RAD HRVATSKE AKADEMIJE ZNANOSTI I UMJETNOSTI MATEMATIČKE ZNANOSTI

M. Calderini, L. Budaghyan and C. Carlet

On known constructions of APN and AB functions and their relation to each other

Manuscript accepted for publication

ON KNOWN CONSTRUCTIONS OF APN AND AB FUNCTIONS AND THEIR RELATION TO EACH OTHER

Marco Calderini, Lilya Budaghyan and Claude Carlet

Abstract. This work is dedicated to APN and AB functions which are optimal against differential and linear cryptanlysis when used as S-boxes in block ciphers. They also have numerous applications in other branches of mathematics and information theory such as coding theory, sequence design, combinatorics, algebra and projective geometry. In this paper we give an overview of known constructions of APN and AB functions, in particular, those leading to infinite classes of these functions. Among them, the bivariate construction method, the idea first introduced in 2011 by the third author of the present paper, turned out to be one of the most fruitful. It has been known since 2011 that one of the families derived from the bivariate construction contains the infinite families derived by Dillon's hexanomial method. Whether the former family is larger than the ones it contains has stayed an open problem which we solve in this paper. Further we consider the general bivariate construction from 2013 by the third author and study its relation to the recently found infinite families of bivariate APN functions.

1. Introduction

Vectorial Boolean functions are mappings between the vector spaces $\mathbb{F}_2^n$ and $\mathbb{F}_2^m$ for some positive integers n and m, where $\mathbb{F}_2$ is the finite field with two elements. We shall call them (n, m)-functions when we will need to specify the numbers of input and output bits. These functions play an important role in many different areas of mathematics, computer science and engineering. In particular, (n, m)-functions are of critical importance in the field of cryptography: virtually, all modern block ciphers incorporate one or several (n, m)-functions (usually referred to as "substitution boxes" - in brief, "S-boxes" - in

2010 *Mathematics Subject Classification.* 94A60, 94A15.

Key words and phrases. Boolean functions, almost perfect nonlinear (APN) functions, almost bent (AB) functions, cryptography.

this context) as their only nonlinear components, and as such, the security of the encryption directly depends on the properties of the (n, m)-functions.

Various properties measuring the resistance of an (n, m)-function to different kinds of cryptanalysis have been defined, including nonlinearity, differential uniformity, boomerang uniformity, algebraic degree, and so forth. One of the most efficient attacks that can be employed against block ciphers, the differential cryptanalysis [5], is based on the study of how differences in an input can affect the resultant difference at the output. The resistance to differential attacks for a function F from $\mathbb{F}_2^m$ to $\mathbb{F}_2^m$, used as an S-box in the cipher, is high when the value

$$\delta_F = \max_{a,b \in \mathbb{F}_2^m, a \neq 0} |\{x \in \mathbb{F}_2^m : F(x+a) + F(x) = b\}|$$

is small. When $n = m$, which is the main case of our interest, the differential uniformity of any (n, n)-function is at least 2, and the (n, n)-functions meeting this bound are called almost perfect nonlinear (APN). Another powerful attack on block ciphers is linear cryptanalysis [48] which relies on the search for linear approximations to the action of the cipher. The so-called almost bent (AB) functions are optimal against this attack [33]. Every AB function is also APN, while the converse is not true in general.

Discovering new examples and constructions of APN and AB functions is thus a matter of significant practical importance since they enable the design of new block ciphers. APN and AB functions are interesting from a theoretical point of view as well, as they correspond to optimal objects within other areas of mathematics and computer science, e.g. coding theory, combinatorics, and projective geometry.

The APNness and ABness of functions are preserved by some equivalence relations, mainly the so-called CCZ- and EA-equivalences, and it is important when several functions are considered, to determine whether they correspond to each others by such equivalences. CCZ-equivalence is the most general known equivalence relation preserving APN and AB properties while all other known equivalence relations for these functions are just particular cases of CCZ-equivalence[1]. Classification of APN and AB functions, up to CCZ- and EA-equivalences, is a hard open problem. Complete classification is known only for $n \leq 5$, see [9]. Finding new constructions of APN functions is difficult too. APN functions have been known and studied since the early 90's [49] but, to date, only six infinite families of APN monomials (see the definition of this term in Section 2) and more or less 15 (depending on how we count) infinite families of quadratic APN polynomials are known. Together, these cover only a tiny fraction of all APN functions: for instance, more than 20 000

[1] EA-equivalence needs however to be considered as well, because CCZ-equivalence is much more difficult to verify and/or to enforce than EA-equivalence. The first step when checking if two functions are really different is then to see whether they are EA-inequivalent.

CCZ-inequivalent APN functions have been determined over $\mathbb{F}_2^8$ [2, 53], yet none of them has been classified into general constructions yet. Finding new examples of infinite families is an area of intense ongoing research. Tables 1 and 2 list all currently known infinite families of APN functions. The first four cases in Table 1, and, for n odd, all cases in Table 2 are also AB. All families in Tables 1 and 2 are pairwise CCZ-inequivalent for general n [17, 34, 41].

In this paper we recall known constructions of APN and AB functions, in particular, those which have led to infinite classes. Then we consider the bivariate and Dillon's hexanomial constructions and prove that families of APN functions derived by these methods in [19, 29] coincide with each other. Further we study the relation between the general bivariate construction of [30] with families F10 and F12. We show that, while containing families F10 and F12, the construction given in [30] can lead (at least in small dimensions) to APN functions that are not included in F10 and F12, nor in any other known APN family. This shows that this general construction by the third author of the present paper may potentially lead to further infinite families.

In the last part, we consider a new bivariate construction over $\mathbb{F}_{2^{2m}}$ based on bivariate projective polynomials, that is, polynomials of the type $ax^{q+1} + bx^qy + cxy^q + dy^{q+1} \in \mathbb{F}_{2^m}[x, y]$, where q is a power of 2. Using, these polynomials Göloğlu [41] and Kaleyski and Li [43] were able to provide new families of APN functions F14, F15 and the one of Theorem 7.3. We will discuss some equivalence properties of the APN functions coming from this approach, and we will show that the family discovered by Kaleyski and Li is included in F15.

2. Preliminaries

Let n be a positive integer. We denote by $\mathbb{F}_{2^n}$ the finite field with 2^n elements, and by $\mathbb{F}_{2^n}^*$ the set of its non-zero elements, i.e. its multiplicative group. For $m \mid n$, we denote by $Tr_n^m : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ the trace function $Tr_n^m(x) = \sum_{i=0}^{n/m-1} x^{2^{mi}}$ from $\mathbb{F}_{2^n}$ into its subfield $\mathbb{F}_{2^m}$ (simply denoted by Tr when $m = 1$).

It is convenient to identify the vector space $\mathbb{F}_2^n$ with the finite field $\mathbb{F}_{2^n}$ and to consider an (n, n)-functions F as a mapping $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. Any such function can be expressed as a polynomial of the form

$$F(x) = \sum_{i=0}^{2^n-1} a_i x^i,$$

for $a_i \in \mathbb{F}_{2^n}$. This is the *univariate representation* of F, and it is unique. Function F is then called a *power function* or a *monomial function* if its univariate representation consists in one single monomial. The *algebraic degree* of F, denoted by $\deg(F)$, is the largest binary weight of an exponent i with $a_i \neq 0$ in the univariate representation, where the *binary weight* of an integer is the number of ones in its binary notation, i.e. the minimum number of distinct powers of two that sum up to it. Functions of algebraic degree 1, resp, 2, resp. 3 are called *affine*, resp. *quadratic*, resp. *cubic.* An affine function F satisfying $F(0) = 0$ is called *linear.*

Given an (n, n)-function F, we denote by $\Delta_F(a, b)$ the number of solutions x to the equation $D_aF(x) = b$, where $D_aF(x) = F(x + a) + F(x)$ is the *derivative* of F in direction $a \in \mathbb{F}_{2^n}$. The largest value of $\Delta_F(a, b)$ among all $a \neq 0$ and all b is denoted by Δ_F and is called the *differential uniformity* of F. If $\Delta_F = 2$, we say that F is *almost perfect nonlinear (APN).*

The *Walsh transform* of $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is the integer-valued function

$$W_F(a, b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{b \cdot F(x) + a \cdot x}$$

for $a, b \in \mathbb{F}_{2^n}$, where the inner product "$\cdot$" can be defined as $a \cdot b = Tr(ab)$ for $a, b \in \mathbb{F}_{2^n}$ without loss of generality. Function $b \cdot F$ for $b \neq 0$ is called a *component function* of F. The values of $W_F(a, b)$ for $a, b \in \mathbb{F}_{2^n}$ are the *Walsh coefficients* of F, and the multiset $W_F = \{W_F(a, b) : a, b \in \mathbb{F}_{2^n}\}$ is called the *Walsh spectrum* of F. The multiset $\{|W_F(a, b)| : a, b \in \mathbb{F}_{2^n}\}$ of the absolute values of the Walsh transform is the *extended Walsh spectrum.* If the Walsh spectrum of F consists of values $0, \pm 2^{\frac{n+1}{2}}$ then the function F is called AB. Such AB functions exist for n odd only and contribute optimally to the resistance against linear cryptanalysis when they are used as S-boxes. Besides, every AB function is APN [33], and in the n odd case, any quadratic function is APN if and only if it is AB [32]. Comprehensive surveys on APN and AB functions can be found in [12, 31].

Since the number of distinct (n, n)-functions, viz. $(2^n)^{2^n}$, grows rapidly with the dimension, (n, n)-functions are classified only up to a suitable equivalence relation which preserves the properties being studied. The most general known equivalence relation which preserves the differential uniformity and the extended Walsh spectrum (and, therefore, the APN and AB properties) is the so-called *Carlet-Charpin-Zinoviev equivalence (CCZ-equivalence)*: we say that two (n, n)-functions F and G are CCZ-equivalent if there is an affine permutation $\mathcal{L}$ of $\mathbb{F}_{2^n}^2$ which maps the graph $\mathcal{G}_F = \{(x, F(x)) : x \in \mathbb{F}_{2^n}\}$ of F to the graph $\mathcal{G}_G$ of G. Deciding whether two given functions F and G are CCZ-equivalent is a difficult problem in general, mathematically and computationally, and is typically resolved via code isomorphism. More precisely, a linear code $\mathcal{C}_F$ with the generating matrix

$$\mathcal{C}_F = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 0 & \alpha & \dots & \alpha^{2^n-1} \\ F(0) & F(\alpha) & \dots & F(\alpha^{2^n-1}) \end{pmatrix}$$

can be associated with any given (n, n)-function F, where α is a primitive element of $\mathbb{F}_{2^n}$. Then F and G are CCZ-equivalent if and only if $\mathcal{C}_F$ and $\mathcal{C}_G$ are isomorphic [10].

Various CCZ-invariants, i.e. properties or parameters that remain invariant under CCZ-equivalence, can be used to show that a pair of (n, n)-functions is CCZ-inequivalent. These include the differential uniformity and the extended Walsh spectrum.

A special cases of CCZ-equivalence is the so-called *extended affine equivalence (EA-equivalence)*. Two (n, n)-functions F and G are said to be EA-equivalent if $G = A_1 \circ F \circ A_2 + A$ for affine $A_1, A_2, A : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ with A_1, A_2 bijective. EA-equivalence is more restrictive than CCZ-equivalence; for instance, every permutation is CCZ-equivalent to its inverse and is in general not EA-equivalent to it. Also, the algebraic degree of a function is preserved by EA-equivalence (when it is larger than 1) but not by CCZ-equivalence. If we consider two power functions for their CCZ-equivalence then it is enough to restrict to cyclotomic equivalence: two power functions $F(x) = x^d$ and $G(x) = x^e$ over $\mathbb{F}$, where d, e, n are positive integers, are said to be *cyclotomic equivalent* if $d \equiv 2^k e \mod (2^n - 1)$ for some positive integer k, or if $d^{-1} \equiv 2^k e \mod (2^n - 1)$ for some positive integer k in the case that $\gcd(d, 2^n - 1) = 1$, with d^{-1} being the multiplicative inverse of d modulo $2^n - 1$. Cyclotomic equivalence has the advantage of being significantly simpler to test than both EA- and CCZ-equivalences.

TABLE 1. Known APN power functions x^d over $\mathbb{F}_{2^n}$

Functions	Exponents d	Conditions	Degree	In
Gold	$2^i + 1$	$\gcd(i,n)=1$	2	[40, 49]
Kasami	$2^{2i} - 2^i + 1$	$\gcd(i,n)=1$	$i+1$	[42, 44]
Welch	$2^t + 3$	$n = 2t + 1$	3	[35]
Niho	$2^t + 2^{\frac{t}{2}} - 1$, t even $2^t + 2^{\frac{3t+1}{2}} - 1$, t odd	$n = 2t + 1$	$\frac{t+2}{2}$ $t+1$	[36]
Inverse	$2^{2t} - 1$	$n = 2t + 1$	$n - 1$	[4, 49]
Dobbertin	$2^{4i} + 2^{3i} + 2^{2i} + 2^i - 1$	$n = 5i$	$i + 3$	[37]

3. Overview on known constructions of APN and AB functions

There are several known constructions of APN and AB functions which have led to infinite families of these functions. Power functions were the first to be considered, and several infinite classes practically followed from coding theory and sequence design where APN and AB functions define optimal codes and sequences well-studied there for several decades before the notions

Table 2. Known classes of quadratic APN polynomial over $\mathbb{F}_{2^n}$ CCZ-inequivalent to power functions

$N°$	Functions	Conditions	In
F1-F2	$x^{2^s+1} + u^{2^k-1}x^{2^{ik}+2^{mk+s}}$	$n = pk$, gcd$(k,p)=$ gcd(s,pk)=1, $p \in \{3,4\}$, $i = sk$ mod p, $m = p - i$, $n \geq 12$, u primitive in $\mathbb{F}_{2^n}^*$	[20]
F3	$sx^{q+1} + x^{2^i+1} + x^{q(2^i+1)}$ $+cx^{2^iq+1} + c^qx^{2^i+q}$	$q = 2^m$, $n = 2m$, gcd(i,m)=1, $c \in \mathbb{F}_{2^n}$, $s \in \mathbb{F}_{2^n} \setminus \mathbb{F}_q$, $X^{2^i+1} + cX^{2^i} + c^qX + 1$ has no solution x such that $x^{q+1} = 1$	[19]
F4	$x^3 + a^{-1}\,Tr(a^3x^9)$	$a \neq 0$	[21]
F5	$x^3 + a^{-1}\,Tr_n^3(a^3x^9 + a^6x^{18})$	$3\|n$, $a \neq 0$	[22]
F6	$x^3 + a^{-1}\,Tr_n^3(a^6x^{18} + a^{12}x^{36})$	$3\|n$, $a \neq 0$	[22]
F7-F9	$ux^{2^s+1} + u^{2^k}x^{2^{-k}+2^{k+s}} +$ $vx^{2^{-k}+1} + wu^{2^k+1}x^{2^s+2^{k+s}}$	$n = 3k$, gcd$(k,3)=$ gcd$(s,3k)$=1, $v, w \in \mathbb{F}_{2^k}$, $vw \neq 1$, $3\|(k+s)$ u primitive in $\mathbb{F}_{2^n}^*$	[7, 8]
F10	$(x + x^{2^m})^{2^i+1} +$ $u'(ux + u^{2^m}x^{2^m})^{(2^i+1)2^j} +$ $u(x + x^{2^m})(ux + u^{2^m}x^{2^m})$	$n = 2m$, $m \geq 2$ even, gcd$(i,m) = 1$ and $j \geq 2$ even u primitive in $\mathbb{F}_{2^n}^*$, $u' \in \mathbb{F}_{2^m}$ not a cube	[54]
F11	$L(x)^{2^i}x + L(x)x^{2^i}$	$n = km$, $m > 1$, gcd$(n,i) = 1$ $L(x) = \sum_{j=0}^{k-1} a_jx^{2^{jm}}$ satisfies the conditions in Theorem 6.3 of [13]	[13]
F12	$u(u^qx + x^qu)(x^q + x) + (u^qx + x^qu)^{2^{2i}+2^{3i}}$ $+a(u^qx + x^qu)^{2^{2i}}(x^q + x)^{2^i} + b(x^q + x)^{2^i+1}$	$q = 2^m$, $n = 2m$, gcd(i,m)=1, u primitive in $\mathbb{F}_{2^n}^*$ $X^{2^i+1} + aX + b$ has no solution over $\mathbb{F}_{2^m}$	[51]
F13	$x^3 + ax^{2^k(2^i+1)} + bx^{3\cdot 2^m} + cx^{2^{n+k}(2^i+1)}$	$n = 2m = 10, (a,b,c) = (\beta,0,0), i = 3, k = 2, \mathbb{F}_4^* = \langle\beta\rangle$ $n = 2m, m$ odd, $3 \nmid m, (a,b,c) = (\beta,\beta^2,1)$, $\mathbb{F}_4^* = \langle\beta\rangle$, $i \in \{m-2, m, 2m-1, (m-2)^{-1} \mod n\}$	[25]
F14	$u[(u^qx + x^qu)^{2^i+1} + (u^qx + x^qu)(x^q + x)^{2^i} + (x^q + x)^{2^i+1}]$ $+(u^qx + x^qu)^{2^{2i}+1} + (u^qx + x^qu)^{2^{2i}}(x^q + x) + (x^q + x)^{2^{2i}+1}$	$q = 2^m$, $n = 2m$, gcd$(3i,m)$=1, u primitive in $\mathbb{F}_{2^n}^*$	[41]
F15	$u[(u^qx + x^qu)^{2^i+1} + (u^qx + x^qu)(x^q + x)^{2^i} + (x^q + x)^{2^i+1}]$ $+(u^qx + x^qu)^{2^{3i}}(x^q + x) + (u^qx + x^qu)(x^q + x)^{2^{3i}}$	m odd, $q = 2^m$, $n = 2m$, gcd$(3i,m)$=1, u primitive in $\mathbb{F}_{2^n}^*$	[41]

of APN and AB functions were defined. These were Gold, Kasami, Welch and Niho APN power functions which all have so called classical Walsh spectrum, that is, they are AB when n is odd and for n even the Walsh coefficients take the values in the set $\{0, \pm 2^{\frac{n}{2}}, \pm 2^{\frac{n+2}{2}}\}$.

The inverse function is APN when n is odd and differentially 4-uniform when n is even. The inverse APN function is not AB since it has the algebraic degree $n-1$ while the algebraic degree of any AB function is not greater than $(n+1)/2$ (see [32]). The Walsh spectrum of the inverse function was determined by Lachaud and Wolfmann in [47]. If n is even then it consists of all integers $s = 0 \mod 4$ in the range $-2^{\frac{n}{2}+1}, ..., 2^{\frac{n}{2}+1}$ and, therefore, the inverse function has the best known nonlinearity for n even.

The last case of APN power functions was found in 1999 by Canteaut and Dobbertin, and proven by Dobbertin in 2000. It is shown in [28] that this function is not AB, because at least one of its Walsh transform values is not divisible by $2^{2n/5+1}$. A conjecture has been recently proposed in [16] on the set of those Walsh values of the Dobbertin function, depending on the parity of n. It was conjectured by Dobbertin in 2000 that the lists of APN and AB power functions were complete and this conjecture stays open up to now.

APN power functions are permutations for n odd and 3-to-1 for n even (as proved by Dobbertin and reported in [31]). Power APN and AB functions are considered up to cyclotomic equivalence since according to [34] two power functions are CCZ-equivalent if and only if they are cyclotomic equivalent. It is easy to observe that cyclotomic equivalence preserves the pair of algebraic degrees of the power function and its inverse (when it exists). Hence, the 6 known families of APN power functions are pairwise CCZ-inequivalent since, in general, they (and their inverses when they exist) have different algebraic degrees.

One more reason why the first found APN functions were power functions is that checking the APN and AB properties of power functions is easier than in the case of arbitrary polynomials. If F is a power function, that is $F(x) = x^d$, then F is APN if and only if the derivative D_1F is a two-to-one mapping. Indeed, since for any $a \neq 0$

$$D_aF(x) = (x + a)^d + x^d = a^d D_1F(x/a)$$

then D_aF is a two-to-one mapping if and only if D_1F is two-to-one.
Besides, the function $F(x) = x^d$ is AB if and only if $W_F(a, b) \in \{0, \pm 2^{\frac{m+1}{2}}\}$ for $a \in \mathbb{F}_2$, $b \in \mathbb{F}_{2^n}^*$, since $W_F(a, b) = W_F(1, a^{-d}b)$ for $a \in \mathbb{F}_{2^n}^*$.

The first successful attempt to construct non-power APN functions was by enforcing the CCZ-equivalence [23]. Before that work, APN and AB functions were considered up to EA-equivalence and taking inverses for permutations. In [23] it was proven that CCZ-equivalence is more general than the two aforementioned transformations when applied to the Gold power APN functions. This led to the first classes of APN and AB functions EA-inequivalent to power functions which was also the first evidence of existence of such functions. In addition, it disproved a conjecture from [32] that all AB functions are EA-equivalent to permutations [23] . Further it was also proven in [23] that the number of different (up to EA-equivalence) classes of AB functions is infinite. The recent works [18, 21] show that CCZ-equivalence can be more general than EA-equivalence together with inverse transformation not only for Gold power functions but also for other quadratic APN polynomials and for APN polynomials CCZ-inequivalent to both quadratic and power functions. However, it is conjectured in [18] (based on computational data on small dimensions) that for non-Gold power APN functions, CCZ-equivalence coincides with EA-equivalence taken together with the inverse transformation. For the case of the inverse function, such a conjecture has been recently confirmed in [46].

Using CCZ-equivalence for constructing APN functions turned out to be a very fruitful idea: it did not only allow to increase the algebraic degree of APN functions but also to construct APN permutations in even dimensions and by that to solve one of the main and hardest problems related to APN functions. Indeed, in 2006, Dillon and his team applied CCZ-equivalence to a quadratic

APN mapping in dimension 6 and obtained the first and the only currently known APN permutation in even dimension [11]. An interesting fact is that quadratic APN functions, and more generally APN functions with quadratics components, in even dimension are never permutations because they have (partially-)bent component functions (see [27, 50]) but CCZ-equivalence allows to increase the algebraic degree and can mix the Walsh spectrum such that none of the component functions of the resulted map are (partially-)bent.

By construction, the APN and AB polynomials of [23] were CCZ-equivalent to power functions. The first idea leading to APN functions CCZ-inequivalent to power functions, introduced in [38], was to consider a sum of two power functions, and more exactly of two Gold APN maps, which led to two sporadic examples in dimensions 10 and 12. This idea was successfully implemented mathematically in [20] for constructing the first infinite families of APN and AB functions: two families of APN binomials CCZ-inequivalent to power functions for dimensions n divisible by 3 and 4. These classes of binomials proved the existence of AB functions CCZ-inequivalent to power functions. Besides, they were the first counterexamples for the conjecture of [32] on nonexistence of quadratic AB functions inequivalent to the Gold maps [20].

Moreover, these families of binomials have also contributed to the study of so-called crooked functions. An (n, n)-function F is called crooked if $F(x)+F(y)+F(z)+F(x+y+z) \neq 0$ for any three distinct elements x, y, z, $F(0) = 0$, and $F(x) + F(y) + F(z) + F(x + a) + F(y + a) + F(z + a) \neq 0$ for any $a \neq 0$ and x, y, z arbitrary [3]. Note, that crooked mappings are permutations, since if $F(x) = F(x + a)$ for some $a \neq 0$, then considering $z = y = x$, we would have $F(x) + F(y) + F(z) + F(x + a) + F(y + a) + F(z + a) = 0$. On one hand, every crooked function gives rise to a distance regular rectagraph of diameter 3, and on the other hand every quadratic AB permutation is crooked [3]. The converse is not known, that is, whether a crooked function is necessarily a quadratic AB permutation. A rectagraph is a graph without triangles in which every pair of vertices at distance 2 lies in a unique 4-cycle. There are not too many constructions of rectagraphs known, especially rectagraphs of small diameter. Hence, the construction of such functions would provide not only interesting building blocks for symmetric cryptosystems but would also provide new distance regular rectagraphs. Nowadays only two families of crooked functions are known: one is the family of Gold functions with n odd and the other one is the family of APN binomials with n odd and divisible by 3 from [20].

The idea of adding new quadratic terms to a known APN function, to construct a new one, was further applied in [7, 8, 25]. In the first two papers the authors generalize one of the two families of APN binomials (for n divisible by 3) to trinomials and quadrinomials. An infinite class of APN quadrinomials constructed in the third paper, covered the APN binomial $x^3 + ax^{36}$ over

$\mathbb{F}_2^{10}$ (where a has the order 3 or 93) of [38], which was an open case for a generalization into a family since 2006.

In [21], a family of APN and AB functions $x^3 + Tr(x^9)$ over $\mathbb{F}_2^n$ was constructed using an observation that for any APN function F and any Boolean function f the sum $F + f$ can have differential uniformity at most 4. The functions of this family served as the first examples of APN and AB polynomials CCZ-inequivalent to power functions whose all coefficients were in $\mathbb{F}_2$. Moreover it is still the only family of APN and AB polynomials CCZ-inequivalent to power functions which is defined for all n (recall that in case of power APN and AB functions only the Gold function x^3 possesses this property). Although simple, the idea to consider the sum $F + f$ have not yet provided any further infinite families of APN functions. However, following the aforementioned work, functions of a more general form

$$F(x) = L_1(x^3) + L_2(x^9)$$

where L_1 and L_2 are linear functions from $\mathbb{F}_{2^n}$ to itself, were considered in [22]. In particular, it was proven there that, if n is even and the function $L_1(x) + L_2(x^3)$ is a permutation of $\mathbb{F}_{2^n}$, then F is APN. This approach gave two more infinite families of APN and AB functions F5 and F6 in Table 2.

Note that if the output of $F(x) = x^3 + Tr(x^9)$ is decomposed over an $\mathbb{F}_2$-basis of $\mathbb{F}_{2^n}$, in which the (say) last element equals the unit 1 of $\mathbb{F}_{2^n}$, function $x^3 + Tr(x^9)$, now valued in $\mathbb{F}_2^n$, differs from x^3 by only its last coordinate function. This led in [39] (on the basis of an idea due to Dillon) to the so-called switching construction, in which a known APN function F is changed into a function G by modifying one of its coordinate functions. If we view the functions as valued in $\mathbb{F}_{2^n}$, we have the following equivalent definition: functions F and G belong to the same switching class if there exist an element $u \in \mathbb{F}_{2^n}^*$ and a Boolean function f over $\mathbb{F}_{2^n}$ such that $G(x) = F(x) + uf(x)$. It is easily seen that if F is APN then G has differential uniformity at most 4. In [39] an APN (6,6)-function CCZ inequivalent to power functions and to quadratic functions was deduced by computer search. This is the only known function with such properties, but note that this APN function had been in fact previously found in [9] (the authors had however missed that it is inequivalent to quadratic functions). It seems fair to call it the *Brinkmann-Leander-Edel-Pott function.* It equals, given α primitive:

$$\begin{aligned}&x^3 + \alpha^{17}(x^{17} + x^{18} + x^{20} + x^{24}) + \alpha^{14}\, Tr_1^2(x^{21}) + \alpha^{14}\, Tr_1^3(\alpha^{18}x^9)\\&+\alpha^{14}\, Tr_1^6\,(\alpha^{52}x^3 + \alpha^6x^5 + \alpha^{19}x^7 + \alpha^{28}x^{11} + \alpha^2x^{13}).\end{aligned}$$

As shown in [10], one of the ways to construct APN polynomials is to consider quadratic hexanomials of the type

$$F(x) = x(Ax^2 + Bx^q + Cx^{2q}) + x^2(Dx^q + Ex^{2q}) + Gx^{3q} \tag{3.1}$$

over $\mathbb{F}_{2^{2m}}$ with $q = 2^m$. These polynomials are good candidates for being differentially 4-uniform, and potentially APN. This approach gave new examples of quadratic APN functions over $\mathbb{F}_{2^6}$ and $\mathbb{F}_{2^8}$ which are CCZ-inequivalent to power functions [10]. Later, several generalizations of this method were proposed in [19], in particular, the following infinite family, corresponding to F3, was deduced:

Theorem 3.1. *Let n and i be any positive integers, $n = 2m$, $\gcd(i, m) = 1$, and $c, d \in \mathbb{F}_{2^n}$ be such that $d \notin \mathbb{F}_{2^m}$. Then, the hexanomial*

$$H(x) = dx^{2^i(2^m+1)} + x^{(2^m+1)} + (x^{2^i+1} + x^{2^m(2^i+1)} + cx^{2^{m+i}+1} + c^{2^m}x^{2^i+2^m})$$

is APN if and only if the equation

$$x^{2^i+1} + cx^{2^i} + c^{2^m}x + 1 = 0$$

has no solution x such that $x^{2^m+1} = 1$.

While trying to find an equivalence notion that preserves the differential uniformity and is more general than CCZ-equivalence, the authors of [13] obtained instead a new construction method which they called isotopic shift and which led to the APN family F11. They considered the so-called isotopic equivalence which is defined for quadratic planar functions only, where a function F from $\mathbb{F}_{p^n}$ to itself is planar if $F(x + a) - F(x)$ is a permutation for every non-zero $a \in \mathbb{F}_{p^n}$ (p must be odd then). Isotopic equivalence is known to be more general than CCZ-equivalence and, for planar functions, CCZ-equivalence coincides with EA-equivalence [24]. Isotopic equivalence cannot be extended directly to APN functions in fields of even characteristic but may be potentially used as an analogue with some modifications or restrictions. As a result of this study the isotopic shift construction is obtained: for a function F and a linear function L, the isotopic shift of F by L is the map $F_L(x) = F(x + L(x)) - F(x) - F(L(x))$. Whether it can lead to an equivalence relation, by finding more restrictions, is a matter of further investigations. However, it turned out that this construction may be also used for construction of new (up to isotopic equivalence) planar functions [15]. Some generalisations of the isotopic shift constructions are proposed in [14]. In one of them an isotopic shift is applied to Gold-like functions which gives $F_L(x) = x^{2^i}L(x) + xL(x)^{2^i}$ but two different linear maps L_1 and L_2 are used instead of one L, that is, $x^{2^i}L_1(x) + xL_2(x)^{2^i}$. For the second generalisation, functions F_L with L not necessarily linear are considered.

The so-called binomial construction of APN functions which led to several infinite families of APN functions (F10, F12, F14 and F15) was first introduced in [29] and further developed in [30, 41, 51, 54] . It is considered in details in the following sections.

Note that in addition to the APN families in Table 2, there have been several other families of quadratic APN functions constructed. However, due to the work [18] they were identified as equivalent to previously known ones. There have been also several other interesting construction methods for APN functions but currently they are known to work only in small dimensions [2, 52, 53].

4. Equivalence between the APN hexanomials and Carlet's bivariate APN construction

In [29], the third author of the present paper introduced a method for constructing APN functions in bivariate form, that is, he considered functions F defined over $\mathbb{F}_{2^{2m}}$ given by $F(x,y) = (B(x,y), G(x,y))$, where $\mathbb{F}_{2^{2m}}$ is decomposed as $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$. Since all the known APN functions were in univariate form, the idea was that considering bivariate form could provide new functions up to equivalence. A second ingredient was to take for B a bent function from $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ to $\mathbb{F}_{2^m}$ (while G could be any function from $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ to $\mathbb{F}_{2^m}$). Indeed, such function F is APN if and only if the system

$$\begin{cases} B(x+a, y+b) + B(x,y) = c \\ G(x+a, y+b) + G(x,y) = d \end{cases}$$

has 2 or 0 solutions for any $(a,b) \neq (0,0)$ and $c, d \in \mathbb{F}_{2^n}$, and taking B bent made that the first equation in this system has the same number of solutions for every nonzero (a,b) and every (c,d). Moreover, considering the simplest Maiorana-McFarland function $B(x,y) = xy$, where the product is in the field $\mathbb{F}_{2^m}$, then from [29] we have the following conditions for F to be APN:

- the function $x \mapsto G(x,y)$ is APN for any fixed y;
- the function $y \mapsto G(x,y)$ is APN for any fixed x;
- the function $G(x, bx+c)$ is APN for any b and c.

If G is also quadratic then we can assume $c = 0$. From this, the following class of APN functions was deduced in [29].

Theorem 4.1. *Let $n = 2m$; let i, j be such that $\gcd(i-j, m) = 1$ and let $s, t \neq 0$, u and v in $\mathbb{F}_{2^m}$. Set $G(x,y) = sx^{2^i+2^j} + ux^{2^i}y^{2^j} + vx^{2^j}y^{2^i} + ty^{2^i+2^j}$. Then $F(x,y) = (xy, G(x,y))$ is APN if and only if the polynomial $G(X,1) = sX^{2^i+2^j} + uX^{2^i} + vX^{2^j} + t$ has no zero in $\mathbb{F}_{2^m}$.*

This construction can be simplified as shown by Taniguchi.

Proposition 4.2 ([51]). *Let $n = 2m$. The function $F(x,y) = (xy, G(x,y))$, with $G(x,y) = sx^{2^i+2^j} + ux^{2^i}y^{2^j} + vx^{2^j}y^{2^i} + ty^{2^i+2^j}$, is equivalent to $F'(x,y) = (xy, G'(x,y))$ with $G'(x,y) = x^{2^k+1} + axy^{2^k} + by^{2^k+1}$ with $k = i-j$, $a \in \{0,1\}$ and b in $\mathbb{F}_{2^m}^\star$.*

In [29], the third author of the present paper showed that the hexanomials introduced in [19] can be seen as a case of the APN functions in Theorem 4.1. The same was proved for trinomials introduced in the same paper [19] and for multinomials introduced in [7], but in [17], it has been shown that these two classes are contained in the class of the hexanomials. In fact, we will show in the following that the construction of Theorem 4.1 coincides with the hexanomials' class.

From the results in [17] we have that the family of APN hexanomial introduced in [19] (see Theorem 3.1) can be represented as a pentanomial:

Theorem 4.3. *Let n and i be any positive integers, $n = 2m$, $\gcd(i, m) = 1$, and $c, d \in \mathbb{F}_{2^n}$ be such that $d \notin \mathbb{F}_{2^m}$. Then, the pentanomial*

$$P(x) = dx^{2^m+1} + x^{2^i+1} + x^{2^m(2^i+1)} + cx^{2^{m+i}+1} + c^{2^m}x^{2^i+2^m},$$

is APN if and only if the equation

$$x^{2^i+1} + cx^{2^i} + c^{2^m}x + 1 = 0$$

has no solution x such that $x^{2^m+1} = 1$. Moreover, the class of APN hexanomials of Theorem 3.1 and the class of these APN pentanomials coincide.

Hence, when proving the equivalence between the APN functions as in Theorem 4.1 and the functions in the class of APN hexanomials, we will rather consider the pentanomials given in Theorem 4.3.

Theorem 4.4. *Let $n = 2m$. Let $F(x, y) = (xy, G(x, y))$ with $G(x, y) = x^{2^i+1} + axy^{2^i} + by^{2^i+1}$ with $gcd(i, m) = 1$, $a \in \{0, 1\}$ and b in $\mathbb{F}^{\star}_{2^m}$ be APN. Then F is EA-equivalent to an APN function in the hexanomial class as in Theorem 3.1.*

Proof. Let us consider first the case m odd. Since F is APN, the polynomial $X^{2^i+1} + aX + b$ has no zero in $\mathbb{F}_{2^m}$. In this case $a = 1$ otherwise we have no possible choice for b.

Fixing an element $\beta \notin \mathbb{F}_{2^m}$, any element of $\mathbb{F}_{2^n}$ can be represented as $z = x + \beta y$, where $x, y \in \mathbb{F}_{2^m}$, and then we can write $x = \frac{\beta^{2^m}z+z^{2^m}\beta}{\beta^{2^m}+\beta}$ and $y = \frac{z+z^{2^m}}{\beta^{2^m}+\beta}$. We then substitute $z' = z/(\beta^{2^m}+\beta)$ and we obtain $x = \beta^{2^m}z' + z'^{2^m}\beta$ and $y = z' + z'^{2^m}$. So, substituting x and y (and abusing notation), the function F is EA-equivalent to the function in univariate form

$$\begin{aligned}F'(x) =&\beta(\beta^{2^m}x + x^{2^m}\beta)(x + x^{2^m}) + (\beta^{2^m}x + x^{2^m}\beta)^{2^i+1}+\\&(\beta^{2^m}x + x^{2^m}\beta)(x + x^{2^m})^{2^i} + b(x + x^{2^m})^{2^i+1}.\end{aligned}$$

Now, F' is EA-equivalent to

$$\begin{aligned}F''(x) =&(\beta^{2^m+1} + \beta^2)x^{2^m+1} + (\beta^{2^i+1} + \beta + b)^{2^m}x^{2^i+1} + (\beta^{2^i+1}+\\&\beta + b)x^{2^m(2^i+1)} + (\beta^{2^{m+i}+1} + \beta + b)x^{2^m+2^i}+\\&(\beta^{2^{m+i}+1} + \beta + b)^{2^m}x^{2^{m+i}+1}.\end{aligned}$$

Now, if i is even then $\gcd(i,n)=\gcd(2i,n)=2$ and

$$\gcd(2^i+1,2^n-1)=\frac{\gcd(2^{2i}-1,2^n-1)}{\gcd(2^i-1,2^n-1)}=\frac{2^{\gcd(2i,n)}-1}{2^{\gcd(i,n)}-1}=1,$$

thus x^{2^i+1} is a permutation over $\mathbb{F}_{2^n}$, implying that there exists $\lambda\in\mathbb{F}_{2^n}$ such that $\lambda^{2^i+1}=(\beta^{2^i+1}+\beta+b)^{2^m}$. Note that we can always choose β such that $\beta^{2^i+1}+\beta+b\neq 0$ and thus $\lambda\neq 0$ (see for instance [6]). So, evaluating $F''(1/\lambda x)$ we obtain the function

$$\tilde{F}(x)=dx^{2^m+1}+x^{2^i+1}+x^{2^m(2^i+1)}+cx^{2^m+2^i}+c^{2^m}x^{2^{m+i}+1},$$

for some d and c such that $d\notin\mathbb{F}_{2^m}$. Now, since the function $\tilde{F}$ is APN, from Theorem 4.3, we have that

$$x^{2^i+1}+cx^{2^i}+c^{2^m}x+1=0$$

has no solution x such that $x^{2^m+1}=1$ and this function is EA-equivalent to an APN hexanomial as in Theorem 3.1.

Similarly, if i is odd we have that $\gcd(i+m,n)=\gcd(2(i+m),n)=2$ and the mapping $x^{2^{m+i}+1}$ permutes $\mathbb{F}_{2^n}$, implying that there exists $\lambda\in\mathbb{F}_{2^n}$ such that $\lambda^{2^{m+i}+1}=(\beta^{2^{m+i}+1}+\beta+b)^{2^m}$. As above, we can assume $\beta^{2^{i+m}+1}+\beta+b\neq 0$. Evaluating $F''(1/\lambda x)$ and letting $j=m+i$ we obtain the APN function

$$\tilde{F}(x)=dx^{2^m+1}+x^{2^j+1}+x^{2^m(2^j+1)}+cx^{2^m+2^j}+c^{2^m}x^{2^{m+j}+1},$$

and, as above, we conclude that this is EA-equivalent to an APN function in the hexanomial class.

Now, consider the case m even. As before, we obtain the univariate polynomial equivalent to F

$$\begin{aligned}F''(x)=&(\beta^{2^m+1}+\beta^2)x^{2^m+1}+(\beta^{2^i+1}+a\beta+b)^{2^m}x^{2^i+1}+\\&(\beta^{2^i+1}+a\beta+b)x^{2^m(2^i+1)}+(\beta^{2^{m+i}+1}+a\beta+b)x^{2^m+2^i}+\\&(\beta^{2^{m+i}+1}+a\beta+b)^{2^m}x^{2^{m+i}+1}.\end{aligned}$$

Since m is even we have that $\gcd(3,2^m+1)=1$ and then we can divide the set $\mathbb{F}_{2^n}^\star$ as

$$\mathbb{F}_{2^n}^*=U\cup\rho U\cup\rho^2U$$

with

$$U:=\{x^{2^i+1}\,:\,x\in\mathbb{F}_{2^n}^\star\}=\{x^3\,:\,x\in\mathbb{F}_{2^n}^\star\}.$$

and $\rho=\beta^{2^m+1}\in\mathbb{F}_{2^m}$.

Now, as before we can assume $\beta^{2^i+1}+a\beta+b\neq 0$ and thus we can have three cases

- $(\beta^{2^i+1}+a\beta+b)^{2^m}\in U$,

- $(\beta^{2^i+1}+a\beta+b)^{2^m}\in\rho U$,
- $(\beta^{2^i+1}+a\beta+b)^{2^m}\in\rho^2 U$.

If we have the first case, the proof is completed. Indeed, there exists an element λ such that $\lambda^{2^i+1}=(\beta^{2^i+1}+a\beta+b)^{2^m}$ and substituting $x\mapsto\lambda^{-1}x$ we will obtain a pentanomial as in Theorem 4.3.

Otherwise, suppose that $(\beta^{2^i+1}+a\beta+b)^{2^m}\in\rho U$ (or $(\beta^{2^i+1}+a\beta+b)^{2^m}\in\rho^2 U$) and multiply $F'(x)$ by $\rho^2\in\mathbb{F}_{2^m}$ (or multiply by $\rho\in\mathbb{F}_{2^m}$) obtaining

$$F''(x)=d'x^{2^m+1}+a'x^{2^i+1}+a'^{2^m}x^{2^m(2^i+1)}+b'x^{2^{m+i}+1}+b'^{2^m}x^{2^i+2^m},$$

with $d'\notin\mathbb{F}_{2^m}$ and $a'\in U$. Let us consider an element λ such that $\lambda^{2^i+1}=a'$, then substituting $x\mapsto\lambda^{-1}x$ we will obtain an APN pentanomial of Theorem 4.3 which is EA-equivalent to a function in the hexanomial family. □

Another interesting fact that can be proved for this construction is that when the coefficient a is zero (thus m is even), for a fixed i coprime with m, we have that for any possible b we obtain the same function (up to equivalence). This has been also recently proved in [45] for the more general case of the Zhou-Pott family which includes this special case. Recall their result that any function $F(x,y)=(xy,x^{2^i+1}+by^{2^i+1})$ is APN if and only if b lies outside the set $\{x^{2^i+1} : x\in\mathbb{F}_{2^n}^\star\}$, that is, is not a cube (see Theorem 5.1 in the next section).

Proposition 4.5. *Let $n=2m$ with m even, and i such that* $\gcd(i,m)=1$. *Let b and b' not in the set $U:=\{x^{2^i+1} : x\in\mathbb{F}_{2^n}^\star\}=\{x^3 : x\in\mathbb{F}_{2^n}^\star\}$. Then $F(x,y)=(xy,x^{2^i+1}+by^{2^i+1})$ and $F'(x,y)=(xy,x^{2^i+1}+b'y^{2^i+1})$ are EA-equivalent.*

Proof. We can partition the non cubic elements of $\mathbb{F}_{2^n}$ as $bU\cup b^2U$. So first of all, note that if we substitute y by uy for any $u\neq 0$, then $F(x,y)$ is equivalent to the function $F''(x,y)=(xy,x^{2^i+1}+bu^{2^i+1}y^{2^i+1})$ so if $b'\in bU$ we have the equivalence.

Now, if we consider again F and we divide by b the part $x^{2^i+1}+by^{2^i+1}$, we obtain the equivalent function $F''(x,y)=(xy,\frac{1}{b}x^{2^i+1}+y^{2^i+1})$. Now, we can apply the linear transformation $L(x,y)=(by,x)$, so

$$F''(L(x,y))=(bxy,x^{2^i+1}+b^{2^i}y^{2^i+1})\sim_{EA}(xy,x^{2^i+1}+b^{2^i}y^{2^i+1}).$$

Since i is odd we have that $b^{2^i}\in b^2U$. So, with similar argument as above if $b'\in b^2U$ we obtain that F is EA-equivalent to F'. □

5. On bivariate constructions of APN quadratic functions

Following the construction of Theorem 4.1, other two families of functions have been constructed by Zhou and Pott [54] and Taniguchi [51] and are presented here in Theorems 5.1 and 5.3, respectively.

Theorem 5.1 ([54]). *Let $n = 2m$, m even, and let i be such that* $\gcd(i, m) = 1$. *Set $G(x, y) = x^{2^i+1} + \alpha y^{2^j(2^i+1)}$. Then $F(x, y) = (xy, G(x, y))$ is APN if and only if $\alpha \in \{u^{2^i+1}(t^{2^i} + t)^{1-2^j} \ : \ u, t \in \mathbb{F}_{2^m}\}$. In particular if j is even, then F is APN if and only if α is not a cube.*

Remark 5.2. If j is not even, then $S = \{u^{2^i+1}(t^{2^i} + t)^{1-2^j} \ : \ u, t \in \mathbb{F}_{2^m}\} = \mathbb{F}_{2^m}$ and the family of Zhou-Pott is not defined then. Indeed, since m is even, we can partition $\mathbb{F}^\star_{2^m}$ as $U \cup dU \cup d^2U$, where U is the set of all cubes (different from zero) and $d \notin U$. Since $t^{2^i} + t$ are the elements with null trace we have that $t^{2^i} + t = 1$ for some t, and thus $U \subset S$. We need to show that there exist $(t^{2^i} + t)^{1-2^j} \in dU$ and $(t'^{2^i} + t')^{1-2^j} \in d^2U$ for completing the proof.
Suppose that does not exist $(t^{2^i} + t)^{1-2^j} \in dU$, that implies also there does not exist $(t'^{2^i} + t')^{1-2^j} \in d^2U$. Indeed, if $y \in d^2U$ then $y^2 \in dU$ and, supposing $(t'^{2^i} + t')^{1-2^j} \in d^2U$ we would have $(t'^{2^{i+1}} + t'^2)^{1-2^j} \in dU$, and $Tr(t'^{2^{i+1}} + t'^2) = Tr(t'^{2^i} + t') = 0$.
Thus, if for any x of null trace we have that $x^{1-2^j} \notin dU$, then we obtain $x^{1-2^j} \in U$ for all x of null trace. Since j is odd we have $3 \nmid 2^j - 1$ and so $x \in U$. This implies that $U \cup \{0\}$ contains a vector space of dimension $m - 1$ which is not possible ($|U| = (2^m - 1)/3$).
So, the family of Zhou-Pott can be defined only for j even (this was also noted in [1]).

The family introduced by Taniguchi in [51] is given by the following.

Theorem 5.3 ([51]). *Let $n = 2m$, and let i be such that* $\gcd(i, m) = 1$. *Set $G(x, y) = x^{2^{2i}+2^{3i}} + ax^{2^{2i}}y^{2^i} + by^{2^i+1}$ with $a \in \{0, 1\}$. Then $F(x, y) = (xy, G(x, y))$ is APN if and only if $X^{2^i+1} + aX + b$ has not zero in $\mathbb{F}_{2^m}$.*

Both Zhou-Pott and Taniguchi families are particular cases of a more general construction defined by the third author of the present paper in [30].

Theorem 5.4. *Let $n = 2m$, and let i be such that* $\gcd(i, m) = 1$. *Set $G(x, y) = P(x^{2^i+1}) + Q(x^{2^i}y) + R(xy^{2^i}) + S(y^{2^i+1})$, with P, Q, R and S linear functions. Then, $F(x, y) = (xy, G(x, y))$ is APN if and only if for all $(c, d) \neq (0, 0)$, $T_{c,d}(Y) = P(c^{2^i+1}Y) + Q(c^{2^i}dY) + R(cd^{2^i}Y) + S(d^{2^i+1}Y)$ satisfies:*

- *if m is odd then $T_{c,d}$ is bijective;*
- *if m is even, then $\ker(T_{c,d}) \cap \{u^{2^i+1}(t^{2^i} + t) \ : \ u, t \in \mathbb{F}_{2^m}\} = \{0\}$.*

Remark 5.5. The condition on the function $T_{c,d}$ is deduced from the fact that $G(cx, dx+e)$ equals $T_{c,d}(x^{2^i+1})$ and from Lemma 4.1 in [30]. However, also for m even we need $T_{c,d}$ to be a permutation. Indeed, for any $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ APN and L linear, $L \circ F$ is APN if and only if L is a permutation. If L is not a permutation then without loss of generality L is a linear functions from $\mathbb{F}_2^n \to \mathbb{F}_2^m$ with $m < n$. Thus, if $G = L \circ F$ is APN then $G'(x) = (G(x), 0, ..., 0) : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is also APN. Now, $G'(x+a) + G'(x) = (G(x+a) + G(x), 0, ..., 0)$ and since G is APN then also G' is APN. But this cannot be possible since an APN map has nonlinearity always different from 0 (see [31]).
The same fact can be deduced by Remark 5.2 since we proved that $\{u^{2^i+1}(t^{2^i} + t) : u, t \in \mathbb{F}_{2^m}\} = \mathbb{F}_{2^m}$.

We can observe immediately that P and S are permutations (case c or d equal to 0). Moreover, we can restrict the exponent $i < m/2$. Indeed, if $i > m/2$, then substituting $(x, y) \mapsto (x^{2^{m-i}}, y^{2^{m-i}})$ and composing with the linear function $L(x, y) = (x^{2^i}, y)$, we will obtain an equivalent function, that is

$$L \circ F(x^{2^{m-i}}, y^{2^{m-i}}) = (xy, P(x^{2^j+1}) + Q(xy^{2^j}) + R(x^{2^j}y) + S(y^{2^j+1})),$$

where $j = m - i < m/2$.

In the following we will consider the particular case where P, Q, R and S are monomial linear functions, i.e.

$$G(x, y) = a(x^{2^i+1})^{2^k} + b(x^{2^i}y)^{2^h} + c(xy^{2^i})^{2^r} + d(y^{2^i+1})^{2^s}.$$

Note that we can suppose $k = 0$ since, otherwise, we can raise G to the power of 2^{m-k}. Moreover $a, d \neq 0$ since we need P and S permutations. That is, we can consider the function

$$G(x, y) = x^{2^i+1} + a(x^{2^i}y)^{2^h} + b(xy^{2^i})^{2^k} + c(y^{2^i+1})^{2^r}.$$

We can also restrict $a \in \{0, 1\}$ since we can apply the substitution $y \mapsto (1/a)^{2^{-h}}y$. In the case $a = 0$, we can restrict in the same way $b \in \{0, 1\}$. Thus we have the following result.

Theorem 5.6. *Let*

$$F(x, y) = (xy, a(x^{2^i+1})^{2^k} + b(x^{2^i}y)^{2^h} + c(xy^{2^i})^{2^r} + d(y^{2^i+1})^{2^s})$$

be an APN function over $\mathbb{F}_{2^{2m}}$. Then, F is EA-equivalent to one of the following functions

$$F_1(x, y) = (xy, x^{2^i+1} + x^{2^{i+h}}y^{2^h} + b'x^{2^k}y^{2^{i+k}} + c'y^{2^{i+r}+2^r}),$$
$$F_2(x, y) = (xy, x^{2^i+1} + x^{2^k}y^{2^{i+k}} + c'y^{2^{i+r}+2^r}),$$
$$F_3(x, y) = (xy, x^{2^i+1} + c'y^{2^{i+r}+2^r}),$$

with $c' \neq 0$.

COROLLARY 5.7. *The class of functions* F_3 *in Theorem 5.6 is the Zhou-Pott class (and the Taniguchi class for the case* $a = 0$*). The class of functions* F_2 *in Theorem 5.6 contains the Taniguchi APN functions for the case* $a = 1$.

PROOF. From the result of Zhou and Pott it follows that $F_3(x,y) = (xy, x^{2^i+1} + c'y^{2^{i+r}+2^r})$ is APN over $\mathbb{F}_{2^{2m}}$ if and only if m is even, c' is not a cube and r is even. So, F_3 is exactly the Zhou-Pott case, which contains the Taniguchi APN functions (i.e. $F(x,y) = (xy, x^{2^{2i}+2^{3i}} + ax^{2^{2i}}y^{2^i} + by^{2^i+1}))$ for $a = 0$.

Now, consider the function $F(x,y) = (xy, x^{2^{2i}+2^{3i}} + x^{2^{2i}}y^{2^i} + by^{2^i+1})$, which is the Taniguchi function with $a = 1$. Let $L(x,y) = (y,x)$. Then,

$$\begin{aligned} F \circ L(x,y) &= (xy, bx^{2^i+1} + x^{2^i}y^{2^{2i}} + y^{2^{2i}+2^{3i}}) \\ &\sim_{EA} (xy, x^{2^i+1} + b^{-1}x^{2^i}y^{2^{2i}} + b^{-1}y^{2^{2i}+2^{3i}}). \end{aligned}$$

Applying the substitution $y \mapsto b^{2^{-2i}}y$, and then dividing the left part by $b^{2^{-2i}}$, the last function is equivalent to $(xy, x^{2^i+1} + x^{2^i}y^{2^{2i}} + b^{2^i}y^{2^{2i}+2^{3i}})$, which is of type F_2. ◻

PROPOSITION 5.8. *Let* $n = 2m$, *and* i *be such that* $\gcd(i,m) = 1$. *If*

$$F_1(x,y) = (xy, x^{2^i+1} + x^{2^{i+h}}y^{2^h} + bx^{2^k}y^{2^{i+k}} + cy^{2^{i+r}+2^r})$$

with $b = 0$ *and* $h = m-i$, $r = m-2i$ *is APN over* $\mathbb{F}_{2^n}$, *then it is EA-equivalent to the Taniguchi case.*

PROOF. We have

$$F_1(x,y) = (xy, x^{2^i+1} + (x^{2^i}y)^{2^{-i}} + c(y^{2^i+1})^{2^{-2i}}).$$

Thus, using the linear permutations $L_1 : (x,y) \mapsto (x^{2^{-i}}, y^{2^{-i}})$ and $L_2 : (x,y) \mapsto (x^{2^i}, y)$ we obtain

$$L_2 \circ F_1 \circ L_1(x,y) = (xy, x^{2^{-i}+1} + (xy^{2^{-i}})^{2^{-i}} + c(y^{2^{-i}+1})^{2^{-2i}}).$$

As noted above this is a Taniguchi APN function. ◻

6. OTHER INSTANCES OF APN FUNCTIONS FROM CARLET'S CONSTRUCTION

We give a necessary condition for a function F_1 with $h = m/2$, $k, r = 0$ to be APN.

LEMMA 6.1. *Let* $n = 2m$ *with* $m > 2$ *even. Let* i *coprime with* m. *If*

$$F(x,y) = (xy, x^{2^i+1} + x^{2^{i+m/2}}y^{2^{m/2}} + bxy^{2^i} + cy^{2^i+1})$$

is APN, then $cX^{2^i+1} + bX^{2^i} + X^{2^{m/2}} + 1$ *has no zero in* $\mathbb{F}_{2^m}$.

Proof. $F(x,y) = (xy, G(x,y))$ with $G(x,y) = x^{2^i+1} + x^{2^{i+m/2}}y^{2^{m/2}} + bxy^{2^i} + cy^{2^i+1}$. Since F_1 is APN we have that G satisfies the following conditions

- the function $x \mapsto G(x,y)$ is APN for any fixed y;
- the function $y \mapsto G(x,y)$ is APN for any fixed x;
- the function $G(x, \beta x + \gamma)$ is APN for any β and γ.

From the third condition we have (we can consider $\gamma = 0$ since G is quadratic)

$$G(x, \beta x) = (c\beta^{2^i+1} + b\beta^{2^i} + 1)x^{2^i+1} + \beta^{2^{m/2}}x^{2^{m/2}(2^i+1)}.$$

If we consider $x \in \mathbb{F}_{2^{m/2}}$ we obtain the function $F'(x) = (c\beta^{2^i+1} + b\beta^{2^i} + 1 + \beta^{2^{m/2}})x^{2^i+1}$. From this we have immediately that if there exists β such that $c\beta^{2^i+1} + b\beta^{2^i} + 1 + \beta^{2^{m/2}} = 0$ then for any $a \in \mathbb{F}^\star_{2^{m/2}}$ and for any $x \in \mathbb{F}_{2^{m/2}}$

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

which would imply that $G(x, \beta x)$ is not APN. □

The previous result can be used for filtering the search of the coefficients b and c.

For the new functions we have the following necessary and sufficient condition for the APNness.

Theorem 6.2. *Let $n = 2m$ with m even, and let $i < m/2$ be such that* $\gcd(i,m) = 1$. *Then,*

$$F(x,y) = (xy, x^{2^i+1} + x^{2^{i+m/2}}y^{2^{m/2}} + bxy^{2^i} + cy^{2^i+1})$$

is APN if and only if $(cX^{2^i+1} + bX^{2^i} + 1)^{2^{m/2}+1} + X^{2^{m/2}+1}$ has no zero in $\mathbb{F}_{2^m}$.

Proof. As in the previous proof we have that F is APN if and only if the function $G(x, \beta x) = (c\beta^{2^i+1} + b\beta^{2^i} + 1)x^{2^i+1}\beta^{2^{m/2}}x^{2^{m/2}(2^i+1)}$ is APN for any β.

Note that $G(x, \beta x) = L_\beta(x^{2^i+1})$ where

$$L_\beta(x) = (c\beta^{2^i+1} + b\beta^{2^i} + 1)x + \beta^{2^{m/2}}x^{2^{m/2}}.$$

As noted in Remark 5.5, we have that $L_\beta(x^{2^i+1})$ is APN if and only if L_β is a permutation of $\mathbb{F}_{2^m}$. Denoting by $A = c\beta^{2^i+1} + b\beta^{2^i} + 1$ and $B = \beta^{2^{m/2}}$, this is equivalent to have

$$\begin{bmatrix} A & B^{2^{m/2}} \\ B & A^{2^{m/2}} \end{bmatrix}$$

with determinant different from 0. Thus, L_β is a bijection for any β if and only if $(cX^{2^i+1} + bX^{2^i} + 1)^{2^{m/2}+1} + X^{2^{m/2}+1}$ has no zero in $\mathbb{F}_{2^m}$. □

From the computational results we have that for $n = 8$ the functions as in Theorem 6.2 can produce a new APN function which is CCZ-inequivalent to the function given in the tables in [53] and in [52], and in particular which is not included in any of the known families.

REMARK 6.3. It is easy to note that if we apply the linear transformation $L(x, y) = (y, x)$ to a function as in Theorem 6.2 we obtain

$$F(x, y) = (xy, cx^{2^i+1} + bx^{2^i}y + x^{2^{m/2}}y^{2^{i+m/2}} + y^{2^i+1}).$$

In the case $b \neq 0$, this is equivalent to a function of the first type

$$F_1'(x, y) = (xy, x^{2^i+1} + x^{2^i}y + b'x^{2^{m/2}}y^{2^{i+m/2}} + c'y^{2^i+1}).$$

If $b = 0$ we have that F is equivalent to a function of type

$$F_2'(x, y) = (xy, x^{2^i+1} + x^{2^{m/2}}y^{2^{i+m/2}} + c'y^{2^i+1}).$$

6.1. *Computational results.* We checked the APN functions in small dimensions, obtained from the cases given in Theorem 5.6, that is,

$$\begin{aligned} F_1(x, y) &= (xy, x^{2^i+1} + x^{2^{i+h}}y^{2^h} + bx^{2^k}y^{2^{i+k}} + cy^{2^{i+r}+2^r}), \\ F_2(x, y) &= (xy, x^{2^i+1} + x^{2^k}y^{2^{i+k}} + cy^{2^{i+r}+2^r}), \\ F_3(x, y) &= (xy, x^{2^i+1} + cy^{2^{i+r}+2^r}). \end{aligned}$$

In the computational results we do not consider the case of F_3 which is represented only by the Zhou-Pott family. As noted in the previous section we can consider $i < m/2$ coprime with m. Moreover, when $h, k, r = 0$ then the APN function is equivalent to an APN function of the hexanomial class.

6.1.1. $\mathbf{n = 2 \cdot 4}$. For this dimension we can consider only $i = 1$.

CASE F_1:

$b \neq 0$

-For $h = 0, k = 2, r = 0$ and $h = 2, k = 0, r = 0$, we have that these two cases are equivalent to each other (we can use the linear permutation $(x, y) \mapsto (y, x)$) and the last case ($h = 2, k = 0, r = 0$) produces a new APN function of the form as in Theorem 6.2.

$b = 0$

- For $h = 3, r = 2$ we have the Taniguchi APN functions (see Proposition 5.8).

CASE F_2:

$c \neq 0$

-When $k = 1, r = 2$, we have the Taniguchi APN functions.

6.1.2. $\mathbf{n = 2 \cdot 5}$. For this dimension we can consider only $i = 1, 2$.

CASE F_1:

$b \neq 0$

- In this case we obtain only the hexanomial APN functions.

$b = 0$

-With $i = 1$ and $h = 4, r = 3$, we have the Taniguchi APN functions
-With $i = 2$ and $h = 3, r = 1$, we have the Taniguchi APNfunctions

CASE F_2:

$c \neq 0$

-With $i = 1$ and $k = 1, r = 2$ we have the Taniguchi APN functions.
-With $i = 2$ and $k = 2, r = 4$ we obtain the Taniguchi APN functions.

6.1.3. $\mathbf{n = 2 \cdot 6}$. For this dimension we can consider only $i = 1$.

CASE F_1:

$b \neq 0$

- In this case we obtain only the hexanomial APN functions.

$b = 0$

- For $h = 2, r = 4$ we have APN functions which could be inequivalent to the known cases.
- For $h = 3, r = 0$ we obtain functions as in Theorem 6.2.
- For $h = 5, r = 4$ we have Taniguchi APN functions.

CASE F_2:

$c \neq 0$

- $k = 1, r = 2$ Taniguchi
- $k = 3, r = 0$ this is equivalent to a function as in Theorem 6.2.- $k = 4, r = 2$, this case is equivalent to the second case for $b = 0$.

6.1.4. $\mathbf{n = 2 \cdot 8}$. For this dimension we can consider only $i = 1, 3$.

CASE F_1:

$b \neq 0$

- In this case we obtain only the hexanomial APN functions.

$b = 0$

- $i = 1$: $h = 7, r = 6$ we have Taniguchi APN functions.

CASE F_2:

$c \neq 0$

- $i = 1$: $k = 1, r = 2$ we have Taniguchi APN functions.
- $i = 3$: $k = 3, r = 6$ we have Taniguchi APN functions.

7. On the bivariate construction using projective polynomials

In [29], the third author of the present paper investigates over $\mathbb{F}_{2^6}$ the bivariate construction considering bent functions of the form $B(x,y) = sx^3 + ty^3 + ux^2y + vxy^2$. In particular, the APN function $F(x) = (B(x,y), G(x,y))$ was found (in collaboration with Gregor Leander) where

$$B(x,y) = x^3 + y^3 + x^2y + \alpha^9 xy^2,$$

$$G(x,y) = \alpha^{54}x^5 + \alpha^{54}xy^4 + \alpha^{45}y^5,$$

where α is a primitive element of $\mathbb{F}_{2^3}$.

Switching the function F by the function

$$\begin{aligned} f(x,y) =& \alpha^9x^7 + \alpha^{18}x^6y^4 + \alpha^{18}x^6y^2 + \alpha^{45}x^6y + \alpha^{27}x^5y^4 + \\ & \alpha^{18}x^5y^2 + \alpha^{27}x^5y + \alpha^{54}x^4y^6 + \alpha^{45}x^4y^5 + \alpha^{27}x^4y^3 + \\ & \alpha^{27}x^3y^4 + \alpha^{45}x^3y^2 + \alpha^{45}x^3y + \alpha^{27}x^2y^6 + \alpha^{18}x^2y^5 + \\ & x^2y^3 + \alpha^{45}xy^6 + \alpha^{36}xy^5 + \alpha^{18}xy^3 + \alpha^{27}x^6 + \alpha^{45}x^4y^2 + \\ & \alpha^{54}x^4y + x^3 + \alpha^9x^2y^4 + \alpha^{54}xy + \alpha^{54}y^6 + \alpha^{36}y^3, \end{aligned}$$

that is, considering $F'(x,y) = (B(x,y), G(x,y) + f(x,y))$, they obtained a non-quadratic APN function, which is CCZ-equivalent to the function found by Edel and Pott [39]. Note that $f(x,y) = \alpha^9 f'(x,y)$, with f' a Boolean function.

A classification of the cubic APN functions in dimension 6 with respect to EA-equivalence is given in [26]. In particular, for the case of the non-quadratic APN function its CCZ-equivalence class can be divided into 25 EA-equivalence classes, 10 containing functions of algebraic degree 3, and 15 containing functions of algebraic degree 4. Moreover, for this function CCZ-equivalnece is more general than EA-equivalence together with the inverse transformation [18].

Note that the functions B and G are both of the form

$$g(x,y) = ax^{q+1} + bx^qy + cxy^q + dy^{q+1},$$

with q a power of 2. Polynomials of type $X^{q+1} + aX^q + bX + c$ are called also *projective polynomials.* We will call a polynomial of type $ax^{q+1} + bx^qy + cxy^q + dy^{q+1}$ a *bivariate projective* (or bi-projective) polynomial.

So, a possible construction for APN functions is given by using a bivariate construction with two bi-projective polynomials, that is

$$F(x,y) = (Ax^{2^i+1} + Bx^{2^i}y + Cxy^{2^i} + Dy^{2^i+1}, ax^{2^j+1} + bx^{2^j}y + cxy^{2^j} + dy^{2^j+1}).$$

Without loss of generality, we can suppose that $A, a \neq 0$. Indeed, we can always consider a linear permutation $L(x,y) = (\alpha_1x + \alpha_2y, \beta_1x + \beta_2y)$, and so we will get that the coefficients of x^{2^i+1} and of x^{2^j+1} in $F \circ L$ would be

$$A\alpha_1^{2^i+1} + B\alpha_1^{2^i}\beta_1 + C\alpha_1\beta_1^{2^i} + D\beta_1^{2^i+1}, \quad a\alpha_1^{2^j+1} + b\alpha_1^{2^j}\beta_1 + c\alpha_1\beta_1^{2^j} + d\beta_1^{2^j+1}.$$

We can always choose α_1 and β_1 so that both the coefficients are not zero, otherwise we would have that $B(x,y)$ or $G(x,y)$ are constantly equal to zero (this would implies that F is not APN). Then, we can always choose α_2 and β_2 so that L is a permutation.

So we can restrict to

$$B(x,y) = x^{2^i+1} + Ax^{2^i}y + Bxy^{2^i} + Cy^{2^i+1}$$

and

$$G(x,y) = x^{2^j+1} + ax^{2^j}y + bxy^{2^j} + cy^{2^j+1}.$$

Moreover, using similar steps as for the bivariate construction with $B(x,y) = xy$, considered in the previous section, we can obtain the following result.

Theorem 7.1. *Let $n = 2m$ and let*

$$F(x,y) = (Ax^{2^i+1}+Bx^{2^i}y+Cxy^{2^i}+Dy^{2^i+1}, ax^{2^j+1}+bx^{2^j}y+cxy^{2^j}+dy^{2^j+1})$$

be APN over $\mathbb{F}_{2^n}$. Then F is EA-equivalent to one of the following functions

$$f_1(x,y) = (x^{2^i+1}+x^{2^i}y+Axy^{2^i}+By^{2^i+1}, x^{2^j+1}+ax^{2^j}y+bxy^{2^j}+cy^{2^j+1}) \tag{7.2}$$

$$f_2(x,y) = (x^{2^i+1} + xy^{2^i} + Ay^{2^i+1}, x^{2^j+1} + ax^{2^j}y + bxy^{2^j} + cy^{2^j+1}) \tag{7.3}$$

$$f_3(x,y) = (x^{2^i+1} + Ay^{2^i+1}, x^{2^j+1} + x^{2^j}y + axy^{2^j} + by^{2^j+1}) \tag{7.4}$$

$$f_4(x,y) = (x^{2^i+1} + Ay^{2^i+1}, x^{2^j+1} + axy^{2^j} + by^{2^j+1}) \tag{7.5}$$

where in (7.5) *$a = 0, 1$. Moreover, we can suppose $i, j \leq m/2$.*

Recently, Göloğlu considered the construction of APN functions using bi-projective polynomials [41], obtaining the following families.

Theorem 7.2 ([41]). *The following functions are APN on $\mathbb{F}_{2^{2m}}$:*

- *If* $\gcd(3i, m) = 1$,

$$\mathcal{F}_1(x,y) = (x^{2^i+1} + xy^{2^i} + y^{2^i+1}, x^{2^{2i}+1} + x^{2^{2i}}y + y^{2^{2i}+1});$$

- *If* $\gcd(3i, m) = 1$, *m odd*

$$\mathcal{F}_2(x,y) = (x^{2^i+1} + xy^{2^i} + y^{2^i+1}, x^{2^{3i}}y + xy^{2^{3i}}).$$

Remark 7.3. We can see that $\mathcal{F}_1$ is of type (7.3), while $\mathcal{F}_2$ is EA-equivalent to a function as in (7.2). Indeed, using the substitution $L(x,y) = (\alpha x, x+y)$ with $\alpha \neq 0, 1$ such that $\alpha^{2^i+1} + \alpha + 1 \neq 0$ we obtain

$$\mathcal{F}_2 \circ L(x,y) =$$

$$((\alpha^{2^i+1}+\alpha+1)x^{2^i+1}+x^{2^i}y+(\alpha+1)xy^{2^i}+y^{2^i+1},(\alpha^{2^{3i}}+\alpha)x^{2^{3i}+1}+\alpha^{2^{3i}}x^{2^{3i}}y+\alpha xy^{2^{3i}}).$$

Dividing the left term by $\alpha^{2^i+1} + \alpha + 1$ and the right term by $\alpha^{2^{3i}} + \alpha$, we obtain a function as in (7.2).

Another function constructed using bi-projective polynomials has been constructed also by Nikolay Kaleyski and Kangquan Li [43]. In particular, they obtained the following result.

Theorem 7.4. *Let $(m,i) = (5+6l, 3+4l)$ or $(7+6l, 5+4l)$ with some integer l and*

$$F(x,y) = (x^{2^i+1} + x^{2^i}y + y^{2^i+1}, x^2y + xy^2).$$

Then F is an APN function over $\mathbb{F}_{2^{2m}}$.

However, these functions are included in the construction $\mathcal{F}_2$ of Göloğlu as we prove below.

Proposition 7.5. *The function defined in Theorem 7.4 is equivalent to the function $\mathcal{F}_2$ in Theorem 7.2.*

Proof. We will show the case $(m,i) = (5+6l, 3+4l)$, the case $(m,i) = (7+6l, 5+4l)$ follows in a similar way.

First of all, note that $m - i = 2 + 2l$. So, applying $L(x,y) = (x^{2^{m-i}}, y)$ to the function F, we obtain

$$L \circ F(x,y) = (x^{2^{m-i}+1} + xy^{2^{m-i}} + y^{2^{m-i}+1}, x^2y + xy^2).$$

Now, it is easy to note that

$$2^{3(m-i)} = 2^{6+6l} \equiv 2 \mod 2^m - 1.$$

Then,

$$L \circ F(x,y) = (x^{2^{m-i}+1} + xy^{2^{m-i}} + y^{2^{m-i}+1}, x^{2^{3(m-i)}}y + xy^{2^{3(m-i)}}),$$

and this last function is exactly the function $\mathcal{F}_2$ in Theorem 7.2. □

References

[1] N. Anbar, T. Kalaycı, and W. Meidl. *Determining the Walsh spectra of Taniguchi's and related APN-functions.* Finite Fields and their Applications **60** (2019), 101577.

[2] C. Beierle, and G. Leander. *New Instances of Quadratic APN Functions.* ArXiv preprint (2020).

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

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

[5] E. Biham, and A. Shamir. *Differential cryptanalysis of DES-like cryptosystems.* Journal of Cryptology **4** (1991), 3–72.

[6] A. Bluher. *On* $x^{q+1} + ax + b$. Finite Fields and their Applications **10(3)** (2004), 285–305.

[7] C. Bracken, E. Byrne, N. Markin, and G. McGuire. *New Families of Quadratic Almost Perfect Nonlinear Trinomials and Multinomials.* Finite Fields and their Applications **14(3)** (2008), 703–714.

[8] C. Bracken, E. Byrne, N. Markin, and G. McGuire. *A Few More Quadratic APN Functions.* Cryptography and Communications **3** (2011), 43–53.

[9] M. Brinkmann, and G. Leander. *On the classification of APN functions up to dimension five.* Designs, Codes and Cryptography **49** (2008), 273–288.

[10] K. A. Browning, J. F. Dillon, R. E. Kibler, and M. T. McQuistan. *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, **34** (2009), 135–159.

[11] K. A. Browning, J. F. Dillon, M. T. McQuistan, and 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 **518** (2010), 33–42.

[12] L. Budaghyan. *Construction and Analysis of Cryptographic Functions.* Springer Verlag, 2015.

[13] L. Budaghyan, M. Calderini, C. Carlet, R. Coulter, and I. Villa. *Constructing APN functions through isotopic shift.* IEEE Trans. Inform. Theory **66(8)** (2020), 5299–5309.

[14] L. Budaghyan, M. Calderini, C. Carlet, R. Coulter, and I. Villa. *Generalized isotopic shift construction for APN functions.* Designs, Codes and Cryptography, **89** (2020), 19–32.

[15] L. Budaghyan, M. Calderini, C. Carlet, R. Coulter, and I. Villa. *On isotopic shift construction for planar functions*, 2019 IEEE International Symposium on Information Theory (ISIT), 2962–2966, (2019).

[16] L. Budaghyan, M. Calderini, C. Carlet, D. Davidova, and N. Kaleyski. *A note on the Walsh spectrum of Dobbertin APN functions*, Proceedings of SETA 2020.

[17] L. Budaghyan, M. Calderini, and I. Villa. *On equivalence between known families of quadratic APN functions.* Finite Fields and their Applications **66** (2020), 101704.

[18] L. Budaghyan, M. Calderini, and I. Villa. *On relations between CCZ- and EA- equivalences.* Cryptography and Communications **12** (2020), 85–100.

[19] L. Budaghyan, and C. Carlet. *Classes of Quadratic APN Trinomials and Hexanomials and Related Structures.* IEEE Trans. Inform. Theory **54(5)** (2008), 2354–2357.

[20] L. Budaghyan, C. Carlet, and G. Leander. *Two classes of quadratic APN binomials inequivalent to power functions.* IEEE Trans. Inform. Theory **54(9)** (2008), 4218–4229.

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

[22] L. Budaghyan, C. Carlet, and G. Leander. *On a construction of quadratic APN functions.* Proceedings of IEEE Information Theory workshop ITW'09, (2009), 374–378.

[23] L. Budaghyan, C. Carlet, and A. Pott. *New Classes of Almost Bent and Almost Perfect Nonlinear Functions.* IEEE Trans. Inform. Theory **52(3)** (2006), 1141–1152.

[24] L. Budaghyan, T. Helleseth. *New commutative semifields defined by new PN multinomials.* Cryptography and Communications **3(1)** (2011), 1–16.

[25] L. Budaghyan, T. Helleseth, and N. Kaleyski. *A new family of APN quadrinomials.* IEEE Trans. Inform. Theory **66(11)** (2020), 7081–7087,.

[26] M. Calderini. *On the EA-classes of known APN functions in small dimensions.* Cryptography and Communications **12** (2020), 821–840.

[27] M. Calderini, M. Sala, and I. Villa. *A note on APN permutations in even dimension.* Finite Fields and their Applications **46** (2017), 1–16.

[28] A. Canteaut, P. Charpin, and H. Dobbertin. *Weight divisibility of cyclic codes, highly nonlinear functions on $\mathbb{F}_{2^m}$, and crosscorrelation of maximum-length sequences.* SIAM Journal on Discrete Mathematics **13(1)** (2000), 105–138.

[29] C. Carlet. *Relating three nonlinearity parameters of vectorial functions and building APN functions from bent functions.* Designs, Codes and Cryptography **59** (2011), 89–109.

[30] C. Carlet. *More constructions of APN and differentially 4-uniform functions by concatenation.* Science China Mathematics **56(7)** (2013),1373–1384.

[31] C. Carlet. *Boolean Functions for Cryptography and Coding Theory.* Cambridge University Press, 2020.

[32] C. Carlet, P. Charpin, and V. Zinoviev. *Codes, bent functions and permutations suitable for DES-like cryptosystems.* Designs, Codes and Cryptography **15(2)** (1998), 125–156.

[33] F. Chabaud, and S. Vaudenay. *Links between Differential and Linear Cryptanalysis.* Proceedings of EUROCRYPT 1994, Lecture Notes in Computer Science **950** (1995), 356-365.

[34] U. Dempwolff. *CCZ equivalence of power functions.* Designs, Codes and Cryptography **86(3)** (2018), 665–692.

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

[36] H. Dobbertin. *Almost perfect nonlinear power functions over $GF(2^n)$: the Niho case.* Inform. and Comput. **151(1-2)** (1999), 57–72.

[37] H. Dobbertin. *Almost perfect nonlinear power functions over $GF(2^n)$: a new case for n divisible by 5.* Proceedings of Finite Fields and Applications FQ5, (2000), 113–121.

[38] Y. Edel, G. Kyureghyan, and A. Pott. *A new APN function which is not equivalent to a power function.* IEEE Trans. Inform. Theory **52(2)** (2006), 744–747.

[39] Y. Edel, and A. Pott. *A new almost perfect nonlinear function which is not quadratic.* Adv. in Math. of Comm. **3(1)** (2009), 59–81.

[40] R. Gold. *Maximal recursive sequences with 3-valued recursive cross-correlation functions.* IEEE Trans. Inform. Theory **14** (1968), 154–156.

[41] F. Göloğlu. *Gold-hybrid APN functions.* Preprint (2020).

[42] H. Janwa, and R. Wilson. *Hyperplane sections of Fermat varieties in P^3 in char. 2 and some applications to cyclic codes.* Proceedings of AAECC-10, LNCS **673** (1993), Berlin, Springer-Verlag, 180–194.

[43] N. Kaleyski, and K. Li. Personal communications, (2020).

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

[45] C. Kaspers, and Y. Zhou. *A lower bound on the number of inequivalent APN functions.* ArXiv preprint (2020).

[46] L. Kölsch. *On CCZ-equivalence of the inverse function.* ArXiv preprint (2020).

[47] G. Lachaud, and J. Wolfmann. *The Weights of the Orthogonals of the Extended Quadratic Binary Goppa Codes.* IEEE Trans. Inform. Theory **36** (1990), 686–692.

[48] M. Matsui. *Linear cryptanalysis methods for DES cipher.* Advances in Cryptology, Eurocrypt'93, Lecture Notes in Comput.Sci. **65** (1993), 386–397.

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

[50] K. Nyberg. *S-boxes and round functions with controllable linearity and differential uniformity.* Fast Software Encryption 1994, Lecture Notes in Computer Science **1008** (1995), 111–130.

[51] H. Taniguchi. *On some quadratic APN functions.* Designs, Codes and Cryptography **87** (2019), 1973–1983.

[52] G. Weng, Y. Tan, and G. Gong. *On quadratic almost perfect nonlinear functions and their related algebraic object.* Proceedings of Workshop on Coding and Cryptography (2013).

[53] Y. Yu, M. Wang, and Y. Li. *A matrix approach for constructing quadratic APN functions.* Designs, Codes and Cryptography **73** (2014), 587–600.

[54] Y. Zhou, and A. Pott. *A New Family of Semifields with 2 Parameters.* Advances in Mathematics **234** (2013), 43–60.

Naslov

Marco Calderini, Lilya Budaghyan i Claude Carlet

Sažetak. Hrvatski prijevod sažetka.

Marco Calderini
Department of Informatics
University of Bergen
Bergen 5005, Norway
E-mail: marco.calderini@uib.no

Lilya Budaghyan
Department of Informatics
University of Bergen
Bergen 5005, Norway
E-mail: lilya.budaghyan@uib.no

Claude Carlet
Department of Informatics
University of Bergen
Bergen 5005, Norway
LAGA, University of Paris 8
Saint-Denis 93526, France.
E-mail: claude.carlet@gmail.com