of the EA-class from the Table 7.

Table 8

**Classes of 4-dimensional permutations with optimal nonlinear indicators**

| No. EA-class | $\boldsymbol{x}$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | $S_1$ | 0 | 1 | 2 | 13 | 4 | 7 | 15 | 6 | 8 | 11 | 12 | 9 | 3 | 14 | 10 | 5 |
| | $S_2$ | 0 | 1 | 2 | 13 | 4 | 7 | 15 | 6 | 8 | 14 | 9 | 5 | 10 | 11 | 3 | 12 |
| 3 | $S_3$ | 0 | 1 | 2 | 13 | 4 | 7 | 15 | 6 | 8 | 11 | 14 | 3 | 5 | 9 | 10 | 12 |
| | $S_4$ | 0 | 1 | 2 | 13 | 4 | 7 | 15 | 6 | 8 | 11 | 14 | 3 | 10 | 12 | 5 | 9 |
| 4 | $S_5$ | 0 | 1 | 2 | 13 | 4 | 7 | 15 | 6 | 8 | 14 | 12 | 11 | 9 | 3 | 10 | 5 |
| 8 | $S_6$ | 0 | 1 | 2 | 13 | 4 | 7 | 15 | 6 | 8 | 14 | 12 | 9 | 5 | 11 | 10 | 3 |
| 9 | $S_7$ | 0 | 1 | 2 | 13 | 4 | 7 | 15 | 6 | 8 | 12 | 9 | 11 | 10 | 14 | 5 | 3 |
| | $S_8$ | 0 | 1 | 2 | 13 | 4 | 7 | 15 | 6 | 8 | 12 | 11 | 9 | 10 | 14 | 5 | 3 |
| 10 | $S_9$ | 0 | 1 | 2 | 13 | 4 | 7 | 15 | 6 | 8 | 12 | 14 | 11 | 10 | 9 | 3 | 5 |
| | $S_{10}$ | 0 | 1 | 2 | 13 | 4 | 7 | 15 | 6 | 8 | 14 | 11 | 10 | 5 | 9 | 12 | 3 |
| | $S_{11}$ | 0 | 1 | 2 | 13 | 4 | 7 | 15 | 6 | 8 | 14 | 11 | 10 | 9 | 3 | 12 | 5 |
| 11 | $S_{12}$ | 0 | 1 | 2 | 13 | 4 | 7 | 15 | 6 | 8 | 14 | 11 | 3 | 5 | 9 | 10 | 12 |
| | $S_{13}$ | 0 | 1 | 2 | 13 | 4 | 7 | 15 | 6 | 8 | 14 | 11 | 5 | 10 | 9 | 3 | 12 |
| 12 | $S_{14}$ | 0 | 1 | 2 | 13 | 4 | 7 | 15 | 6 | 8 | 14 | 12 | 11 | 3 | 9 | 5 | 10 |
| 13 | $S_{15}$ | 0 | 1 | 2 | 13 | 4 | 7 | 15 | 6 | 8 | 12 | 5 | 3 | 10 | 14 | 11 | 9 |
| | $S_{16}$ | 0 | 1 | 2 | 13 | 4 | 7 | 15 | 6 | 8 | 12 | 11 | 9 | 10 | 14 | 3 | 5 |

Note also that permutations from the second and third EA-classes have 3 quadratic nonzero linear combinations of coordinate functions, permutations from the fourth, eleventh and twelfth EA-classes have 1 such quadratic combination, and for permutations from the eighth, ninth, tenth and thirteenth EA-classes, all nonzero linear combinations of coordinate functions are cubic. In addition, all power 4-dimensional permutations, namely $x^7$, $x^{11}$, $x^{13}$ and $x^{14}$, are in the same thirteenth EA-class.

## 5. Conclusion

The nonlinearity of a vectorial function shows the minimum number of mismatches between its images and the images of an arbitrary affine mapping. Here we study the behavior of this nonlinearity for the class of mappings of the space $\mathbb{F}_2^n$ into itself, which have an optimal nonlinearity of a different form, namely, APN functions. For comparison and completeness, the behavior of the nonlinearity defined as the maximum nonlinearity of all nonzero combinations of coordinate functions is also given.

Among the most significant results is the lower bound on the nonlinearity of APN functions, obtained in Theorem 1 and Corollary 1. The lower bound obtained here, together with the upper bound from [15], leave a rather narrow range for possible nonlinearity values of APN functions, which is presented in Table 9 for $n \leqslant 8$.

Table 9

**Bounds on nonlinearity of APN functions**

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| Lover bound (9) or (11) | 0 | 1 | 4 | 10 | 24 | 53 | 112 | 233 |
| Exact value (Section 3) | 0 | 1 | 4 | 10 | 25 | (55) ? | ? | ? |
| Upper bound (6) | 0 | 1 | 4 | 10 | 25 | 56 | 119 | 246 |

In addition, the lower nonlinearity bound makes it possible to obtain a lower bound on the affinity order of such mappings (Corollary 2), which guarantees that in an arbitrary

piecewise affine representation of any APN function $F$ there is at least the obtained number of affinity domains. This number directly affects the complexity of solving the system of nonlinear equations given by $F$ [20].

The results obtained for the nonlinearity of APN functions in small dimension allow us to formulate some problems and make conjectures about its behavior in the general case. As has been shown, all APN functions of fixed dimension up to 5 have the same nonlinearity value (in contrast to the nonlinearity defined as the minimal nonlinearity of nonzero combinations of coordinate functions). In this regard, the following question arises.

**Problem 1.** Do all APN functions in fixed dimension really have the same nonlinearity value?

It was also shown here that all APN functions in dimension up to 5 have the maximum possible nonlinearity among all mappings in the corresponding dimension. Therefore, if the answer to the first question is yes, then the second question arises.

**Problem 2.** Is the value of the nonlinearity of APN functions the maximum possible among all mappings in the corresponding dimension?

In [7] it was conjectured that the nonlinearity of all vectorial Boolean functions from $P_2^{n,k}$ is less than or equal to $(1-2^{-k})(2^n-2^{n/2})$, and, accordingly, for $k=n$, the conjectured upper bound has the form

$$N_F \leqslant 2^n - 2^{n/2} - 1 + 2^{-n/2}. \tag{14}$$

From the results obtained above, it is easy to see that the studied 6-dimensional permutation also has a nonlinearity value coinciding with (14). In a sense, this confirms the conjecture that all APN functions have the same nonlinearity, which is the maximum possible among all mappings in corresponding dimension.

In the paper, the distribution of power APN permutations over 5 classes of EA-equivalence of APN functions in dimension 5 is obtained (Proposition 2).

All possible 9 classes of EA-equivalent differentially 4-uniform vectorial functions in dimension 4, containing permutations and having optimal two other nonlinearity indicators are also presented (Proposition 3). Using Table 7 and Table 8, it is much easier to find combinations of not EA-equivalent 4-dimensional permutations with all three optimal nonlinearity indicators.

## REFERENCES


1. *Glukhov M. M.* O priblizhenii diskretnykh funktsiy lineynymi funktsiyami [On the approximation of discrete functions by linear functions]. Matematicheskiye Voprosy Kriptografii, 2016, vol. 7, no. 4, pp. 29–50. (in Russian)
2. *Nyberg K.* On the construction of highly nonlinear permutations. LNCS, 1993, vol. 658, pp. 92–98.
3. *Nyberg K.* Differentially uniform mappings for cryptography. LNCS, 1994, vol. 765, pp. 55–64.
4. *Nyberg K. and Knudsen L. R.* Provable security against a differential attack. LNCS, 1993, vol. 740, pp. 566–574.
5. *Chen L. and Fu F.* On the nonlinearity of multi-output Boolean functions. Acta Scientiarum Naturalium Universitatis Nankaiensis, 2001, vol. 34, no. 4, pp. 28–33. (in Chinese)
6. *Liu J. and Chen L.* On nonlinearity of the second type of multi-output Boolean functions. Chinese J. Eng. Math., 2014, vol. 31, no. 1, pp. 9–22. (in Chinese)
7. *Liu J., Mesnager S., and Chen L.* On the nonlinearity of $S$-boxes and linear codes. Cryptography and Communications, 2017, vol. 9, no. 1, pp. 345–361.
8. *Nagy G. P.* Thin Sidon sets and the nonlinearity of vectorial Boolean functions. `https://arxiv.org/pdf/2212.05887.pdf`, 2022.

9. *Ryabov V. G.* O priblizhenii vektornykh funktsiy nad konechnymi polyami i ikh ogranicheniy na lineynyye mnogoobraziya affinnymi analogami [On approximation of vectorial functions over finite fields and their restrictions to linear manifolds by affine analogues]. Diskretnaya Matematika, 2022, vol. 34, no. 2, pp. 83–105. (in Russian)
10. *Ryabov V. G.* K voprosu o priblizhenii vektornykh funktsiy nad konechnymi polyami affinnymi analogami [On the question of approximation of vectorial functions over finite fields by affine analogues]. Matematicheskiye Voprosy Kriptografii, 2022, vol. 13, no. 4, pp. 125–146. (in Russian)
11. *Carlet C. and Ding C.* Nonlinearities of S-boxes. Finite Fields Appl., 2007, vol. 13, no. 1, pp. 121–135.
12. *Carlet C.* Relating three nonlinearity parameters of vectorial functions and building APN functions from bent functions. Designs Codes Cryptography, 2011, vol. 59, no. 1–3, pp. 89–109.
13. *Carlet C.* Open questions on nonlinearity and on APN functions. LNCS, 2015, vol. 9061, pp. 83–107.
14. *Carlet C.* On the properties of the Boolean functions associated to the differential spectrum of general APN functions and their consequences. IEEE Trans. Inform. Theory, 2021, vol. 67, no. 10, pp. 6926–6939.
15. *Carlet C.* Bounds on the nonlinearity of differentially uniform functions by means of their image set size, and on their distance to affine functions. IEEE Trans. Inform. Theory, 2021, vol. 67, no. 12, pp. 8325–8334.
16. *Carlet C., Heuser A., and Picek S.* Trade-offs for S-Boxes: cryptographic properties and side-channel resilience. LNSC, 2017, vol. 10355, pp. 393–414.
17. *Gorodilova A. A., Tokareva N. N., Agievich S. V., et al.* An overview of the Eight International Olympiad in Cryptography "Non-Stop University CRYPTO". Sibirskiye Elektronnyye Matematicheskiye Izvestiya, 2022, vol. 19, no. 1, pp. A.9–A.37.
18. *Hou X.* Affinity of permutations of $F_2^n$. Discrete Appl. Math., 2006, vol. 154, no. 2, pp. 313–325.
19. *Carlet C.* Vectorial Boolean functions for cryptography. In Y. Crama & P. Hammer (eds.) Boolean Models and Methods in Mathematics, Computer Science, and Engineering (Encyclopedia of Mathematics and its Applications), Cambridge, Cambridge University Press, 2010, pp. 398–470.
20. *Gorshkov S. P. and Dvinyaninov A. V.* Nizhnyaya i verkhnyaya otsenki poryadka affinnosti preobrazovaniy prostranstv bulevykh vektorov [Lower and upper bounds on the affinity order of transformations of spaces of Boolean vectors]. Prikladnaya Diskretnaya Matematika, 2013, no. 2(20), pp. 14–18. (in Russian)
21. *Brinkmann M. and Leander G.* On the classification of APN functions up to dimension five. Designs Codes Cryptography, 2008, vol. 49, no. 1–3, pp. 273–288.
22. *Brinkmann M.* Extended Affine and CCZ Equivalence up to Dimension 4. `https://eprint.iacr.org/2019/316.pdf`, 2019.
23. *Budaghyan L., Carlet C., and Pott A.* New classes of almost bent and almost perfect nonlinear polynomials. IEEE Trans. Inform. Theory, 2006, vol. 52, no. 3, pp. 1141–1152.
24. *Dobbertin H.* Almost perfect nonlinear power functions on GF($2^n$): the Niho case. Information and Computation, 1999, vol. 151, no. 1–2, pp. 57–72.
25. *Yoshiara S.* Equivalences of power APN functions with power or quadratic APN functions. J. Algebraic Combinatorics, 2016, vol. 44, no. 3, pp. 561–585.
26. *Dempwolff U.* CCZ equivalence of power functions. Designs Codes Cryptography, 2018, vol. 86, no. 3, pp. 665–692.

27. *Dempwolff U.* Correction to: CCZ equivalence of power functions. Designs Codes Cryptography, 2022, vol. 90, no. 2, pp. 473–475.
28. *Calderini M.* On the EA-classes of known APN functions in small dimensions. `https://eprint.iacr.org/2019/369.pdf`, 2019.
29. *Calderini M.* On the EA-classes of known APN functions in small dimensions. Cryptography and Communications, 2020, vol. 12, no. 5, pp. 821–840.
30. *Browning K. A., Dillon J. F., McQuistan M. T., and Wolfe A. J.* An APN permutation in dimension six. Finite Fields: Theory and Appl., 2010, pp. 33–42.
31. *Leander G. and Poschmann A.* On the classification of 4 bit S-boxes. LNCS, 2007, vol. 4547, pp. 156–176.