On a remarkable property of APN Gold functions *

Anastasiya Gorodilova
Sobolev Institute of Mathematics, Novosibirsk, Russia

E-mail: gorodilova@math.nsc.ru

Abstract. In [13] for a given vectorial Boolean function F from $\mathbb{F}_2^n$ to itself it was defined an associated Boolean function $\gamma_F(a,b)$ in $2n$ variables that takes value 1 iff $a \neq \mathbf{0}$ and equation $F(x)+F(x+a)=b$ has solutions. In this paper we introduce the notion of differentially equivalent functions as vectorial functions that have equal associated Boolean functions. It is an interesting open problem to describe differential equivalence class of a given APN function. We consider the APN Gold function $F(x)=x^{2^k+1}$, where $\gcd(k,n)=1$, and prove that there exist exactly $2^{2n+n/2}$ distinct affine functions A such that F and $F+A$ are differentially equivalent if $n=4t$ for some t and $k=n/2\pm 1$; otherwise the number of such affine functions is equal to 2^{2n}. This theoretical result and computer calculations obtained show that APN Gold functions for $k=n/2\pm 1$ and $n=4t$ are the only functions (except one function in 6 variables) among all known quadratic APN functions in $2,\ldots,8$ variables that have more than 2^{2n} trivial affine functions $A^F_{c,d}(x)=F(x)+F(x+c)+d$, where $c,d\in\mathbb{F}_2^n$, preserving the associated Boolean function when adding to F.

Keywords. Boolean function, Almost perfect nonlinear function, Almost bent function, Crooked function, Differential equivalence

1 Introduction

Almost perfect nonlinear (APN) and almost bent (AB) functions are of a great interest for using in cryptographic applications as S-boxes due to their optimal differential and nonlinear properties (see paper [30] of K. Nyberg). An actual problem in cryptographic vectorial Boolean functions is to find new constructions of APN and AB functions. In the well known paper [13] of C. Carlet, P. Charpin and V. Zinoviev for a given vectorial Boolean function F from $\mathbb{F}_2^n$ to itself it was defined an associated Boolean function $\gamma_F(a,b)$ in $2n$ variables that takes value 1 if $a\neq\mathbf{0}$ and equation $F(x)+F(x+a)=b$ has solutions and value 0 otherwise. It was observed that F is APN (AB) if and only if γ_F has weight $2^{2n-1}-2^{n-1}$ (is a bent function).

In paper [22] we obtained that there do not exist two APN functions F and F' such that $\gamma_F(a,b)=\gamma_{F'}(a,b)+1$ for all $a,b\in\mathbb{F}_2^n$, $a\neq\mathbf{0}$, when $n\geq 2$. But for a given APN function F in n variables there always exist at least 2^{2n} distinct functions $F_{c,d}(x)=F(x+c)+d$ such that $\gamma_F=\gamma_{F_{c,d}}$ for all $c,d\in\mathbb{F}_2^n$, $n\geq 2$ (see proposition 1). The question arises: do there exist more than 2^{2n} (n,n)-functions with the same associated Boolean function for a given APN function? Surprisingly, working on paper [22] we computationally found an example of such an

*The author was supported by the Russian Foundation for Basic Research (project no. 15-31-20635).

APN function in 4 variables. In this paper we introduce the following definition: two (n,n)-functions F and F' are called *differentially equivalent* if their associated functions γ_F and $\gamma_{F'}$ are equal. Note that using this notion one of the open problems mentioned by C. Carlet in [12] can be formulated as follows: is it possible to describe differentially equivalent functions to a given APN function? The answer to this question can potentially lead to new APN (AB) functions. In this paper we study the mentioned question for APN Gold functions.

We start in section 2 by discussing basic definitions with paying attention to APN and AB functions. In section 3 we introduce definition of differential equivalence of vectorial Boolean functions and describe its general properties. Several conjectures about differential equivalence of quadratic APN functions are formulated. Section 4 contains the main result of the paper, where we start to analyze differential equivalence classes of APN Gold functions $F(x) = x^{2^k+1}$ over the finite field $\mathbb{F}_{2^n}$ with $\gcd(k,n)=1$, which are also AB if n is odd. We prove that there exist exactly $2^{2n+n/2}$ distinct affine functions A such that F and $F+A$ are differentially equivalent if $n = 4t$ for some t and $k = n/2 \pm 1$; otherwise the number of such affine functions is equal to 2^{2n}. In section 5 the computational results are presented. Section 6 concludes the paper where the problem remains open is formulated.

2 Definitions

2.1 Vectorial Boolean functions

Let $\mathbb{F}_{2^n}$ be the finite field of order 2^n and $\mathbb{F}_2^n$ be the n-dimensional vector space over $\mathbb{F}_2$. Let $\mathbf{0}$ denote the zero vector of $\mathbb{F}_2^n$. A mapping $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is called *a vectorial Boolean function* or *a (n,m)-function*. When $m = 1$ a function F is called *a Boolean function*. The *Hamming weight* $\mathrm{wt}(f)$ of a Boolean function f is defined as $\mathrm{wt}(f) = |\{x \in \mathbb{F}_2^n : \ f(x) = 1\}|$ and the *Hamming distance* between f and g is $\mathrm{dist}(f,g) = |\{x \in \mathbb{F}_2^n : \ f(x) \neq g(x)\}|$. Any (n,m)-function F can be considered as the set of m Boolean functions that are called *coordinate functions* of F in the form $F(x) = (f_1(x), \ldots, f_m(x))$, where $x \in \mathbb{F}_2^n$. Any such a function F has its unique *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 the power set of $N = \{1, \ldots, n\}$ and a_I belongs to $\mathbb{F}_2^m$. Here $+$ denotes the coordinate-wise sum of vectors modulo 2. The *algebraic degree* of F is degree of its ANF: $\deg(F) = \max\{|I| : \ a_I \neq \mathbf{0}, \ I \in \mathcal{P}(N)\}$. A function is called *affine* if its algebraic degree is not more than 1 or, equivalently, if $F(x+y) = F(x) + F(y) + F(\mathbf{0})$ for any $x, y \in \mathbb{F}_2^n$. An affine function F is *linear* if $F(\mathbf{0}) = \mathbf{0}$. Functions of algebraic degree 2 are called *quadratic*.

In this paper we will consider only (n,n)-functions and Boolean functions. Further, by vectorial Boolean functions we mean only (n,n)-functions. It is convenient to identify the vector space $\mathbb{F}_2^n$ with the finite field $\mathbb{F}_{2^n}$ and to consider vectorial Boolean functions as mappings from $\mathbb{F}_{2^n}$ to itself. Any such a function F has the unique representation as a univariate polynomial over $\mathbb{F}_{2^n}$ of degree not more than $2^n - 1$

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

It is widely known that algebraic degree of F can be calculated as $\deg(F) = \max_{i=0,\ldots,2^n-1}\{\mathrm{wt}(i) : \lambda_i \neq 0\}$, where $\mathrm{wt}(i)$ denotes binary weight of integer i. In this representation any affine function F has a form $F(x) = \lambda + \sum_{i=0}^{n} \lambda_i x^{2^i}$, where $\lambda, \lambda_i \in \mathbb{F}_{2^n}$. And F is linear if $\lambda = 0$.

Since a Boolean function f on $\mathbb{F}_{2^n}$ is a particular case of vectorial Boolean functions then it also can be uniquely represented as a univariate polynomial that takes values only from $\mathbb{F}_2$. But there is a more convenient representation of f that is called *trace form* (it is not unique):

$$f(x) = \mathrm{tr}\big(\sum_{i \in CS} \lambda_i x^i + \lambda x^{2^n-1}\big),$$

where $\lambda_i, \lambda \in \mathbb{F}_{2^n}$, tr denotes the *trace function* $\mathrm{tr}(x) = x + x^2 + x^{2^2} + \ldots + x^{2^{n-1}}$ and CS is the set of representatives of *cyclotomic classes* modulo $2^n - 1$. Recall that the trace function takes values only from $\mathbb{F}_2$ and it is a linear function. A cyclotomic class modulo $2^n - 1$ of an integer i is the set $C(i) = \{i \cdot 2^j \bmod (2^n - 1),\ j = 0, \ldots, n-1\}$. Cardinality of any cyclotomic class modulo $2^n - 1$ is at most n and divides n.

There are two notions of equivalence of vectorial Boolean functions that are usually considered studying cryptographic functions. Let F and F' be (n,n)-functions. F and F' are called *extended affine equivalent* (EA-equivalent) if $F' = A' \circ F \circ A'' + A$, where A', A'' are affine permutations of $\mathbb{F}_2^n$ and A is an affine function on $\mathbb{F}_2^n$. Two functions F and F' are said to be *Carlet-Charpin-Zinoviev equivalent* (CCZ-equivalent) if their graphs $\mathcal{G}_F = \{(x, F(x)) : x \in \mathbb{F}_2^n\}$ and $\mathcal{G}_{F'} = \{(x, F'(x)) : x \in \mathbb{F}_2^n\}$ are affine equivalent, that is, there exists an affine permutation $A = (A_1, A_2)$ of $\mathbb{F}_2^n \times \mathbb{F}_2^n$ (where A_1, A_2 are affine functions from $\mathbb{F}_2^n \times \mathbb{F}_2^n$ to $\mathbb{F}_2^n$), such that $y = F(x)$ if and only if $A_2(x, y) = F'(A_1(x, y))$ for all $x, y \in \mathbb{F}_2^n$.

Both these equivalences preserve the properties of a vectorial Boolean function to be APN and AB. But, in general, CCZ-equivalence in contrast to EA-equivalence modifies the algebraic degree of a function. EA-equivalence is a particular case of CCZ-equivalence, although in several cases they coincide, for example, for Boolean functions and vectorial bent Boolean functions as shown by L. Budaghyan and C. Carlet in [8]. Also, it was proved in [34] by S. Yoshiara that two quadratic APN functions are CCZ-equivalent if and only if they are EA-equivalent.

2.2 APN and AB functions

A function F from $\mathbb{F}_2^n$ to itself is called *almost perfect nonlinear* (APN) if for any $a, b \in \mathbb{F}_2^n$, $a \neq \mathbf{0}$, equation $F(x) + F(x + a) = b$ has at most 2 solutions. Equivalently, F is APN if $|B_a(F)| = |\{F(x) + F(x + a) \mid x \in \mathbb{F}_2^n\}| = 2^{n-1}$ for any nonzero vector a.

The *nonlinearity* $\mathcal{N}_F$ of a (n,m)-function F is the minimum Hamming distance between all nonzero linear combinations of coordinate functions of F and all affine Boolean functions on $\mathbb{F}_2^n$. There is the universal bound on nonlinearity of an arbitrary (n,m)-function: $\mathcal{N}_F \leq 2^{n-1} - 2^{n/2-1}$. A (n,m)-function is called a *bent function* if its nonlinearity is equal to $2^{n-1} - 2^{n/2-1}$. In [29] K. Nyberg proved that bent functions exist only if $m \leq n/2$ and n is even. When $n = m$, there is a better upper bound on nonlinearity (the Sidelnikov-Chabaud-Vaudenay bound) equal to $2^{n-1} - 2^{(n-1)/2}$. Vectorial functions on $\mathbb{F}_2^n$ that achieve this bound are called *almost bent* (AB). It is easy to see that AB functions exist only for odd n. Every AB function is APN but the converse is not true. However, it was proved [13] that every quadratic APN function in odd number of variables is AB.

Although APN and AB functions are intensively studied, it is very hard to give completed descriptions of these classes. *Power* or *monomial* functions, that are functions over $\mathbb{F}_{2^n}$ of the

form $F(x) = x^d$, are the simplest candidates to study whether they are APN (AB) or not. Table 1 illustrates the list of all known APN and AB power functions. There is a conjecture [14] of H. Dobbertin that this list is complete. Note that in paper [20] M. M. Glukhov mentions that the APN property of the inverse function (see Table 1) was already proved in 1968 by V. A. Bashev and B. A. Egorov. Infinitive families of APN and AB polynomials are also found (see, for example, surveys [31] of A. Pott, [32] of M. E. Tuzhilin).

Table 1: Known APN and AB power functions x^d on $\mathbb{F}_{2^n}$.

Functions	Exponents d	Conditions	$\deg(x^d)$	AB	Ref.
Gold	$d = 2^t + 1$	$\gcd(t, n) = 1$	2	for odd n	[21], [30]
Kasami	$d = 2^{2t} - 2^t + 1$	$\gcd(t, n) = 1$	$t + 1$	for odd n	[26], [27]
Welch	$2^t + 3$	$n = 2t + 1$	3	yes	[11], [15]
Niho	$2^t + 2^{\frac{t}{2}} - 1$, if t is even $2^t + 2^{\frac{3t+1}{2}} - 1$, if t is odd	$n = 2t + 1$	$(t + 1)/2$ $t + 1$	yes	[14], [24]
Inverse	$2^{2t} - 1$	$n = 2t + 1$	$n - 1$	no	[3], [30]
Dobbertin	$2^{4t} + 2^{3t} + 2^{2t} + 2^t - 1$	$n = 5t$	$t + 3$	no	[16]

Another longstanding problem in APN functions is the existence of APN permutations in even number of variables n. There are several partial nonexistence results on APN permutations (for example, [2], [19], [25]) and the only APN permutation in even n is discovered in [7] for $n = 6$ by J. F. Dillon et al. In [33] V. Vitkup considers sets of different values of an arbitrary APN function and study their properties and bounds on their cardinalities.

Complete classification over EA and CCZ-equivalence of APN functions up to dimension 5 was obtained in [5] by M. Brinkman and G. Leander. For $n = 6$ there are also known all 13 CCZ-inequivalent quadratic APN functions (found in [6], verified in [17] by Y. Edel). In paper [36] Y. Yu, M. Wang, Y. Li developed a new approach to find CCZ-inequivalent quadratic APN functions and in updated version of [35] presented 487 CCZ-inequivalent quadratic APN functions for $n = 7$ and 8179 for $n = 8$.

3 Differential equivalence of vectorial Boolean functions

In this section we introduce the notion of differential equivalence of vectorial Boolean functions and consider its basic properties in general case and more precisely in case of quadratic functions.

3.1 Definition and basic properties of differential equivalence

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a vectorial Boolean function. In [13] a Boolean function $\gamma_F : \mathbb{F}_2^{2n} \to \mathbb{F}_2$ associated to F was introduced in the following way: $\gamma_F(a, b)$ takes value 1 if and only if $a \neq \mathbf{0}$ and $F(x) + F(x + a) = b$ has solutions. It was shown that F is APN (AB) if and only if γ_F has the Hamming weight $2^{2n-1} - 2^{n-1}$ (is a bent function, respectively).

Let us introduce the following definition.

Definition 1. *Two functions F, F' from $\mathbb{F}_2^n$ to itself are called differentially equivalent if $\gamma_F = \gamma_{F'}$. Denote the differential equivalence class of F by $\mathcal{DE}_F$.*

Problem 1. *[12] Is it possible to find a systematic way, given an APN function F, to build another function F' such that $\gamma_F = \gamma_{F'}$?*

This open problem can be also formulated in terms of differential equivalence: is it possible to describe the differential equivalence class of a given APN function? It is a rather natural question, but it seems to be difficult to find an answer for an arbitrary APN function. Indeed, we could not even say that differential equivalence between two APN functions implies EA- or CCZ-equivalence between them. It makes this problem more interesting since we potentially could find new APN functions studying differential equivalence classes of known ones.

Let us denote the set $\{F(x) + F(x+a) \mid x \in \mathbb{F}_2^n\}$ by $B_a(F)$, where $a \in \mathbb{F}_2^n$.

Proposition 1. *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be an APN function and $n > 1$. Then $F_{c,d}(x) = F(x+c) + d$ is differentially equivalent to F for all $c, d \in \mathbb{F}_2^n$ and all the functions $F_{c,d}$ are pairwise distinct.*

Proof. Consider $B_a(F_{c,d})$ for an arbitrary nonzero a from $\mathbb{F}_2^n$:

$$\begin{aligned} B_a(F_{c,d}) &= \{F(x+c) + d + F(x+c+a) + d \mid x \in \mathbb{F}_2^n\} \\ &= \{F(y) + F(y+a) \mid y \in \mathbb{F}_2^n\} = B_a(F). \end{aligned}$$

Thus, by definition F and $F_{c,d}$ are differentially equivalent for any $c, d \in \mathbb{F}_2^n$.

Suppose that there exist $c, d, c', d' \in \mathbb{F}_2^n$ such that $F_{c,d} = F_{c',d'}$. Then $F(x+c) + d = F(x+c') + d'$ for all $x \in \mathbb{F}_2^n$. Since $n > 1$, it follows that equation $F(x) + F(x+a) = b$ has at least 4 solutions if $a = c + c'$ and $b = d + d'$. So, it is impossible for F to be APN if $c \neq c'$ or $d \neq d'$. □

The next proposition means that we only need to study differential equivalence classes of the representatives of EA-equivalence classes of vectorial Boolean functions.

Proposition 2. *Let F, G be EA-equivalent functions from $\mathbb{F}_2^n$ to itself. Then $|\mathcal{DE}_F| = |\mathcal{DE}_G|$. Moreover, if $G = A' \circ F \circ A'' + A$ and $\mathcal{DE}_F = \{F_1, \ldots, F_k\}$, then $\mathcal{DE}_G = \{A' \circ F_1 \circ A'' + A, \ldots, A' \circ F_k \circ A'' + A\}$.*

Proof. Let us show that functions $G_i' = A' \circ F_i \circ A'' + A$, $i = 1, \ldots, k$, belong to $\mathcal{DE}_G$. Indeed,

$$\begin{aligned} B_a(G_i') &= \{G_i'(x) + G_i'(x+a) \mid x \in \mathbb{F}_2^n\} \\ &= \{A'\big(F_i(A''(x))\big) + A(x) + A'\big(F_i(A''(x+a))\big) + A(x+a) \mid x \in \mathbb{F}_2^n\} \\ &= \{A'\big(F_i(y) + F_i(y + A''(a) + A''(0))\big) + A'(0) + A(a) + A(0) \mid y \in \mathbb{F}_2^n\} \\ &= A'\big(B_{A''(a)+A''(0)}(F_i)\big) + A'(0) + A(a) + A(0). \end{aligned}$$

Similarly, $B_a(G) = A'\big(B_{A''(a)+A''(0)}(F)\big) + A'(0) + A(a) + A(0)$. Since $B_{A''(a)+A''(0)}(F) = B_{A''(a)+A''(0)}(F_i)$ for all $a \in \mathbb{F}_2^n$ and A' is a one-to-one function, then $B_a(G_i') = B_a(G)$ for all $a \in \mathbb{F}_2^n$. So, $G_i' \in \mathcal{DE}_G$, $i = 1, \ldots, k$. Thus, $|\mathcal{DE}_G| \geq k$, since $F_i \neq F_j$ implies $G_i' \neq G_j'$, where $i, j = 1, \ldots, k$, $i \neq j$.

On the other hand, $F = (A')^{-1} \circ G \circ (A'')^{-1} + (A')^{-1} \circ A \circ (A'')^{-1} + (A')^{-1}(0) = \tilde{A}' \circ G \circ \tilde{A}'' + \tilde{A}$. Similarly, we get $k \geq |\mathcal{DE}_G|$ that completes the proof. □

There is the next natural question: "Is it true that an analogue of proposition 2 for CCZ-equivalent functions takes place?". Let us consider the case $n = 4$: there exist 2 EA-equivalence classes of APN functions and their representatives are CCZ-equivalent (see [5]). We computationally found that cardinalities of differential equivalence classes of these two representatives are equal to each other (see section 5). So, such an analogue holds for all numbers of variables up to 4.

3.2 Differential equivalence of quadratic APN functions

Quadratic APN functions are the simplest APN functions due to their algebraic degree, since affine APN functions on $\mathbb{F}_2^n$ do not exist if $n > 1$. But even in this case APN and AB functions are still not classified for arbitrary number of variables. Studying quadratic functions we make use of the following their useful property. If F is a quadratic function from $\mathbb{F}_2^n$ to itself then $B_a(F)$ is an affine subspace for all nonzero $a \in \mathbb{F}_2^n$ (recall that $B_a(F) = \{F(x) + F(x+a) \mid x \in \mathbb{F}_2^n\}$). If F is APN, then $B_a(F)$ is an affine hyperplane (i. e. has cardinality 2^{n-1}) for all $a \neq \mathbf{0}$.

In [1] definition of the *crooked* functions was introduced in connection with distance regular graphs by T. D. Bending and D. Fon-Der-Flaass. In [28] G. Kyureghyan generalized this definition to the following: a function F is called *crooked* if $B_a(F)$ is an affine hyperplane for all $a \neq \mathbf{0}$. Obviously, quadratic APN functions are always crooked. There is also a conjecture (proved for monomial [28] and special binomial [4] functions):

Conjecture 1. *[28] All crooked functions are quadratic.*

If conjecture 1 is true, then for solving problem 1 for a quadratic APN function F we only need to study if there exist quadratic functions differentially equivalent to F. The first natural step in this direction is to study whether EA-equivalent to F function G is also differentially equivalent to F.

Let $G = A' \circ F \circ A'' + A$, where F is a quadratic APN function, A', A'' are affine permutations and A is an affine function. Denote by L', L'', L linear parts of A', A'', A respectively, i. e. $L'(x) = A'(x) + A'(\mathbf{0})$, $L''(x) = A''(x) + A''(\mathbf{0})$, $L(x) = A(x) + A(\mathbf{0})$. Then

$$B_a(G) = L'\big(B_{L''(a)}(F)\big) + L(a). \tag{1}$$

Proposition 3. *Let F, A', A'', A be functions from $\mathbb{F}_2^n$ to itself, where F is a quadratic APN permutation, A', A'' are affine permutations and A is an affine function. Then F and $A' \circ F \circ A'' + A$ are differentially equivalent if and only if F and $A' \circ F \circ A''$ are differentially equivalent and F and $F + A$ are differentially equivalent.*

Proof. Denote by L', L'', L linear parts of A', A'', A respectively. The sufficient condition follows immediately from (1) and differential equivalence definition. Let us prove the necessary condition. Let F and $G = A' \circ F \circ A'' + A$ be differentially equivalent. Since F is a quadratic permutation, then $B_a(F)$ is a complement of a hyperplane for all nonzero $a \in \mathbb{F}_2^n$. From (1) and $B_a(G) = B_a(F)$ we get that linear parts of $B_a(F)$ and $L'\big(B_{L''(a)}(F)\big)$ are equal. Hence, $B_a(F) = L'\big(B_{L''(a)}(F)\big)$, since L', L'' are linear permutations and $\mathbf{0} \notin B_a(F)$ for all $a \neq \mathbf{0}$. This implies that F and $A' \circ F \circ A''$ are differentially equivalent. Therefore, F and $F + A$ are also differentially equivalent. □

Thus, according to proposition 3 for quadratic APN permutations we could separately consider when F and $A' \circ F \circ A''$ are differentially equivalent, where A', A'' are affine permutations, and whether there exist an affine function A for a quadratic APN function F such that F and $F + A$ are differentially equivalent. There is also the following conjecture that holds for $2, 3, 4$ number of variables.

Conjecture 2. *Proposition 3 is also true when F is an arbitrary quadratic APN function.*

Note that at least 2^{2n} distinct affine functions A such that F and $F+A$ are differentially equivalent exist for any quadratic APN function F on $\mathbb{F}_2^n$. Indeed, $A_{c,d}^F(x) = F(x)+F(x+c)+d$ is affine for all $c, d \in \mathbb{F}_2^n$ and $F(x) + A_{c,d}^F(x) = F(x+c)+d$, which is differentially equivalent to F according to proposition 1. So, all these functions $A_{c,d}^F$ are distinct and lead only to functions belonging to the set of trivial differentially equivalent to F functions $\{F(x+c)+d \mid c, d \in \mathbb{F}_2^n\}$. The question arises: do there exist other affine functions? It is easy to see that the number of affine functions A for a given quadratic APN function F such that $F + A \in \mathcal{DE}_F$ is an EA invariant.

We have the following conjecture for odd number variables that is verified (see section 5) for all quadratic APN functions in $3, 5$ variables and for all 487 known EA-equivalence classes of quadratic APN functions from [35], [36] in 7 variables. Recall that in these cases APN functions are also AB.

Conjecture 3. *Let n be odd and F be a quadratic APN function in n variables. Then there exist exactly 2^{2n} affine functions such that F and $F + A$ are differentially equivalent.*

If n is even then an analogue of conjecture 3 is not true when $n \geq 4$. The illustration of this fact we will see in the next section, where APN Gold functions are studied.

Studying when quadratic APN functions F and $L' \circ F \circ L''$ are differentially equivalent for small number of variables, where L', L'' are linear permutations, we came to the following conjecture (proved for $n = 2, 3, 4$).

Conjecture 4. *Let F be a quadratic APN function in n variable. Then F and $L' \circ F \circ L''$ are differentially equivalent, where L', L'' are linear permutations on $\mathbb{F}_2^n$, if and only if $F = L' \circ F \circ L''$.*

4 APN Gold functions

An APN Gold function is a quadratic monomial function of the form $F(x) = x^{2^k+1}$ over $\mathbb{F}_{2^n}$, where $\gcd(k, n) = 1$. Thus, it follows [13] that it is also AB for odd n. It is easy to see that Gold functions are permutations if n is odd and 3-to-1 functions otherwise.

APN Gold functions take a special place among APN functions. At first, these functions were proved to be the only *exceptional* monomial functions [23] along with APN Kasami functions by F. Hernando, G. McGuire. Also, despite the fact these functions seem to be rather simple due to their algebraic degree and the univariate representation, other interesting constructions of APN functions have been found based on them (for example, [9], [10], [18]).

Working on paper [22], where we tried to find an affine function A for a given quadratic APN function such that $B_a(F+A) = \mathbb{F}_2^n \backslash B_a(F)$ for as many vectors a as possible, we found that for the APN Gold function in 4 variables there exist 2^{10} affine functions such that $B_a(F + A) = B_a(F)$ for all $a \in \mathbb{F}_2^4$. This result shows us that the differential equivalence class of this function F includes functions that do not belong to the trivial set $\{F(x+c)+d \mid c, d \in \mathbb{F}_2^4\}$.

In this section we prove that for an APN Gold function $F(x) = x^{2^k+1}$ there exist exactly $2^{2n+n/2}$ distinct affine functions A such that F and $F + A$ are differentially equivalent if $n = 4t$ for some t and $k = n/2 \pm 1$; otherwise the number of such affine functions is equal to 2^{2n}.

4.1 Preliminary lemmas

Here we consider two lemmas that will be used for proving the main result of the paper.

Lemma 1. *Let n be an integer. Let $P_k^i = 2^i - 2^k - 1$, where $i = 0, \ldots, n-1$ and k runs from 1 to $n-1$ except the case $k = n/2$ if n is even. Then the following statements hold:*

(1) P_k^0 and P_k^k are in one cyclotomic class modulo $2^n - 1$ (say, C) for all k;

(2) P_k^i and P_k^j are in distinct cyclotomic classes modulo $2^n - 1$ not equal to C for all $i \neq j$ and $i, j \neq 0, k$;

(3) if n is odd, then $|C(P_k^i)| = n$ for all i and k;

(4) if n is even, then $|C(P_k^i)| = n$ for all i and k except the following cases: $|C(P_{n/2-1}^{n-1})| = |C(P_{n/2+1}^{k-1})| = n/2$.

Proof. (1) Let us further by P_k^i mean the representative of P_k^i congruence class modulo $2^n - 1$ belonging to the interval from 0 to $2^n - 2$. By definition, binary weights of $P_k^0 = -2^k$ and $P_k^k = -1$ are equal to $n-1$. It is easy to see that all integers from 0 to $2^n - 2$ of binary weight $n-1$ are in one cyclotomic class modulo $2^n - 1$ (say, C) of cardinality n.

(2) Let us consider all integers P_k^i and their binary representations, see Table 2. The integers $P_k^1, \ldots, P_k^{k-1}$ have binary weights $n-k, \ldots, n-2$ correspondingly. Thus, they are in pairwise distinct cyclotomic classes modulo $2^n - 1$ not equal to C. Similarly, the integers $P_k^{k+1}, \ldots, P_k^{n-1}$ belong to pairwise distinct cyclotomic classes modulo $2^n - 1$ not equal to C since their binary weights runs from k to $n-2$.

Table 2: Binary representations of integers P_k^i.

i	$P_k^i = 2^i - 2^k - 1 \bmod (2^n - 1) = (b_{n-1}, \ldots, b_k, \ldots, b_0) \in \mathbb{F}_2^n$														$wt(P_k^i)$
0	1	1	…	1	1	**0**	1	1	…	1	1	1	1	1	$n-1$
1	1	1	…	1	1	**1**	0	0	…	0	0	0	0	0	$n-k$
2	1	1	…	1	1	**1**	0	0	…	0	0	0	1	0	$n-k+1$
3	1	1	…	1	1	**1**	0	0	…	0	0	1	1	0	$n-k+2$
…	…														…
$k-1$	1	1	…	1	1	**1**	0	1	…	1	1	1	1	0	$n-2$
k	1	1	…	1	1	**1**	1	1	…	1	1	1	1	0	$n-1$
$k+1$	0	0	…	0	0	**0**	1	1	…	1	1	1	1	1	k
$k+2$	0	0	…	0	1	**0**	1	1	…	1	1	1	1	1	$k+1$
…	…														…
$n-1$	0	1	…	1	1	**0**	1	1	…	1	1	1	1	1	$n-2$

The binary representation of P_k^i consist of two groups of consecutive 1s that have lengths $n-k$ and $i-1$ if $i = 1, \ldots k-1$, and k and $i-k-1$ if $i = k+1, \ldots, n-1$. Since the necessary condition for two such integers be in the same cyclotomic classes is the equality of lengths of consecutive 1s groups, then any two integers from different considered groups belong to different classes. Indeed, $n-k \neq k$ by proposition condition and $n-k \neq i-k-1$ for all $i = k+1, \ldots, n-1$.

(3), (4) According to the previous studying of P_k^i binary representations the only possible case when $|C(P_k^i)| \neq n$ is the following: if lengths of consecutive 1s groups in P_k^i are both equal to $n/2 - 1$. If n is odd, this case is not realized. If n is even, then these possibilities are the following: $i = n-1$ if $k = n/2-1$ and $i = k-1$ if $k = n/2+1$. In both these cases $P_k^i = 2^{n/2} P_k^i$ modulo $2^n - 1$ that completes the proof. □

Lemma 2. *Let ℓ be an integer, $\ell > 1$. If ℓ is even, then $gcd(2\ell, \ell \pm 1) = 1$; if ℓ is odd, then $gcd(2\ell, \ell \pm 1) = 2$.*

Proof. Let $\gcd(2\ell, \ell \pm 1) = d$. Then $2\ell = xd$ and $\ell \pm 1 = yd$, where $\gcd(x, y) = 1$. Extracting ℓ from the second equality and putting it to the first equality we get $2 = (\mp x \pm 2y)d$. Hence the only possible cases are:

1) $d = 2$, $\mp x \pm 2y = 1$. Then $\ell = 2y \mp 1$ is an odd integer.

2) $d = 1$, $\mp x \pm 2y = 2$. Then $2\ell = x$ and $\ell = y \mp 1$. Since x is even and $\gcd(x, y) = 1$, then y is odd and as a result ℓ is even. □

4.2 The main result

For an APN Gold function F the explicit form of the associated Boolean function γ_F is known [13]. For completeness we present it with a proof.

Proposition 4. *Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a Gold function $F(x) = x^{2^k+1}$, where $gcd(k, n) = 1$. Then $\gamma_F(a, b) = tr\big((a^{2^k+1})^{-1}b\big) + tr(1) + 1$ if $a \neq 0$ and $\gamma_F(0, b) = 0$ for all $b \in \mathbb{F}_{2^n}$.*

Proof. By definition, $\gamma_F(a, b) = 1$ if and only if $a \neq 0$ and equation $F(x) + F(x + a) = b$ has solutions. Let us consider this equation for a Gold function:

$$x^{2^k+1} + (x + a)^{2^k+1} = b,$$

$$x^{2^k}a + xa^{2^k} = b + a^{2^k+1} \quad / \cdot a^{-1}(a^{2^k})^{-1},$$

$$x^{2^k}(a^{-1})^{2^k} + xa^{-1} = b(a^{2^k+1})^{-1} + 1.$$

If a solution exists, then by applying the function trace to both sides of the equation we get:

$$tr\big(x^{2^k}(a^{-1})^{2^k} + xa^{-1}\big) = 0 = tr\big(b(a^{2^k+1})^{-1} + 1\big).$$

Then $\gamma_F(a, b) = tr\big(b(a^{2^k+1})^{-1} + 1\big) + 1 = tr\big((a^{2^k+1})^{-1}b\big) + tr(1) + 1$.

□

The following theorem contains the main result of the paper.

Theorem 1. *Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a Gold function $F(x) = x^{2^k+1}$, where $gcd(k, n) = 1$. Then the following statements hold:*

(1) if $n = 4t$ for some t and $k = n/2 \pm 1$, then there exist exactly $2^{2n+n/2}$ distinct affine functions A of the form $A(x) = \alpha + \lambda^{2^k}x + \lambda x^{2^k} + \delta x^{2^j}$ such that F and $F + A$ are differentially equivalent, where $\alpha, \lambda, \delta \in \mathbb{F}_{2^n}$, $\delta = \delta^{2^{n/2}}$, and $j = k - 1$ for $k = n/2 + 1$ and $j = n - 1$ for $k = n/2 - 1$;

(2) otherwise there exist exactly 2^{2n} distinct affine functions A of the form $A(x) = \alpha + \lambda^{2^k}x + \lambda x^{2^k}$ such that F and $F + A$ are differentially equivalent, where $\alpha, \lambda \in \mathbb{F}_{2^n}$.

Proof. From proposition 4 we get that $\gamma_F(a, b) = tr\big((a^{2^k+1})^{-1}b\big) + tr(1) + 1$ if $a \neq 0$ and $\gamma_F(0, b) = 0$ for all $b \in \mathbb{F}_{2^n}$. Let A be an affine function from $\mathbb{F}_{2^n}$ to itself and L be its linear part, i. e. $L(x) = A(x) + A(0)$. Then

$$\gamma_{F+A}(a, b) = \gamma_F\big(a, b + L(a)\big) = tr\big((a^{2^k+1})^{-1}(b + L(a)\big) + tr(1) + 1$$

$$= tr\big((a^{2^k+1})^{-1}b\big) + tr\big(((a^{2^k+1})^{-1}L(a)\big) + tr(1) + 1.$$

Thus, $\gamma_{F+A}(a,b) = \gamma_F(a,b) + tr\big((a^{2^k+1})^{-1}L(a)\big)$. So, F and $F+A$ are differentially equivalent if and only if the linear part L of A satisfies the equality $tr\big((a^{2^k+1})^{-1}L(a)\big) = 0$ for all $a \in \mathbb{F}_{2^n}$. Denote by N the number of such affine functions A.

Let $A(x) = \alpha + L(x) = \alpha + \sum_{i=0}^{n-1} \lambda_i x^{2^i}$ be an affine function, where $\alpha, \lambda_i \in \mathbb{F}_{2^n}$, $i = 0, \ldots, n-1$. Then the following equalities hold for all $a \in \mathbb{F}_{2^n}$:

$$tr\big((a^{2^k+1})^{-1}L(a)\big) = tr\big(\sum_{i=0}^{n-1} \lambda_i a^{2^i}(a^{2^k+1})^{-1}\big) = \sum_{i=0}^{n-1} tr(\lambda_i a^{2^i-2^k-1}) = 0.$$

The last equality represents a polynomial equation in variable a of degree not more than 2^n-1 that has 2^n solutions. So, all its coefficients must be equal to 0. Let us find the coefficients of all monomials x^d, $d = 0, \ldots, 2^n-1$. To do this we need to study cyclotomic classes of all exponents $P_k^i = 2^i - 2^k - 1$, $i = 0, \ldots, n-1$, for a given k. From lemma 1 (1,2) it follows that there are only two exponents P_k^0 and P_k^k belonging to one cyclotomic class modulo 2^n-1. So, we get that there is a relation between λ_0 and λ_k in the form $\lambda_0 = (\lambda_k)^{2^k}$ for all n since $P_k^0 = 2^k P_k^k \pmod{(2^n-1)}$. To study the other coefficients consider the following cases.

Case 1. If n is odd, then from lemma 1 (2,3) we get that $\lambda_i = 0$ if $i \neq 0, k$. Thus, $N = 2^{2n}$ since we can choose α, λ_k be arbitrary elements from $\mathbb{F}_{2^n}$.

Let $n = 2\ell$ be even. There are two different possibilities.

Case 2. If ℓ is odd, then $\gcd(n, n/2 \pm 1) = 2$ according to lemma 2. So, we do not consider $k = n/2 \pm 1$ by theorem condition and as a result $\lambda_i = 0$ if $i \neq 0, k$ according to lemma 1 (4). Similarly to case 1, $N = 2^{2n}$.

Case 3. If ℓ is even, then according to lemma 2 $\gcd(n, n/2 \pm 1) = 1$.

— If $k \neq n/2 \pm 1$, then according to lemma 1 (4) we have $\lambda_i = 0$ if $i \neq 0, k$. Thus, $N = 2^{2n}$.

— If $k = n/2 + 1$, then according to lemma 1 (4) we have $\lambda_i = 0$ if $i \neq 0, k-1, k$ and $\lambda_{k-1} = (\lambda_{k-1})^{2^{n/2}}$. Since the number of elements $x \in \mathbb{F}_{2^n}$ satisfying the equality $x = x^{2^{n/2}}$ is equal to $2^{n/2}$, we have $N = 2^{2n+n/2}$.

— If $k = n/2 - 1$, then according to lemma 1 (4) we have $\lambda_i = 0$ if $i \neq 0, k, n-1$ and $\lambda_{n-1} = (\lambda_{n-1})^{2^{n/2}}$. Similarly to the previous, $N = 2^{2n+n/2}$. □

Theorem 1 shows that the class of APN Gold functions contains quadratic APN functions F whose differential equivalence classes are wider than trivial classes $\{F_{c,d}(x) = F(x+c)+d \mid c, d \in \mathbb{F}_2^n\}$ of cardinality 2^{2n} (recall that for a quadratic function F functions $F_{c,d} = F + A_{c,d}$, where $A_{c,d}$ is affine for all $c, d \in \mathbb{F}_2^n$). Indeed, the cardinality of $\mathcal{DE}_F$, where $F(x) = x^{2^{n/2\pm1}+1}$, $n = 4t$, is greater or equal to $2^{2n+n/2}$ according to theorem 1 (1). Also, as we will see in section 5 these APN Gold functions are the only functions (except one function in 6 variables) among all quadratic APN functions in $2, \ldots, 6$ variables and all known quadratic APN functions in 7, 8 variables that have more than 2^{2n} affine functions preserving the associated Boolean functions when adding to the original functions and as a result have differential equivalence classes wider than trivial. That is why we call this property of APN Gold functions remarkable.

5 Computational results

Here we present results that were obtained using computer calculations.

Table 3 illustrates a classification under differential equivalence of APN functions in small number of variables n. For these dimensions we see that differential equivalence between two functions implies also their EA-equivalence.

Table 3: Cardinalities of differential equivalence classes of APN functions on $\mathbb{F}_2^n$.

n	# APN functions	EA	deg	# differential equivalence classes with cardinalities
2	192	x^3	2	12 classes of 2^4 functions
3	688128	x^3	2	10752 classes of 2^6 functions
4	18 940 805 775 360	x^3	2	1 156 055 040 classes of 2^{10} functions
		f [10]	3	17 340 825 600 classes of 2^{10} functions

Here $f(x) = x^3 + (x^2 + x + 1)tr(x^3)$.

Further we study how many affine functions A in n variables exist for a given quadratic APN function such that F and $F + A$ belong to one differential equivalence class. At first we present mathematical background for our search.

Let F be a quadratic APN function. Then γ_F is of the form $\gamma_F(a, b) = \Phi(a) \cdot b + \varphi(a) + 1$, where $\Phi : \mathbb{F}_2^n \to \mathbb{F}_2^n$, $\varphi : \mathbb{F}_2^n \to \mathbb{F}_2$ are uniquely defined from

$$B_a(F) = \{y \in \mathbb{F}_2^n \mid \Phi_F(a) \cdot y = \varphi_F(a)\}$$

for all $a \neq \mathbf{0}$ and $\Phi_F(\mathbf{0}) = \mathbf{0}$, $\varphi_F(\mathbf{0}) = 1$. Here $x \cdot y = x_1y_1 + \ldots + x_ny_n$ denotes the inner product of vectors $x, y \in \mathbb{F}_2^n$.

Let A be an affine function from $\mathbb{F}_2^n$ to itself and $L(x) = A(x) + A(\mathbf{0})$. Then

$$\gamma_{F+A}(a, b) = \gamma_F(a, b + L(a)) = \Phi_F(a) \cdot \big(b + L(a)\big) + \varphi_F(a) + 1$$

$$= \gamma_F(a, b) + \Phi_F(a) \cdot L(a).$$

Thus, F and $F + A$ are differentially equivalent if and only if

$$\Phi_F(a) \cdot L(a) = 0 \text{ for all } a \in \mathbb{F}_2^n. \tag{2}$$

The equalities (2) form the system of equations over n^2 binary variables $\ell_{i,j}$, $i, j = 1, \ldots, n$, if we represent L as $L(x) = (\sum_{i=1}^n \ell_{1,i}x_i, \ldots, \sum_{i=1}^n \ell_{n,i}x_i)$. Let r be rank of this system. Then there exist exactly 2^{n^2-r+n} affine functions A such that F and $F + A$ are differentially equivalent.

We computationally study ranks of system (2) for all known EA-equivalence classes of quadratic APN functions in $2, \ldots, 8$ variables. Recall that the exact numbers of EA-equivalence classes of quadratic APN functions are known for all n from 2 to 6 ([5], [6], [17]). For n equal to 7, 8 there are known partial results from [36] and updated version of [35]. Our computational results are listed in Table 4. As we can see for almost all considered EA-equivalence classes in n variables with representative F there exist exactly 2^{2n} trivial affine functions A such that F and $F + A$ are differentially equivalent. The exceptional cases are the following functions in even number of variables:

$n = 4$: APN Gold function x^3;

$n = 6$: 4th APN function from [6] $u^7x^3 + x^5 + u^3x^9 + u^4x^{10} + x^{17} + u^6x^{18}$;

$n = 8$: APN Gold function x^9.

Table 4: Numbers of affine functions A on $\mathbb{F}_2^n$ such that F and $F+A$ are differentially equivalent, where F is a EA-equivalence representative of quadratic APN functions.

n	# EA classes	rank of system (2)	# affine functions A: $F + A \in \mathcal{DE}_F$
2	1	2	2^4
3	1	6	2^6
4	1	10	2^{10}
5	2	for all 2 classes: 20	for all 2 classes: 2^{10}
6	13	for 12 classes: 30; for 1 class: 29	for 12 classes: 2^{12}; for 1 class: 2^{13}
7	≥ 487	for all known 487 classes: 42	for all known 487 classes: 2^{14}
8	≥ 8179	for 1 class from known 8179: 52 for other 8178 classes: 56	for 1 class from known 8179: 2^{20} for other 8178 classes: 2^{16}

6 Conclusion

In this paper we introduced the notion of differential equivalence of vectorial Boolean functions and considered its basic properties in general and quadratic cases. We started to analyze differential equivalence classes of APN Gold functions by studying functions that are obtained by adding affine functions to a given Gold function. This theoretical result and computer calculations for small number of variables shown us a remarkable property of APN Gold functions that is not usual for almost all known quadratic APN functions. Also, we formulated several conjectures about differential equivalence of quadratic APN functions that would be interesting to study further. But the most exciting problem that remains open about differential equivalence is the existence of two differentially equivalent APN functions that are not CCZ-equivalent. The positive answer to this question can give a new method for constructing APN functions inequivalent to the known ones.

Acknowledgements. We thank Natalia Tokareva, Nikolay Kolomeec and Valeriya Vitkup for fruitful discussions relating to this work and their valuable comments on the paper.

References

[1] Bending T. D., Fon-Der-Flaass D.: Crooked functions, bent functions, and distance regular graphs. Electron. J. Combin. 5 (1) (1998) R34.

[2] Berger T.P., Canteaut A., Charpin P., Laigle-Chapuy Y.: On almost perfect nonlinear functions over $\mathbb{F}_2^n$. IEEE Trans. Inf. Theory 52, 4160–4170 (2006).

[3] Beth T., Ding C.: On almost perfect nonlinear permutations. Advances in Cryptology-EUROCRYPT'93, Lecture Notes in Computer Science, 765, Springer-Verlag, New York, pp. 65–76 (1993).

[4] Bierbrauer J., Kyureghyan G. M.: Crooked binomials. Des. Codes Cryptogr. 46, 269–301 (2008).

[5] Brinkman M., Leander G.: On the classification of APN functions up to dimension five. Proc. of the International Workshop on Coding and Cryptography 2007 dedicated to the memory of Hans Dobbertin. Versailles, France, 39–48 (2007).

[6] Browning K. A., Dillon J. F., Kibler R. E., McQuistan M. T.: APN Polynomials and Related Codes. Journal of Combinatorics, Information and System Science, Special Issue in honor of Prof. D.K Ray-Chaudhuri on the occasion of his 75th birthday, vol. 34, no. 1-4, pp. 135–159 (2009).

[7] 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, v. 518, pp. 33–42 (2010).

[8] Budaghyan L., Carlet C.: CCZ-equivalence of single and multi output Boolean functions. Post-proceedings of the 9-th International Conference on Finite Fields and Their Applications Fq'09, Contemporary Math., AMS, v. 518, pp. 43–54 (2010).

[9] Budaghyan L., Carlet C., Leander G.: Constructing new APN functions from known ones. Finite Fields and Their Applications. 15(2), 150–159 (2009).

[10] Budaghyan L., Carlet C., Pott A.: New classes of almost bent and almost perfect nonlinear polynomials. IEEE Trans. Inform. Theory 52, 1141–1152 (2006).

[11] Canteaut A., Charpin P., Dobbertin H.: Binary m-sequences with three-valued crosscorrelation: a proof of Welch conjecture, IEEE Trans. Inf. Theory. 46(1), 4–8 (2000).

[12] Carlet C.: Open Questions on Nonlinearity and on APN Functions. Arithmetic of Finite Fields, Lecture Notes in Computer Science. 9061, 83–107 (2015).

[13] Carlet C., Charpin P., Zinoviev V.: Codes, bent functions and permutations suitable for DES-like cryptosystems. Des. Codes Cryptogr. 15, 125–156 (1998).

[14] Dobbertin H.: Almost perfect nonlinear functions over $GF(2^n)$: the Niho case. Inform. and Comput. 151, 57–72 (1999).

[15] Dobbertin H.: Almost perfect nonlinear power functions on $GF(2^n)$: the Welch case. IEEE Trans. Inf. Theory. 45(4), 1271–1275 (1999).

[16] 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).

[17] Edel Y.: Quadratic APN functions as subspaces of alternating bilinear forms. Contact Forum Coding Theory and Cryptography III, Belgium (2009), pp. 11–24 (2011).

[18] Edel Y., Pott A.: A new almost perfect nonlinear function which is not quadratic. Advances in Mathematics of Communications. 3(1), 59–81 (2009).

[19] Glukhov M. M.: On the matrices of transitions of differences for some modular groups. Mathematical Aspects of Cryptography. 4(4), 27–47 (2013) (in Russian).

[20] Glukhov M. M.: On perfect and almost perfect nonlinear functions. Mathematical Aspects of Cryptography. To appear (2016) (in Russian).

[21] Gold R.: Maximal recursive sequences with 3-valued recursive crosscorrelation functions. IEEE Trans. Inform. Theory. 14, 154–156 (1968).

[22] Gorodilova A.: A characterization of almost perfect nonlinear functions in terms of subfunctions. Diskretnaya Matematika, 27(3), 3–16 (2015) (in Russian).

[23] Hernando F., McGuire G.: Proof of a conjecture on the sequence of exceptional numbers, classifying cyclic codes and APN functions. Journal of Algebra. 343(1), 78–92 (2011).

[24] Hollmann H., Xiang Q.: A proof of the Welch and Niho conjectures on crosscorrelations of binary m-sequences. Finite Fields and Their Applications. 7, 253–286 (2001).

[25] Hou X.-D.: Affinity of permutations of $\mathbb{F}_2^n$. Discret. Appl. Math. 154, 313–325 (2006).

[26] 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, LNCS, vol. 673, Berlin, Springer-Verlag, pp. 180–194 (1993).

[27] Kasami T.: The weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes. Inform. and Control. 18, 369–394 (1971).

[28] Kyureghyan G.: Crooked maps in F_2^n. Finite Fields Their Appl. 13(3), 713–726 (2007).

[29] Nyberg K.: Perfect nonlinear S-boxes. In: Davies, D.W. (ed.) EUROCRYPT 1991. LNCS, vol. 547, pp. 378–386. Springer, Heidelberg (1991).

[30] Nyberg K.: Differentially uniform mappings for cryptography. Advances in Cryptography, EUROCRYPT'93, Lecture Notes in Computer Science. 765, 55–64 (1994).

[31] Pott A.: Almost perfect and planar functions. Des. Codes Cryptogr. 78, 141–195 (2016).

[32] Tuzhilin M. E.: APN functions. Prikladnaya Diskretnaya Matematika. 3, 14–20 (2009) (in Russian).

[33] Vitkup V.: On symmetric properties of APN functions. Journal of Applied and Industrial Mathematics. 10(1), To appear (2016).

[34] Yoshiara S.: Equivalences of quadratic APN functions. J. Algebr. Comb. 35, 461–475 (2012).

[35] Yu Y., Wang M., Li Y.: A matrix approach for constructing quadratic apn functions. Cryptology ePrint Archive, Report 2013/007 (2013). http://eprint.iacr.org/.

[36] Yu Y., Wang M., Li Y.: A matrix approach for constructing quadratic APN functions. Des. Codes Cryptogr. 73, 587–600 (2014).