Noname manuscript No.
(will be inserted by the editor)

The classification of quadratic APN functions in 7 variables

Konstantin Kalgin · Valeriya Idrisova

Received: date / Accepted: date

Abstract Almost perfect nonlinear functions possess the optimal resistance to the differential cryptanalysis and are widely studied. Most known APN functions are obtained as functions over finite fields $GF(2^n)$ and very little is known about combinatorial constructions of them in $\mathbb{F}_2^n$. In this work we propose two approaches for obtaining quadratic APN functions in $\mathbb{F}_2^n$. The first approach exploits a secondary construction idea, it considers how to obtain a quadratic APN function in $n+1$ variables from a given quadratic APN function in n variables using special restrictions on new terms. The second approach is searching quadratic APN functions that have matrix form partially filled with standard basis vectors in a cyclic manner. This approach allowed us to find a new APN function in 7 variables. We proved that the updated list of quadratic APN functions in dimension 7 is complete up to CCZ-equivalence.

Keywords Boolean function · APN function · quadratic function · differential uniformity · S-box

The work is supported by Mathematical Center in Akademgorodok under agreement No. 075-15-2019-1613 with the Ministry of Science and Higher Education of the Russian Federation and Laboratory of Cryptography JetBrains Research. We are grateful to the Supercomputing Center of the Novosibirsk State University for provided computational resources.

Konstantin Kalgin
Sobolev Institute of Mathematics,
Institute of Computational Mathematics and Mathematical Geophysics of the Siberian Branch of the RAS,
Novosibirsk State University, Novosibirsk, Russia
E-mail: kalginkv@gmail.com

Valeriya Idrisova
Sobolev Institute of Mathematics, Novosibirsk, Russia
E-mail: vvitkup@yandex.com

1 Introduction

Vectorial Boolean functions play the crucial role for protecting block ciphers against various kinds of attacks. Functions that show an optimal resistance to the differential attack are called almost perfect nonlinear (APN) functions. APN functions are widely studied by many researchers, but there is still a significant list [16] of important open questions, such as lower and upper bounds on the number of APN functions, an upper bound on algebraic degree of an APN function [8], the existence of bijective APN functions in even dimensions, etc. To find secondary constructions of APN functions is a well known open problem, in particular, it was stated as Problem 3.8 in [16]. Another problem is to find new APN functions in vectorspace $\mathbb{F}_2^n$, since, to the best of our knowledge all the known constructions of this class are found only as polynomials over the finite fields, and there are only a few combinatorial approaches to search for APN functions over $\mathbb{F}_2^n$. To find a classification of APN functions is a hard open problem. The complete classification was obtained for APN functions up to 5 variables, also, quadratic and cubic APN functions were classified for dimension 6.

This paper is devoted to methods of searching for APN functions and to corresponded problems. We investigate a few combinatorial approaches to search for almost perfect nonlinear functions, in particular, quadratic APN functions. Moreover, we provide the complete classification of quadratic APN functions in dimension 7. Generally, quadratic APN functions are not suitable as secure S-boxes due to the low algebraic degree, but obtaining new quadratic representatives can lead us to another useful functions, we discuss it in this work as well. This is especially important for even $n \geqslant 8$, since new APN permutations CCZ-equivalent to quadratic functions can be found for these dimensions [6].

We start in Section 2 by considering necessary definitions, discussing relevant open problems and observing some results in this area. Further, we propose two approaches for generating quadratic APN functions in $\mathbb{F}_2^n$. The first approach is described in Section 3. It considers the algebraic normal form of a given quadratic APN function G in n variables and extends it into an ANF of a quadratic function F in $n+1$ variables, using special restrictions on coefficients of new terms. In Section 4 we propose another method to generate quadratic APN functions, so-called, cyclic approach. In this method we consider special matrices that are partially filled with vectors of standard basis and search for corresponding APN functions using the same idea of restrictions. Using this approach we found one previously unknown (in the sense of CCZ-equivalence) quadratic APN function for $n = 7$. In Section 5 we show that the updated list of quadratic APN functions in 7 variables is complete up to CCZ-equivalence. Thus, there exist exactly 488 CCZ-equivalence classes of APN functions that contains quadratic functions in 7 variables. In Section 6.1 we observe that quadratic parts of many non-quadratic APN functions have a low differential uniformity. We introduce the new notion of stacked APN function and found such functions in dimensions up to 6 using quadratic APN functions obtained with approaches mentioned above.

2 Preliminaries

2.1 Definitions

Let us recall some definitions. Let $\mathbb{F}_2^n$ be the n-dimensional vector space over $\mathbb{F}_2$. A function F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$, where n and m are integers, is called a *vectorial Boolean function.* If $m = 1$ such a function is called *Boolean.* Every vectorial Boolean function F can be represented as an ordered set of m *coordinate functions* $F = (f_1, \dots, f_m)$, where f_i is a Boolean function in n variables. Any vectorial function F can be represented uniquely in its *algebraic normal form (ANF)*:

$$F(x) = \sum_{I \in \mathcal{P}(N)} a_I \Big(\prod_{i \in I} x_i \Big),$$

where $\mathcal{P}(N)$ is a power set of $N = \{1, \dots, n\}$ and $a_I \in \mathbb{F}_2^m$. The *algebraic degree* of a given function F is the degree of its ANF: deg (F) =max$\{|I| : a_I \neq 0, I \in \mathcal{P}(N)\}$. If algebraic degree of a function F is not more than 1 then F is called *affine.* If for an affine function F it holds $F(\mathbf{0}) = \mathbf{0}$ then F is called *linear.* If algebraic degree of a function F is equal to 2 then F is called *quadratic.*

Let us further consider the case $m = n$ only. It is well known that we can put the finite field $GF(2^n)$ in one-to-one correspondence to the vector space $\mathbb{F}_2^n$ and consider vectorial Boolean functions as functions over $\mathbb{F}_{2^n}$. Then any vectorial function F has the unique *univariate polynomial representation* over $GF(2^n)$:

$$F(x) = \sum_{i=0}^{2^n-1} \lambda_i x^i, \;\; \lambda_j \in \mathbb{F}_{2^n}.$$

2.2 APN functions

Let F be a vectorial Boolean function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. For vectors $a, b \in \mathbb{F}_2^n$, where $a \neq 0$, consider the value

$$\delta(a,b) = \big|\{ \; x \in \mathbb{F}_2^n \;\big|\; F(x+a) + F(x) = b\}\big|.$$

Denote by Δ_F the following value:

$$\Delta_F = \max_{a \neq \mathbf{0}, \; b \in \mathbb{F}_2^n} \delta(a,b).$$

Then F is called *differentially Δ_F-uniform* function. The smaller the parameter Δ_F, the better the resistance of a cipher containing F as an S-box

Table 1 Known APN power functions x^d on $GF(2^n)$.

Functions	Exponents	Conditions	References
Gold	$d = 2^t + 1$	$\gcd(t, n) = 1$	[25], [36]
Kasami	$d = 2^{2t} - 2^t + 1$	$\gcd(t, n) = 1$	[33], [32]
Welch	$2^t + 3$	$n = 2t + 1$	[15], [20]
Niho	$2^t + 2^{\frac{t}{2}} - 1$, t even $2^t + 2^{\frac{3t+1}{2}} - 1$, t odd	$n = 2t + 1$	[21], [30]
Inverse	$2^{2t} - 1$	$n = 2t + 1$	[2], [36]
Dobbertin	$2^{4t} + 2^{3t} + 2^{2t} + 2^t - 1$	$n = 5t$	[22]

to differential attack. For the vectorial functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ the minimal possible value of Δ_F is equal to 2. In this case the function F is called *almost perfect nonlinear (APN)*. This notion was introduced by K. Nyberg in [36], also differential properties of vectorial functions were investigated (see [28] of of M. M. Glukhov) in USSR behind closed doors. APN functions are of central interest in the area of vectorial Boolean functions and draw attention of many researchers. Exhaustive discussion of the topic can be found in reviews [4] of C. Blondeau and K. Nyberg, [16] of C. Carlet, [28] of M. M. Glukhov, [37] of A. Pott, [38] of M. E. Tuzhilin, in books [7] of L. Budaghyan, [17] of C. Carlet etc.

Most known APN functions are monomial functions over $GF(2^n)$, they are provided in Table 1. Also, there exist many constructions and infinite families of APN functions over finite fields (for example, see papers [9], [10], [11], [12] and [13] of L. Budaghyan et al., [24] of Y. Edel et al., etc.). There were proposed several combinatorial approaches how to search new APN functions from known ones. In work [23] of Y. Edel and A. Pott there was proposed so-called switching method that searches for suitable coordinate functions in order to obtain a new APN function from a given one. A combinatorial approach using subfunctions was proposed in [26] of A. Gorodilova. An approach for finding APN permutations using 2-to-1 APN functions was introduced in [31] of V. Idrisova.

2.3 Classifications of APN functions

Let us remind main relationships of equivalence that preserve an APN property of a given vectorial function. Two vectorial functions F and G are *extended affinely equivalent (EA-equivalent)* if $F = A_1 \circ G \circ A_2 + A$ where A_1, A_2 are affine permutations on $\mathbb{F}_2^n$ and A is an affine function. Two functions F and G are called *Carlet-Charpin-Zinoviev [18] equivalent (CCZ-equivalent)* if their graphs $\{(x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \mid y = F(x)\}$ and $\{(x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \mid y = G(x)\}$ are affinely equivalent, that is, if there exists an affine automorphism $A = (A_1, A_2)$ of $\mathbb{F}_2^n \times \mathbb{F}_2^n$ such that $y = F(x) \Leftrightarrow A_2(x, y) = G(A_1(x, y))$. Let us recall that in case of quadratic APN functions, CCZ-equivalence coincides with EA-equivalence [39]. In [18] there was introduced the associated Boolean function $\gamma_F(a, b)$ in $2n$ variables for a given vectorial Boolean function F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. It takes value 1 if a is nonzero and equation $F(x)+F(x+a) = b$ has solutions, and 0 otherwise. Two functions F and G are called *differentially equivalent* if $\gamma_F = \gamma_G$. This notion of equivalence was introduced by A. Gorodilova in [27].

To find the complete classification of APN functions under CCZ-equivalence is complicated open question. A complete classification for APN functions was found by M. Brinkmann and G. Leander in [5] only up to $n = 5$. When $n = 6$ APN functions classified only for degrees up to 3 (the list can be found in [5] and the complete classification of cubics was described by P. Langevin in [35]). Also, in paper [14] of M. Calderini EA-classes of all known APN functions in 6 variables were provided as well as partial results for 7, 8 and 9 variables. Moreover, the classification up to $n = 9$ was obtained in [41] of Y. Yu et al. for quadratic APN functions over $GF(2^n)$ with coefficients from $GF(2)$. Until recently there were known 487 CCZ-classes of quadratic APN functions in 7 variables and 8179 CCZ-classes of quadratic APN functions in 8 variables, most of them were found in [40] of Y. Yu et al. However, in the very recent breakthrough work [1] of C. Beierle and G. Leander there were found 12923 new quadratic APN functions in dimension 8, 35 new quadratic APN functions in dimension 9 and five new quadratic APN functions in dimension 10 (all are different up to CCZ-equivalence). In the conference version of this paper [34] we found a new APN function in 7 variables, later this function was also independently found in [1].

3 On secondary approach to search for quadratic APN functions

Since EA-equivalence preserves the APN property, it is always possible to omit linear and constant terms in the algebraic normal form of a given APN function. We shall then consider quadratic vectorial Boolean functions that have only quadratic terms in their ANF. The following result of T. Beth and C. Ding gives a necessary condition on the ANF of a given APN function.

Theorem 1 *(see Theorem 6 in [2]) Let $F = (f_1, \ldots, f_n)$ be an APN function in n variables. Then every quadratic term $x_i x_j$, where $i \neq j$, appears at least in one coordinate function of F.*

This property motivated us to suggest the following construction of quadratic APN functions. Let $G = (g_1, \ldots, g_n)$ be a quadratic APN-function in n variables. Consider vectorial function $F = (f_1, \ldots, f_n, f_{n+1})$ in $n + 1$ variables such that:

$$\begin{aligned} &f_1 = g_1 + \sum_{i=1}^{n} \alpha_{1,i} x_i x_{n+1};\\ &\dots\\ &f_n = g_n + \sum_{i=1}^{n} \alpha_{n,i} x_i x_{n+1};\\ &f_{n+1} = g_{n+1} + \sum_{i=1}^{n} \alpha_{n+1,i} x_i x_{n+1}, \end{aligned} \tag{1}$$

where $\alpha_{1,i} \dots, \alpha_{n+1,i} \in \mathbb{F}_2$ for $i = 1, \dots, n$ and $g_{n+1} = \sum_{1 \leqslant j < k \leqslant n} \beta_{j,k} x_j x_k$ for some fixed $\beta_{j,k} \in \mathbb{F}_2$. Note that if $\alpha_{1,i}, \dots, \alpha_{n,i}$ are such that each term $x_i x_{n+1}$ appears at least in one of the coordinate functions $f_1, \dots, f_n$, then the necessary condition of Theorem 1 is held for the constructed function F. Since the exhaustive search for the given APN function becomes complicated starting from $n = 6$, there is a need to find necessary and sufficient conditions on new coefficients of F.

Let us denote the lexicographically ordered elements of $\mathbb{F}_2^n$ as $x^0, \dots, x^{2^n-1}$. Since all the values $G(x^0), \dots, G(x^{2^n-1})$ of the function G are known, we can represent values of the constructed function F only through unknown coefficients $\alpha_{i,k}$ and some constant terms. Since F is an APN function, for a nonzero a all sums $F(x) + F(x + a)$ and $F(y) + F(y + a)$, where $x \neq y$ and $x \neq y + a$, should be pairwise different. This fact applies special restrictions on coefficients $\alpha_{i,k}$. For the convenient representation of these restrictions further we consider the following matrix approach that was also proposed by T. Beth and C. Ding in [2].

Each quadratic vectorial function G in n variables can be considered as a symmetric matrix $\mathcal{G} = (g_{ij})$, where each element $g_{ij} \in \mathbb{F}_2^n$ is a vector of coefficients corresponding to term $x_i x_j$ in the algebraic normal form of G and all diagonal elements g_{ii} are null.

Example 1 Let us consider function $G = (g_1, g_2, g_3) = (x_1x_2, x_2x_3, x_1x_3) = \begin{bmatrix}1\\0\\0\end{bmatrix} \cdot x_1x_2 + \begin{bmatrix}0\\0\\1\end{bmatrix} \cdot x_1x_3 + \begin{bmatrix}0\\1\\0\end{bmatrix} \cdot x_2x_3$.

Then the corresponding matrix $\mathcal{G}$ is the following:

$$\mathcal{G} = \begin{bmatrix} (000) & (100) & (001)\\ (100) & (000) & (010)\\ (001) & (010) & (000) \end{bmatrix}$$

It is necessary to mention that these matrices also were used in [40] and [41] to construct and classify a lot of new quadratic APN functions over finite fields. Using these matrices the APN property can be formulated in the following way:

Proposition 1 *Let $\mathcal{G}$ be the matrix that corresponds to quadratic vectorial function G. Then function G is APN if and only if $x \cdot (\mathcal{G} \cdot a) \neq 0$ for all $x \neq a$, where $a, x \in \mathbb{F}_2^n$ and $a \neq 0$.*

Proof The proof follows directly from the Theorem 10 of [2], which states that G is APN if and only if $rank(\mathcal{G} \cdot a)$ is equal to $n-1$ for any nonzero $a \in \mathbb{F}_2^n$.

In terms of matrices method (1) can be considered as an extension of a given $\mathcal{G}$ with an extra bit that represents g_{n+1} in every element and an extra pair of row and column that represents a set of new terms $x_i x_{n+1}$.

Example 2 For the considered function $G = (g_1, g_2, g_3) = (x_1x_2, x_2x_3, x_1x_3)$ we choose null g_{n+1} and construct APN function $F = (f_1, f_2, f_3, f_4)$ in 4 variables, where:
$f_1 = g_1$;
$f_2 = g_2 + x_3x_4$;
$f_3 = g_3 + x_2x_4 + x_3x_4$;
$f_4 = x_1x_4 + x_3x_4$.
Then the corresponding matrix $\mathcal{F}$ is the following:

$$\mathcal{F} = \begin{bmatrix} (0000) & (1000) & (0010) & (0001) \\ (1000) & (0000) & (0100) & (0010) \\ (0010) & (0100) & (0000) & (0111) \\ (0001) & (0010) & (0111) & (0000) \end{bmatrix}$$

The next result directly follows from the Proposition 1 and an almost identical property was described as main idea of Algorithm 1 in [40]. Consider a quadratic APN function G and the corresponding $n \times n$ matrix $\mathcal{G}$. Denote the vector of nonzero coefficients for new variables as $\alpha = (\alpha_1, \ldots, \alpha_n)$, where $\alpha_i \in \mathbb{F}_2^{n+1}$. Let us fix g_{n+1} and construct $(n+1) \times (n+1)$ matrix $\mathcal{F}$ by adding $(\alpha_1, \ldots, \alpha_n, 0)$ to $\mathcal{G}$ as the last column and the last row and adding new bit to every element of $\mathcal{G}$ according to the choice of g_{n+1}. Let us denote as $\mathcal{G}'$ the submatrix (f_{ij}) of $\mathcal{F}$, such that $i, j < n+1$. Let $\langle X \rangle$ denote the linear span of an arbitrary set $X \subseteq \mathbb{F}_2^n$ and F be the quadratic vectorial function corresponding to the constructed matrix $\mathcal{F}$. Then the following proposition is true.

Proposition 2 *F is APN if and only if $\alpha \cdot a'$ does not belong to $\langle \mathcal{G}' \cdot a' \rangle$ for all $a' \in \mathbb{F}_2^n$, $a' \neq \boldsymbol{0}$.*

Remark 1 Let us note that Proposition 2 exactly shows how to obtain restrictions on new coefficients in the convenient form. Our algorithm for searching APN functions using these restrictions is very similar to Algorithm 1 in [40], but in our work we start from an APN function matrix $n \times n$, add an extra bit to each element that is corresponding to g_{n+1} and search through all possible last column in order to build an APN function matrix $(n+1) \times (n+1)$. In work [40] the authors started from an APN function matrix $n \times n$ and searched through all possible last column (or more columns) in order to build an APN function matrix $n \times n$.

Let us show that our method can be also extended to the case when G is not an APN function, but the ANF of G and g_{n+1} together contain all possible quadratic terms. The following proposition describes the necessary condition on the choice of such functions.

Proposition 3 *Let G be a quadratic vectorial function in n variables and F be an APN function in $n+1$ variables that it is obtained from G using method (1). Then $\Delta_G \leqslant 4$.*

Proof Consider vectorial function $F = (f_1, \dots, f_{n+1})$ that is obtained from vectorial function $G = (g_1, \dots, g_n)$ using method (1). Then for all arguments $x = (x_1, \dots, x_{n+1})$ such that $x_{n+1} = 0$ holds $F(x) = (g_1, \dots, g_n, g_{n+1})$, where g_{n+1} is a coordinate function that was added according to the method. Since function $F(x)$ is APN for all nonzero $a = (a_1, \dots, a_{n+1})$ such that $a_{n+1} = 0$ and any $b \in \mathbb{F}_2^{n+1}$ equation $F(x) + F(x+a) = b$ has no more than 2 solutions among x such that $x_{n+1} = 0$. Therefore, for any nonzero $a = (a_1, \dots, a_n)$ and any $b \in \mathbb{F}_2^n$ equation $G(x) + G(x+a) = b$ has no more than 4 solutions and G is APN or differentially 4-uniform.

For example, for differentially 4-uniform function $G = (g_1, g_2, g_3, g_4, g_5)$, where:

$g_1 = x_1x_2 + x_3x_5 + x_4x_5;$
$g_2 = x_1x_3 + x_4x_5;$
$g_3 = x_2x_3 + x_1x_4 + x_3x_5 + x_4x_5;$
$g_4 = x_2x_4 + x_1x_5 + x_4x_5;$
$g_5 = x_3x_4 + x_2x_5 + x_4x_5.$

and g_6 contains all the terms x_ix_j, where $i < j \leqslant n$, we obtained 13 CCZ classes of APN functions among constructed functions. Let us recall that there exist only 13 CCZ classes of quadratic APN functions in dimension 6.

Remark 2 It can be seen that any quadratic APN function in n variables can be obtained using method (1) from quadratic APN or differential 4-uniform function in $n-1$ variables .

It is also worth mentioning that when $n = 3, 4$ and 5 for APN functions that are CCZ classes representatives we obtained all the possible classes of quadratic APN functions for $4, 5$ and 6 variables from the classification [5] and large variety of classes for constructing from 6 to 7 variables.

Note that for the given APN function G in n variables we have $2^{\frac{(n^2-n)}{2}}$ possibilities to choose g_{n+1}. It is interesting that the choice of g_{n+1} affects the capability to obtain APN function F in $n+1$ variables, the number of such constructed functions and the variety of different CCZ-classes among constructed classes. For example, when $n = 5$ and g_{n+1} is null both quadratic CCZ-representatives give us the only one CCZ-class for 6 variables (class 11 in the list from [5]). At the same time, when g_{n+1} contains all quadratic terms x_ix_j, these functions give 13 CCZ-classes of quadratic APN functions in 6 variables. Unfortunately, for $n \geqslant 7$ it becomes computationally harder to choose the proper initial function and g_{n+1} and to obtain a large amount of generated functions. It seems that method (1) is not so efficient on large dimensions.

OPEN QUESTION Q1: How to choose properly the initial function G in this approach? It seems that for most APN functions in n variables it is possible to find corresponding APN functions in $n+1$ variables for some g_{n+1}, but we have found one counterexample for $n = 6$.

OPEN QUESTION Q2: Given APN (or differentially 4-uniform) function G, how to choose function g_{n+1} such that the number of classes of obtained APN functions is maximal?

4 On cyclic approach to search for quadratic APN functions

As noted earlier, each row/column of a symmetric matrix that is corresponding to an APN function in n variables consists of $n-1$ linear independent vectors from $\mathbb{F}_2^n$. In this section we consider, in some sense, the minimal values for such vectors, using basis vectors for filling the matrix. Let us introduce another approach for constructing quadratic APN functions using matrix representation from previous section. Let $e_1, \ldots, e_n$ be the standard basis in $\mathbb{F}_2^n$. For the given n consider the following matrix with elements from $\mathbb{F}_2^n$:

$$\mathcal{T} = \begin{bmatrix} 0 & e_1 & e_2 & e_3 & \ldots & e_{n-2} & e_{n-1} \\ e_1 & 0 & e_3 & e_4 & \ldots & e_{n-1} & e_n \\ e_2 & e_3 & 0 & e_5 & \ldots & e_n & t_{3,n} \\ e_3 & e_4 & e_5 & 0 & \ldots & t_{4,n-1} & t_{4,n} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ e_{n-2} & e_{n-1} & e_n & t_{n-1,4} & \ldots & 0 & t_{n-1,n} \\ e_{n-1} & e_n & t_{n,3} & t_{n,4} & \ldots & t_{n,n-1} & 0 \end{bmatrix},$$

where $t_{i,j} = t_{j,i}$ and $t_{i,j}$ denote some unknown elements in $\mathbb{F}_2^n$. Our aim is to find values of missed matrix elements such that matrix $\mathcal{T}$ represents APN function. We can apply the approach with restrictions from the previous section.

Let us consider the following procedure.

1. Without loss of generality consider the first unknown element of matrix $\mathcal{T}$ that is $t_{3,n}$. According to Proposition 2 the last column of $\mathcal{T}$ should satisfy $(e_{n-1}, e_n, t_{3,n}, \ldots, 0) \cdot a' \notin \langle \mathcal{T}' \cdot a' \rangle$, where $a' \in \mathbb{F}_2^{n-1}$, $a' \neq 0$ and $\mathcal{T}' = \mathcal{T} \setminus (e_{n-1}, e_n, t_{3,n}, \ldots, 0)$.
2. We consider all $a' = a'_1, \ldots, a'_{n-1}$ such that $a'_3 = 1$ and $a'_i = 0$, if $i > 3$, and obtain restrictions on the value of $t_{3,n}$ that are independent from any other unknown element of $\mathcal{T}$.

Repeating this procedure step by step for every new element after fixing values of previous variables $t_{i,j}$ allows us to obtain all possible fillings for the given matrix $\mathcal{T}$.

For $n = 3, 4$ and 5 this construction covered all quadratic CCZ classes of APN functions. For $n = 6$ it covered 11 out of 13 classes. Unfortunately, for larger dimensions the number of generated functions dropped dramatically and the construction covers only 7 classes for $n = 7$ and the only one class for $n = 8$. As a consequence, we consider the following generalization of this construction.

Let $\mathcal{T}$ be the same matrix that contains k unknown elements. Consider the diagonal that contains all elements e_n in $\mathcal{T}$. It is easy to see that we can remove any element e_n from this diagonal and apply the above procedure to the new matrix with $k + 1$ unknown elements. Moreover, we can remove any number of elements from $\mathcal{T}$ and the more elements are deleted the more APN functions can be constructed using this matrix.

For $n = 6$ when we removed one element e_n from the diagonal in $\mathcal{T}$ the new matrix had already covered all 13 CCZ classes of quadratic APN functions. For $n = 7$ and the matrix that has no elements e_n on the diagonal we generated more than 2 millions of quadratic APN functions. We have found a new CCZ class for $n = 7$ among obtained functions. Here we provide a representative of this class in the univariate form:

$F(x) = a^{100}x + a^{88}x^2 + a^{89}x^3 + a^{107}x^4 + a^{57}x^5 + a^{98}x^6 + a^{56}x^8 + a^9x^9 + a^{58}x^{10} + a^{60}x^{12} + a^{109}x^{16} + a^{47}x^{17} + a^{44}x^{18} + a^{27}x^{20} + a^{91}x^{24} + a^{71}x^{32} + a^{96}x^{33} + a^{101}x^{34} + a^7x^{36} + a^{12}x^{40} + a^{34}x^{48} + a^{66}x^{64} + a^4x^{65} + a^4x^{66} + a^{73}x^{68} + a^{73}x^{72} + a^{56}x^{80} + a^{20}x^{96}$,

where a is the primitive element whose minimal polynomial over $\mathbb{F}_{2^7}$ is $x^7 + x + 1$.

We also computed CCZ-invariants ($\mathit{\Delta}$-rank and $\mathit{\Gamma}$-rank) for this new function. We provide these values in the table below.

Table 2 Invariants of the new APN function.

$\mathit{\Gamma}$-rank	$\mathit{\Delta}$-rank
4044	212

5 Classification of quadratic APN functions in dimension 7

Let us recall that APN functions are classified only up to $n = 5$ and up to degree 3 for the case $n = 6$. Here we show that there is no quadratic APN functions in 7 variables other than known ones.

A quadratic APN function F is given, let $\mathcal{F}$ be it's corresponding symmetric matrix. It is easy to see that the first row of $\mathcal{F}$ is equal to $(0\ \ 1\ \ 2\ \ 4\ \ 8\ \ 16\ \ 32)$ up to EA-equivalence. It was shown in [40] (see Corollary 1) that if APN functions F and G are EA-equivalent, then for their matrices $\mathcal{F}$ and $\mathcal{G}$ the following relation hold:

$$\mathcal{G} = L(P\mathcal{F}P^t),$$

where P is a bijective matrix with elements from $\mathbb{F}_2$ and L is a linear permutation on $\mathbb{F}_2^n$. Let us briefly describe the procedure of finding lexicographically minimal matrix in the EA-class. Our aim is to transform first k (for $n = 7$ we considered case $k = 2$) rows of a given matrix in order to obtain lexicographically minimal ones using only transformations that are preserve EA-equivalence.

For all possible first two rows of matrices $\mathcal{F}$ such that the condition from Proposition 1 is true we implement the search through all possible matrices P of the form:

$$\mathcal{P} = \begin{bmatrix} x & x & 0 & 0 & 0 & 0 & 0 \\ x & x & 0 & 0 & 0 & 0 & 0 \\ * & * & x & x & x & x & x \\ * & * & x & x & x & x & x \\ * & * & x & x & x & x & x \\ * & * & x & x & x & x & x \\ * & * & x & x & x & x & x \end{bmatrix},$$

where upper left square 2×2 and lower right square 5×5 are bijective matrices and lower left part can be any matrix 5×2. We consider such matrices P since our aim is to find minimal first two rows for a given EA-class and we do not want a diffusion of first two rows with the rest of the rows. For each matrix P we:

P1: Search through all possible L such that first row of $\mathcal{G}$ is equal to $(0\ \ 1\ \ 2\ \ 4\ \ 8\ \ 16\ \ 32)$;

P2: If P and L are such that $\mathcal{G} < \mathcal{F}$ lexicographically, we discard $\mathcal{F}$.

We implemented the above procedure and obtained that there are only five possible options for the second row of a given quadratic matrix up to the EA-equivalence. We list below these options and the number of inequivalent APN functions that have such a lexicographically minimal matrix:

1. Case $(1\ \ 0\ \ 4\ \ 8\ \ 16\ \ 32\ \ 64)$ contains 3 quadratic APN functions up to EA-equivalence (all are equivalent to monomial functions);
2. Case $(1\ \ 0\ \ 4\ \ 6\ \ 16\ \ 32\ \ 64)$ contains 2 functions;
3. Case $(1\ \ 0\ \ 4\ \ 6\ \ 16\ \ 32\ \ 24)$ contains no functions;
4. Case $(1\ \ 0\ \ 4\ \ 6\ \ 16\ \ 26\ \ 64)$ contains 220 functions;
5. Case $(1\ \ 0\ \ 4\ \ 6\ \ 16\ \ 24\ \ 64)$ contains 263 functions.

Thus, there exist only 488 quadratic APN functions up to CCZ-equivalence and the updated list is complete.

For $n = 8$ we implemented the procedure as well and there exist 11 possible options for the second row of a given quadratic matrix (while the first row is equal to $(0\ \ 1\ \ 2\ \ 4\ \ 8\ \ 16\ \ 32\ \ 64)$):

1. Case $(1\ \ 0\ \ 4\ \ 8\ \ 16\ \ 32\ \ 64\ \ 128)$;
2. Case $(1\ \ 0\ \ 4\ \ 8\ \ 16\ \ 32\ \ 64\ \ 18)$;

3. Case (1 0 4 8 16 32 64 6);
4. Case (1 0 4 6 16 32 64 128);
5. Case (1 0 4 6 16 32 64 24);
6. Case (1 0 4 8 16 32 24 128);
7. Case (1 0 4 8 16 26 64 128);
8. Case (1 0 4 8 16 26 64 104);
9. Case (1 0 4 8 16 24 64 128);
10. Case (1 0 4 8 16 24 64 98);
11. Case (1 0 4 8 16 24 64 96).

The number of inequivalent APN functions for each case are being computed at the moment.

6 The use of quadratic functions to search for APN fuctions of higher degrees

In this section we disscuss possible approaches of the use of quadratic functions with low differential uniformity to search for APN fuctions of higher degrees. Also, we introduce the notion of stacked APN functions as APN functions of algebraic degree d such that eliminating monomials of degrees $k+1,\ldots,d$ for any $k<d$ results in APN function of degree k.

6.1 The differential uniformity of quadratic parts of APN functions and the class of stacked APN functions

Let F be a vectorial Boolean function of algebraic degree d. Then it can be represented as sum $F = F^{(c)} + F^{(1)} + F^{(2)} + \ldots + F^{(d)}$, where each function $F^{(j)}$ contains only monomials of algebraic degree j and $F^{(c)}$ is a constant term. We observed that if F is an APN function then its quadratic part $F^{(2)}$ has a low differential uniformity. In particular, the following proposition was computationally proven:

Proposition 4 *Let F be an APN function in 4 variables. Then $\varDelta_{F^{(2)}} \leqslant 4$.*

Many APN functions in $5, 6$ and 7 variables have a quadratic part with differential uniformity not more than 4. For Dillon (see Dillon) permutation P of $\mathbb{F}_2^n$ value $\varDelta_{P^{(2)}}$ is equal to 8. When $n = 8, 9$ there also exist APN functions F (e.g. Kasami power functions for $n = 8$ and Inverse function for $n = 9$) such that $\varDelta_{F^{(2)}} = 8$. Nevertheless, for these large dimensions the differential uniformity of quadratic parts is still quite low. Further we consider only functions without affine terms. The observation on low differential uniformity of quadratic parts of APN functions motivated us to introduce a new subclass of APN functions.

Definition 1 Let $F = F^{(2)}+\ldots+F^{(d)}$ be an APN function of algebraic degree d. If all functions $F - F^{(d)}$, $F - F^{(d)} - F^{(d-1)}, \ldots, F - F^{(d)} - F^{(d-1)} - \ldots - F^3$ are APN functions then F is called a *stacked APN function.*

Let us describe one of the possible approaches to construct stacked APN functions of degree 3. Let h be a cubic Boolean function in n variables with no affine or quadratic terms, i.e. homogenous one. Let us call vectorial function H a *cubic shift* if $H = h \cdot v$ for a nonzero vector v in $\mathbb{F}_2^n$. In work [23] of Y. Edel and A. Pott there was introduced a new approach for searching APN functions, so-called *the switching method.* It describes how to find new APN function from known one by changing it's coordinates functions. In particular, the following result for functions of the form $F + f \cdot v$ was obtained.

Theorem 2 *(Theorem 3 in [23]) Let F be an APN function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. Let v be a nonzero vector in $\mathbb{F}_2^n$, and h be a Boolean function in n variables. Then function $F + h \cdot v$ is an APN if and only if*

$$h(x) + h(x + a) + h(y) + h(y + a) = 0$$

for all x, y, a such that

$$F(x) + F(x + a) + F(y) + F(y + a) = 0$$

and $x \neq y$, $x \neq y + a$.

Proposition 5 *Let F be an APN function in n variables. Let v be a nonzero vector in $\mathbb{F}_2^n$, and h_1, h_2 be different Boolean functions in n variables. If both functions $F + h_1 \cdot v$ and $F + h_2 \cdot v$ are APN functions, then function $F + h_1 \cdot v + h_2 \cdot v$ is also APN.*

Proof This property directly follows from the Theorem 2 since if

$$h_1(x) + h_1(x + a) + h_1(y) + h_1(y + a) = 0$$

and

$$h_2(x) + h_2(x + a) + h_2(y) + h_2(y + a) = 0$$

for all x, y, a such that

$$F(x) + F(x + a) + F(y) + F(y + a) = 0$$

and $x \neq y$, $x \neq y + a$, then

$$h_1(x)+h_2(x)+h_1(x+a)+h_2(x+a)+h_1(y)+h_2(y)+h_1(y+a)+h_2(y+a) = 0$$

for these x, y, a either. Therefore, $F + h_1 \cdot v + h_2 \cdot v$ is also an APN function.

The next simple corollary follows from Proposition 5 and allows us to potentially reduce the search of cubic shifts.

Corollary 1 *Let F be a quadratic APN function in n variables. Suppose that there exist homogenous cubic Boolean functions h_1, h_2 such that both functions $F + h_1 \cdot v$ and $F + h_2 \cdot v$ are APN. Therefore, there exist Boolean function h, where $h = h_1$ or $h = h_2$ or $h = h_1 + h_2$, such that h contains even (or, equivalently, odd) number of monomials and $F + h \cdot v$ is an APN function.*

For $n = 4, 5$ we implemented the search of cubic APN functions $F = F^{(2)} + F^{(3)}$ such that $F^{(3)}$ is some cubic part and $F^{(2)}$ is an APN quadratic function, that is constructed using the cyclic matrix $\mathcal{T}$ from the previous section. For $n = 6$ we implemented the similar search, but $F^{(3)}$ was a cubic shift since it is computationally hard to search through all the possible cubic parts. We have found a large amount of cubic stacked APN functions for $n = 4, 5, 6$. Some examples are listed in Table 3.

Table 3 Examples of stacked cubic APN functions (both F and $F^{(2)}$ are APN).

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

It is worth mentioning that for quadratic APN functions from different CCZ classes for $n = 6$ we have found more than 70 000 cubic stacked APN functions and all these functions belong to the same CCZ-class that is the only known class that does not contain quadratic functions (class number 13 in the list from [5]), despite that all 14 CCZ classes contains (see [14]) cubic representatives.

6.2 A generalization of the switching method on differentially 4-uniform functions

Here we show that the switching method mentioned earlier can be applied not only to APN functions, but also to differentially 4-uniform functions.

Proposition 6 *Let F be a vectorial Boolean function in n variables. Let v be a nonzero vector in $\mathbb{F}_2^n$, and h be a Boolean function in n variables, such that $F + h \cdot v$ is an APN function. Then there are exist vectorial function G, such that G is EA-equivalent to F such that $G + h \cdot e_1$ is APN.*

Proof Consider the bijective linear mapping L such that $L(v) = e_1$. Then $L(F + h \cdot v) = L(F) + h \cdot e_1 = G + h \cdot e_1$ and G is EA-equivalent to F.

It is interesting that for $n = 4, 6$ there were found cubic APN functions C such that $C = F + h \cdot e_1$, where F is APN and h is homogenous cubic function, consisting of the only one monomial. An example of such F and C for $n = 4$ can be found in Table 3. An example for $n = 6$ is the following:

$f_1 = x_1x_2 + x_4x_6 + x_5x_6 + x_2x_3x_5$;
$f_2 = x_1x_3 + x_3x_5 + x_4x_5 + x_2x_6 + x_5x_6$;
$f_3 = x_2x_3 + x_1x_4 + x_4x_5 + x_5x_6$;
$f_4 = x_2x_4 + x_1x_5 + x_3x_5 + x_2x_6 + x_3x_6 + x_4x_6 + x_5x_6$;
$f_5 = x_3x_4 + x_2x_5 + x_3x_5 + x_4x_5 + x_1x_6 + x_2x_6 + x_3x_6 + x_5x_6$;
$f_6 = x_3x_5 + x_2x_6 + x_5x_6$.

Remark 3 Let F be an APN function in n variables. If there exist Boolean function f such that $G = F + f \cdot e_1$ then $\Delta_G \leqslant 4$, since changing of one coordinate does not change the differential uniformity more than twice. This implies the following result:

Corollary 2 *Let F be a vectorial Boolean function in n variables. Let v be a nonzero vector in $\mathbb{F}_2^n$, and h be a Boolean function in n variables, such that $F + h \cdot v$ is an APN function. Then $\Delta_F \leqslant 4$.*

This corollary implies that the switching method for obtaining APN functions can be applied only to APN and differentially 4-uniform functions. Let us provide an analog of Theorem 2 for differentially 4-uniform functions below (the proof is straightforward).

Theorem 3 *Let F be a differentially 4-uniform function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. Let v be a nonzero vector in $\mathbb{F}_2^n$, and h be a Boolean function in n variables. Then function $F + h \cdot v$ is an APN if and only if the following conditions hold:*
C1.

$$h(x) + h(x + a) + h(y) + h(y + a) = 0$$

for all x, y, a such that

$$F(x) + F(x + a) + F(y) + F(y + a) = v$$

and $x \neq y$, $x \neq y + a$.

C2.

$$h(x) + h(x + a) + h(y) + h(y + a) = 1$$

for all x, y, a *such that*

$$F(x) + F(x + a) + F(y) + F(y + a) = 0$$

and $x \neq y$, $x \neq y + a$.

Remark 4 Similarly to results in [23] the searching for the switching candidates for the given differentially 4-uniform can be implemented through solving the system of linear equations. Let us note that there exist differential 4-uniform functions such that function F is given, there are no nonzero vector v and Boolean function h (in this example h is not necessarily cubic) such that function $F + h \cdot v$ is an APN.

Remark 5 These results are humble, but they emphasize the possible role of quadratic APN and differential 4-uniform functions in obtaining new APN functions of higher degrees and motivates to continue research in this direction.

OPEN QUESTION Q3: Are there exist stacked APN functions of larger algebraic degrees?

OPEN QUESTION Q4: Are there exist stacked APN functions for larger dimensions?

7 Conclusion

In this paper we considered two combinatorial approaches that allow to search for quadratic APN functions using special matrices. Given a quadratic APN function in n variables the first approach searches for quadratic APN functions in $n + 1$ variables using restrictions that can be described in terms of matrices. The second approach uses minimal matrices of cyclic form to generate quadratic APN functions. Using these approaches we found a new APN functions in 7 variables. Moreover, we obtained the complete classification of quadratic APN functions up to CCZ-equivalence in dimension 7 and proved that the list of quadratic APN functions updated with this new function is complete now. Also, we noted that quadratic parts of many APN functions have a low differential uniformity and introduced the notion of stacked APN functions.

Acknowledgements We would like to cordially thank Natalia Tokareva for her valuable remarks. We are much indebted to the reviewers of SETA-2020 conference for their helpful reviews. We are grateful to Anastasia Gorodilova and Nikolay Kolomeec for their useful observations and fruitful discussions. The work is supported by Mathematical Center in Akademgorodok under agreement No. 075-15-2019-1613 with the Ministry of Science and Higher Education of the Russian Federation and Laboratory of Cryptography JetBrains Research. We are grateful to the Supercomputing Center of the Novosibirsk State University for provided computational resources.

References

1. Beierle C., Leander G.: New Instances of Quadratic APN Functions. CoRR abs/2009.07204 (2020).
2. Beth T., Ding C.: On almost perfect nonlinear permutations. Advances in Cryptology, EUROCRYPT'93, Lecture Notes in Computer Science, vol. 765, pp. 65-76 (1993).
3. Biham E., Shamir A.: Differential cryptanalysis of DES-like cryptosystems. Journal of Cryptology, vol. 4(1), pp. 3-72 (1991).
4. Blondeau C., Nyberg K.: Perfect nonlinear functions and cryptography. Finite Fields and Their Applications, vol.32 (March), pp. 120-147(2015).
5. Brinkmann M., Leander G.: On the classification of APN functions up to dimension five. Des. Codes Cryptogr., vol. 49, Issue 13, pp. 273-288 (2008).
6. Browning K. A., Dillon J. F., McQuistan M. T., Wolfe A. J.: An APN Permutation in Dimension Six. Post-proceedings of the 9-th International Conference on Finite Fields and Their Applications Fq'09, Contemporary Math., AMS, vol. 518, pp. 33-42 (2010).
7. Budaghyan L.: Construction and analysis of cryptographic functions. Springer International Publishing, VIII, 168 pp. (2014).
8. Budaghyan L., Carlet C., Helleseth T., Li N. and Sun B.: On Upper Bounds for Algebraic Degrees of APN Functions. IEEE Transactions on Information Theory, vol. 64, no. 6, pp. 4399-4411 (2018).
9. Budaghyan L., Carlet C., Leander G.: Constructing new APN Functions from known ones. Finite Fields and Their Applications, vol. 15, I. 2, pp. 150-159 (2009).
10. Budaghyan L., Carlet C. and Leander G.: On a construction of quadratic APN functions. 2009 IEEE Information Theory Workshop, Taormina, pp. 374-378 (2009) .
11. Budaghyan L., Calderini M., Carlet C., Coulter R. S. and Villa I.: Constructing APN Functions Through Isotopic Shifts. IEEE Transactions on Information Theory, vol. 66, no. 8, pp. 5299-5309 (2020).
12. Budaghyan L., Carlet C. and Pott A.: New classes of almost bent and almost perfect nonlinear polynomials. IEEE Transactions on Information Theory, vol. 52, no. 3, pp. 1141-1152 (2006).
13. Budaghyan L. and Carlet C.: Classes of Quadratic APN Trinomials and Hexanomials and Related Structures. IEEE Transactions on Information Theory, vol. 54, no. 5, pp. 2354-2357 (2008).
14. Calderini M.: On the EA-classes of known APN functions in small dimensions. Cryptogr. Commun., vol. 12, pp.821-840 (2020).
15. Canteaut A., Charpin P., Dobbertin H.: Binary m-sequences with three-valued cross-correlation: a proof of Welch conjecture, IEEE Trans. Inf. Theory., vol. 46(1), pp. 4-8 (2000).
16. Carlet C.: Open Questions on Nonlinearity and on APN Functions. Arithmetic of Finite Fields. WAIFI 2014. Lecture Notes in Computer Science, vol. 9061, pp 83-107 (2015).
17. Carlet C.: Vectorial Boolean functions for cryptography. Ch. 9 of the monograph Boolean Methods and Models in Mathematics, Computer Science, and Engineering, Cambridge Univ. Press, pp. 398-472 (2010).
18. Carlet C., Charpin P., Zinoviev V.: Codes, bent functions and permutations suitable for DES-like cryptosystems. Des. Codes Cryptogr., vol. 15, pp. 125-156 (1998).
19. Dobbertin, H.: One-to-One Highly Nonlinear Power Functions on $GF(2^n)$. Appl. Algebra Eng. Commun. Comput., vol. 9(2), pp. 139-152 (1998).
20. Dobbertin H.: Almost perfect nonlinear power functions on $GF(2^n)$: the Welch case. IEEE Trans. Inf. Theory., vol. 45(4), pp. 1271-1275 (1999).
21. Dobbertin H.: Almost perfect nonlinear functions over GF$GF(2^n)$: the Niho case. Inform. and Comput., vol.151, pp. 57-72 (1999).
22. Dobbertin H.: Almost perfect nonlinear power functions over $GF(2^n)$: a new case for n divisible by 5. Proceedings of Finite Fields and Applications FQ5, pp. 113-121 (2000).
23. Edel Y., Pott A.: A new almost perfect nonlinear function which is not quadratic. Advances in Mathematics of Communications, vol. 3 (1), pp. 59-81 (2009).
24. Edel Y., Kyureghyan G. and Pott A.: A new APN function which is not equivalent to a power mapping. IEEE Transactions on Information Theory, vol. 52, no. 2, pp. 744-747 (2006).

25. Gold R.: Maximal recursive sequences with 3-valued recursive crosscorrelation functions. IEEE Trans. Inform. Theory, vol. 14, pp.154-156 (1968).
26. Gorodilova A A.: Characterization of almost perfect nonlinear functions in terms of subfunctions, Diskr. Mat., vol. 27(3), pp. 3-16 (2015); Discrete Math. Appl., vol. 26(4), pp. 193-202 (2016).
27. Gorodilova, A.: On the differential equivalence of APN functions. Cryptography and Communications, 11(4), pp. 793-813 (2019).
28. Glukhov M. M.: On the approximation of discrete functions by linear functions. Matematicheskie Voprosy Kriptografii, vol. 7(4), pp. 29-50 (2016) (in Russian).
29. Glukhov M. M.: On the matrices of transitions of differences for some modular groups. Matematicheskie Voprosy Kriptografii, vol. 4(4), pp. 27-47 (2013) (in Russian).
30. Hollmann H., Xiang Q.: A proof of the Welch and Niho conjectures on crosscorrelations of binary m-sequences. Finite Fields and Their Applications, vol. 7, pp. 253-286 (2001).
31. Idrisova V.: On an algorithm generating 2-to-1 APN functions and its applications to the big APN problem. Cryptogr. Commun. 11, 2139 (2019).
32. Janwa H., Wilson R.: Hyperplane sections of Fermat varieties in P^3 in char. 2 and some applications to cyclic codes. Proceedings of AAECC-10, Lecture Notes in Computer Science, vol. 673, Berlin, Springer-Verlag, pp. 180-194 (1993).
33. Kasami T.: The weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes. Inform. and Control. 18, pp. 369-394 (1971).
34. Kalgin K., Idrisova V.: On secondary and cyclic approaches to search for quadratic APN functions. Proceedings of the 11th international conference on Sequences and Their Applications — SETA-2020 (Saint-Petersburg, Russia, September 22-25, 2020).
35. Langevin P., Saygi Z. and Saygi E.: Classification of APN cubics in dimension 6 over GF(2): http://langevin.univ-tln.fr/project/apn-6/apn-6.html
36. Nyberg K.: Differentially uniform mappings for cryptography. Advances in Cryptography, EUROCRYPT'93, Lecture Notes in Computer Science, vol. 765, pp. 55-64 (1994).
37. Pott A.: Almost perfect and planar functions. Des. Codes Cryptography 78(1), pp.141-195 (2016).
38. Tuzhilin M. E.: APN functions. Prikladnaya Diskretnaya Matematika, vol. 3, pp. 1420 (2009) (in Russian).
39. Yoshiara S.: Equivalences of quadratic APN functions. Journal of Algebraic Combinatorics, 35,461475 (2012).
40. Yu Y., Wang M., Li Y.: A matrix approach for constructing quadratic APN functions. Des. Codes Cryptogr. 73, 587-600 (2014).
41. Yu Y., Kaleyski N. S., Budaghyan L., Li Y.: Classification of quadratic APN functions with coefficients in GF(2) for dimensions up to 9. IACR Cryptol. ePrint Arch.: 1491 (2019).