On combinatorial approaches to search for quadratic APN functions

Konstantin Kalgin[*]
Sobolev Institute of Mathematics
Novosibirsk State University
Novosibirsk, Russia
kalginkv@gmail.com

Valeriya Idrisova
Sobolev Institute of Mathematics
Novosibirsk, Russia
vvitkup@yandex.ru

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 $\mathbb{F}_{2^n}$ and very little is known about combinatorial constructions in $\mathbb{F}_2^n$. In this work we proposed 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 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. Also, we conjectured that a quadratic part of an arbitrary APN function has a low differential uniformity. This conjecture allowed us to introduce a new subclass of APN functions, so-called stacked APN functions. We found cubic examples of such functions for dimensions up to 6.

1 Introduction

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* $F = (f_1, \ldots, f_m)$, where f_i is a Boolean function in n variables. Any vectorial function F can be represented uniquely in its *algebraic normal form (ANF)*:

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

[*]The work was carried out within the framework of the state contract of the Sobolev Institute of Mathematics (project no. 0314-2019-0017) and supported by Russian Foundation for Basic Research (projects no. 18-07-01394 and 20-31-70043) and Laboratory of Cryptography JetBrains Research.

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.*

We can put the finite field $\mathbb{F}_{2^n}$ 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 $\mathbb{F}_{2^n}$:

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

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 [7] 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 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 is the better the resistance of a cipher containing F as an S-box to differential cryptanalysis. 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 [9].

APN functions are widely studied by many researchers, but there is still a significant list [6] 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 [4], the existence of bijective APN functions in even dimensions, etc. We are especially interested in two open problems that are devoted to constructing APN functions. The first one is to find secondary constructions of APN functions, in particular, it was stated as Problem 3.8 in [6]. The second problem is to find new constructions of APN functions in vectorspace $\mathbb{F}_2^n$, since almost all the known constructions of this class are found only as polynomials over the finite fields, and to the best of our knowledge, the only approach to such combinatorial constructions was proposed in [8].

In this work we propose two approaches for generating quadratic APN functions in $\mathbb{F}_2^n$. The first approach 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 the second 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 previously unknown (in the sense of CCZ-equivalence) quadratic APN function for $n = 7$. 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. This is very important for even $n \geqslant 8$, since new APN permutations CCZ-equivalent to quadratic functions can be found for these dimensions [3].

In the last part of the work we conjectured that a quadratic part of an arbitrary APN function has a low differential uniformity. We introduced the new notion of stacked APN function and for dimensions up to 6 found such functions using quadratic APN functions obtained with approaches mentioned above.

2 On secondary approach to search for quadratic APN functions

Since EA-equivalence preserves APNness, 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 known result gives a necessary condition on the ANF of a given APN function.

Theorem 1. *[1] Let $F = (f_1, \dots, f_n)$ 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 $G = (g_1, \dots, g_n)$ be a quadratic APN-function in n variables. Consider vectorial function $F = (f_1, \dots, f_n, f_{n+1})$ 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 proposed by Beth and Ding in [1].

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.

t is necessary to mention that these matrices also were used in [11] and [10] to construct and classify a lot of new quadratic APN functions over finite fields.

Example 2. For $n = 3$ 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 [11] and [10] 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 3. *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 $a \neq 0$.*

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 4. For the considered APN 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:

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

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

Let us note that Proposition 5 shows how to obtain restrictions on new coefficients in the convenient form.

For the given $k \in \mathbb{N}$ let us consider the following sets:

$S_{i,k} = \{\alpha_i + v \mid v \in \langle \mathcal{G}' \cdot (e_i + e_k) \rangle\}$;

$S_{i,j,k} = \{\alpha_i + \alpha_j + v \mid v \in \langle \mathcal{G}' \cdot (e_i + e_j + e_k) \rangle\}$;

$\ldots$

$S_{1,2,\ldots,k-1,k} = \{\alpha_1 + \alpha_2 + \ldots + \alpha_{k-1} + v \mid v \in \langle \mathcal{G}' \cdot (e_1 + e_2 + \ldots + e_{k-1} + e_k) \rangle\}$,

where $e_1, \ldots, e_n$ is the standard basis in $\mathbb{F}_2^n$. Let us call a vector $\alpha = (\alpha_1, \ldots, \alpha_n)$, where $\alpha_i \in \mathbb{F}_2^{n+1}$, *admissible* for matrix $\mathcal{G}'$ if it satisfies the condition in Proposition 5. We call a sequence $(\alpha_1^*, \ldots, \alpha_k^*)$, where $\alpha_i^* \in \mathbb{F}_2^{n+1}$, to be *$k$-admissible* for some $k \leqslant n$, if vector $\alpha^* = (\alpha_1^*, \ldots, \alpha_k^*, \mathbf{0}, \ldots, \mathbf{0})$ of length n is admissible for all nonzero $a' = (a_1', \ldots, a_n') \in \mathbb{F}_2^n$ such that $a_{k+1}' = 0, \ldots, a_n' = 0$. An n-admissible sequence can be considered as an admissible vector of length n. Consider an APN function G in n variables and a fixed g_{n+1}.

Proposition 6. *The number of quadratic APN functions that can be obtained from function G using the construction from (1) is equal to the number of admissible vectors $\alpha = (\alpha_1, \ldots, \alpha_n)$ for matrix $\mathcal{G}'$.*

It can be seen that there are $2^{n+1} - \mid \langle \mathcal{G}' \cdot (e_1) \rangle \mid$ vectors α_1 such that (α_1) is 1-admissible. The following proposition shows how to obtain the number of admissible vectors:

Proposition 7. *Let $(\alpha_1, \alpha_2, \ldots, \alpha_{k-1})$ be the $(k-1)$-admissible sequence for some $k < n+1$. Then there exist*

$$2^{n+1} - \mid \langle \mathcal{G}' \cdot (e_k) \rangle \cup \{\bigcup_{i=1}^{k-1} S_{i,k}\} \cup \{\bigcup_{1 \leqslant i < j < k,} S_{i,j,k}\} \cup \ldots \cup S_{1,2,\ldots,k-1,k} \mid$$

vectors α_k such that sequence $(\alpha_1, \alpha_2, \ldots, \alpha_{k-1}, \alpha_k)$ is k-admissible.

Also, our method can be 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 8. *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 construction (1). Then $\Delta_G \leqslant 4$.*

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.

It can be seen that every quadratic APN function can be obtained using construction from(1). It is 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 [2] 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 [2]). 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.

3 On cyclic approach to search for quadratic APN functions

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. Without loss of generality let us consider the first unknown element of matrix $\mathcal{T}$ that is $t_{3,n}$. According to Proposition 5 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 $\mathcal{T}' = \mathcal{T} \setminus (e_{n-1}, e_n, t_{3,n}, \ldots, 0)$. If we consider all $a' = a'_1, \ldots, a'_{n-1}$ such that $a'_3 = 1$ and $a'_i = 0$, if $i > 3$, we 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 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 2341888 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 $x^7 + x + 1$.

4 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.

Conjecture 9. Let F be an APN function in n variables, where $4 \leqslant n \leqslant 7$. Then $\Delta_{F^{(2)}} \leqslant 4$.

The conjecture is true for $n = 4$. When $n = 8, 9$ there were found APN functions F (e.g. Kasami power functions for $n = 8$ and Inverse function for $n = 9$) such that

$\Delta_{F^{(2)}} = 8$. Nevertheless, for these large dimensions the differential uniformity of quadratic parts is still quite low. Further we consider only functions without affine terms.

Proposition 10. *Let F be an APN function in n variables, where $F = F^{(2)} + F^{(3)} + \ldots + F^{(d)}$. If $H = F + F^{(2)} = (0, \ldots, 0, h_j, 0, \ldots, 0)$ for some $1 \leqslant j \leqslant n$, then $\Delta_{F^{(2)}} \leqslant 4$.*

For $n = 4, 6$ there exist cubic APN functions such that $H = F + F^{(2)} = (0, \ldots, 0, h_j, 0, \ldots, 0)$ for some $1 \leqslant j \leqslant n$. Examples of such F and $F^{(2)}$ for $n = 4$ can be found in Table 1. An example of F for $n = 6$ is the following:

$$\begin{aligned}
&f_1 = x_1x_2 + x_4x_6 + x_5x_6 + x_2x_3x_5;\\
&f_2 = x_1x_3 + x_3x_5 + x_4x_5 + x_2x_6 + x_5x_6;\\
&f_3 = x_2x_3 + x_1x_4 + x_4x_5 + x_5x_6;\\
&f_4 = x_2x_4 + x_1x_5 + x_3x_5 + x_2x_6 + x_3x_6 + x_4x_6 + x_5x_6;\\
&f_5 = x_3x_4 + x_2x_5 + x_3x_5 + x_4x_5 + x_1x_6 + x_2x_6 + x_3x_6 + x_5x_6;\\
&f_6 = x_3x_5 + x_2x_6 + x_5x_6.
\end{aligned}$$

Let us note that these simple results allow us to use quadratic APN or differentially 4-uniform functions to construct functions of higher degrees, particularly, cubic APN functions. The observation on low differential uniformity of quadratic parts of APN functions motivated us to introduce a new subclass of APN functions.

Definition 11. 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 possible approaches to constructing stacked APN functions of degree 3. Let H be a cubic vectorial function in n variables with no affine or quadratic terms. Then $H = \sum_{i,j,k} a_{ijk}x_ix_jx_k$, where $1 \leqslant i < j < k \leqslant n$ and $a_{ijk} \in \mathbb{F}_2^n$. Let $a_{i_1j_1k_1}$ be an arbitrary nonzero coefficient in the ANF of H. Let us call H a *cubic shift* if for all $1 \leqslant i < j < k \leqslant n$ vector a_{ijk} is null or equal to $a_{i_1j_1k_1}$.

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 1.

It is worth mentioning that for quadratic APN functions from differenet 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 [2]), despite that all 14 CCZ classes contains (see [5]) cubic representatives.

Table 1: 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

Acknowledgements

We would like to cordially thank Natalia Tokareva for her valuable remarks. The work was carried out within the framework of the state contract of the Sobolev Institute of Mathematics (project no. 0314-2019-0017) and supported by Russian Foundation for Basic Research (projects no. 18-07-01394 and 20-31-70043) and Laboratory of Cryptography JetBrains Research.

References

[1] T. Beth, C. Ding. On almost perfect nonlinear permutations. *Advances in Cryptology, EUROCRYPT'93, Lecture Notes in Computer Science*, vol. 765, pp. 65-76, 1993.

[2] M. Brinkmann, G. Leander. On the classification of APN functions up to dimension five. *Des. Codes Cryptogr.*, vol. 49, Issue 1–3, pp. 273-288, 2008.

[3] K. A. Browning, J. F. Dillon, M. T. McQuistan, A. J. Wolfe. 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.

[4] L. Budaghyan, C. Carlet, T. Helleseth, N. Li and B. Sun. On Upper Bounds for Algebraic Degrees of APN Functions. *IEEE Transactions on Information Theory*, vol. 64, no. 6, pp. 4399-4411, 2018.

[5] M. Calderini. On the EA-classes of known APN functions in small dimensions. *Cryptogr. Commun.* vol. 12, pp.821-840, 2020.

[6] C. Carlet. 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).

[7] C. Carlet, P. Charpin, V. Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Des. Codes Cryptogr.*, vol. 15, pp. 125-156, 1998.

[8] A. A. Gorodilova. 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.

[9] K. Nyberg. Differentially uniform mappings for cryptography. *Advances in Cryptography, EUROCRYPT'93, Lecture Notes in Computer Science*, vol. 765, pp. 55-64, 1994.

[10] Y. Yu, N. S. Kaleyski, L. Budaghyan, Y. Li. Classification of quadratic APN functions with coefficients in GF(2) for dimensions up to 9. *IACR Cryptol. ePrint Arch.*: 1491, 2019.

[11] Y. Yu, M. Wang, Y. Li. A matrix approach for constructing quadratic APN functions. *Des. Codes Cryptogr.* 73, 587-600, 2014