Classes of Quadratic APN Trinomials and Hexanomials and Related Structures

Lilya Budaghyan* and Claude Carlet†

Abstract

A method for constructing differentially 4-uniform quadratic hexanomials has been recently introduced by J. Dillon. We give various generalizations of this method and we deduce the constructions of new infinite classes of almost perfect nonlinear quadratic trinomials and hexanomials from $\mathbb{F}_{2^{2m}}$ to $\mathbb{F}_{2^{2m}}$. We check for $m = 3$ that some of these functions are CCZ-inequivalent to power functions.

Keywords. Affine equivalence, Almost bent, Almost perfect nonlinear, CCZ-equivalence, Differential uniformity, Nonlinearity, S-box, Vectorial Boolean function.

1 Introduction

A function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is called *differentially δ-uniform* [33] if for every $a \neq 0$ and every b in $\mathbb{F}_2^n$, the equation $F(x)+F(x+a) = b$ admits at most δ solutions. Vectorial Boolean functions used as S-boxes in block ciphers must have low differential uniformity to allow high resistance to the differential cryptanalysis (see [3]). In this sense differentially 2-uniform functions, called *almost perfect nonlinear* (APN), are optimal (since for any function, we have $\delta \geq 2$). The notion of APN function is closely connected to the notion of almost bent (AB) function [18]. A function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is called AB if the minimum Hamming distance between all the Boolean functions $v \cdot F$, $v \in \mathbb{F}_2^n \setminus \{0\}$ (called the *component* functions of F), and all affine Boolean functions on $\mathbb{F}_2^n$ is maximal. AB functions exist for n odd only and oppose an optimum resistance to the linear cryptanalysis (see [31]). Besides, every AB function is APN [18], and in the n odd case, any quadratic function is APN if and only if it is AB [17].

The APN and AB properties are preserved by some transformations of functions [17, 33]. If F is an APN function, A_1, A_2 are affine permutations and A is affine then the function $F' = A_1 \circ F \circ A_2 + A$ is also APN (the functions F and F' are then called extended

[*] Department of Mathematics, University of Trento, I-38050 Povo (Trento), ITALY; e-mail: lilia.b@mail.ru; supported by a postdoctoral fellowship of MIUR-Italy via PRIN 2006

[†] Department of Mathematics, University of Paris 8 (MAATICAH); also with INRIA, Projet CODES, BP 105 - 78153, Le Chesnay Cedex, FRANCE; e-mail: claude.carlet@inria.fr

affine equivalent (*EA-equivalent*) and simply affine equivalent if $A = 0$). Besides, the inverse of any APN permutation is APN too. Until recently, the only known constructions of APN and AB functions were EA-equivalent to power functions $F(x) = x^d$ over finite fields ($\mathbb{F}_{2^n}$ being identified with $\mathbb{F}_2^n$). Table 1 gives all known values of exponents d (up to multiplication by a power of 2 modulo $2^n - 1$, and up to taking the inverse when a function is a permutation) such that the power function x^d over $\mathbb{F}_{2^n}$ is APN. For n odd, the Gold, Kasami, Welch and Niho APN functions from Table 1 are also AB (for the proofs of AB property see [14, 15, 26, 27, 29, 33]).

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

Functions	Exponents d	Conditions	References
Gold	$2^i + 1$	$\gcd(i, n) = 1$	[26, 33]
Kasami	$2^{2i} - 2^i + 1$	$\gcd(i, n) = 1$	[28, 29]
Welch	$2^t + 3$	$n = 2t + 1$	[23]
Niho	$2^t + 2^{\frac{t}{2}} - 1$, t even $2^t + 2^{\frac{3t+1}{2}} - 1$, t odd	$n = 2t + 1$	[22]
Inverse	$2^{2t} - 1$	$n = 2t + 1$	[2, 33]
Dobbertin	$2^{4t} + 2^{3t} + 2^{2t} + 2^t - 1$	$n = 5t$	[24]

In [17], Carlet, Charpin and Zinoviev introduced an equivalence relation of functions, more recently called CCZ-equivalence, which corresponds to the affine equivalence of the graphs of functions and preserves APN and AB properties. EA-equivalence is a particular case of CCZ-equivalence and any permutation is CCZ-equivalent to its inverse [17]. In [11, 12], it is proven that CCZ-equivalence is more general than EA-equivalence, and classes of APN and AB functions being EA-inequivalent to power functions are constructed in [5, 11, 12] by applying CCZ-equivalence to the Gold mappings.

These new results on CCZ-equivalence have raised several interesting questions and the problem of classification (under CCZ-equivalence) of APN functions is wide open. This problem includes three open subproblems: the existence of APN power functions being CCZ-inequivalent to the mappings from Table 1, the existence of APN polynomials being CCZ-inequivalent to power mappings and to quadratic functions and the classification of quadratic APN functions. Regarding the first subproblem, it has been conjectured by Dobbertin that the classification is complete, that is, any APN power function belongs to some of the six classes from Table 1. Some results on CCZ-inequivalence among the classes of APN power functions can be found in [8]. The second of the above mentioned subproblems is an entirely open question. The third question (classifying quadratic APN functions) is wide open too; nevertheless, there are several recent results on quadratic APN functions (see [1, 6, 7, 8, 9, 20, 25, 32]). The present paper is also focused on this problem.

Different approaches for constructing quadratic APN functions being CCZ-inequivalent to power functions are proposed in [6, 20, 25, 32]. Also it is proven in [1] that any function of the type $\sum_{i=0}^{n-1} c_i x^{2^i+1}$, $c_i \in \mathbb{F}_{2^n}$, is not APN, unless only one coefficient is nonzero. Infinite classes of quadratic APN functions being CCZ-inequivalent to power functions are

Table 2
Known APN functions CCZ-inequivalent to power functions on $\mathbb{F}_{2^n}$.

No	Functions	Conditions	References
1	$x^{2^s+1}+wx^{2^{ik}+2^{mk+s}}$	$n=3k$, $\gcd(k,3)=\gcd(s,3k)=1$ $k\geq 4$, $i=sk \mod 3$, $m=3-i$ w has the order $2^{2k}+2^k+1$	[8, 9]
2	$x^{2^s+1}+wx^{2^{ik}+2^{mk+s}}$	$n=4k$, $\gcd(k,2)=\gcd(s,2k)=1$ $k\geq 3$, $i=sk \mod 4$, $m=4-i$ w has the order $2^{3k}+2^{2k}+2^k+1$	[7]
3	$x^3+\mathrm{tr}(x^9)$	$n\geq 7$ $n>2p$ for the smallest possible $p>1$ such that $p\neq 3$, $\gcd(p,n)=1$	[6]
4	$x^{2^{2i}+2^i}+bx^{q+1}+cx^{q(2^{2i}+2^i)}$	$n=2m$, $m\geq 3$, $q=2^m$ $c^{q+1}=1$, $c\notin\{\lambda^{(2^i+1)(q-1)},\lambda\in\mathbb{F}_{2^n}\}$ $\gcd(i,m)=1$, $cb^q+b\neq 0$	Corollary 1 of the present paper
5	$x(x^{2^i}+x^q+cx^{2^iq})$ $+x^{2^i}(c^qx^q+sx^{2^iq})+x^{(2^i+1)q}$	$n=2m$, $m\geq 3$, $q=2^m$ $\gcd(i,m)=1$, $s\notin\mathbb{F}_q$ $x^{2^i+1}+cx^{2^i}+c^qx+1$ is irreducible over $\mathbb{F}_{2^n}$	Corollary 2 of the present paper

constructed in [6, 7, 8, 9]. They are presented in Table 2. It is proven in [4] that there exists no APN function being CCZ-inequivalent to power mappings on $\mathbb{F}_{2^n}$ for $n\leq 5$. However, the classification of quadratic APN functions is far away from being complete. Already for $n=6$ there are at least 9 mutually CCZ-inequivalent quadratic APN polynomials which are CCZ-inequivalent to power functions [20]. In the present paper, we develop the method of constructing differentially 4-uniform quadratic polynomials introduced by Dillon [20]. We construct a new infinite class of quadratic APN trinomials and a new potentially infinite class of quadratic APN hexanomials (presented in Table 2 by cases 4 and 5) which we conjecture to be CCZ-inequivalent to power functions for $n\geq 6$ and we confirm this conjecture for $n=6$.

2 Preliminaries

Let $\mathbb{F}_2^n$ be the n-dimensional vector space over the field $\mathbb{F}_2$. Any function F from $\mathbb{F}_2^n$ to itself can be uniquely represented as a polynomial on n variables with coefficients in $\mathbb{F}_2^n$, whose degree with respect to each coordinate is at most one:

$$F(x_1,...,x_n)=\sum_{u\in\mathbb{F}_2^n}c(u)\Big(\prod_{i=1}^{n}x_i^{u_i}\Big),\qquad c(u)\in\mathbb{F}_2^n.$$

This representation is called the *algebraic normal form* of F and its degree $d^\circ(F)$ the *algebraic degree* of the function F.

Besides, the field $\mathbb{F}_{2^n}$ can be identified with $\mathbb{F}_2^n$ as a vector space. Then, viewed as a function from this field to itself, F has a unique representation as a univariate polynomial over $\mathbb{F}_{2^n}$ of degree smaller than 2^n:

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

For any k, $0 \leq k \leq 2^n - 1$, the number $w_2(k)$ of the nonzero coefficients $k_s \in \{0,1\}$ in the binary expansion $\sum_{s=0}^{n-1} 2^s k_s$ of k is called the 2-*weight* of k. The algebraic degree of F is equal to the maximum 2-weight of the exponents i of the polynomial $F(x)$ such that $c_i \neq 0$, that is, $d^\circ(F) = \max_{0 \leq i \leq n-1, c_i \neq 0} w_2(i)$ (see [17]).

A function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is *linear* if and only if $F(x)$ is a linearized polynomial over $\mathbb{F}_{2^n}$, that is,

$$\sum_{i=0}^{n-1} c_i x^{2^i}, \quad c_i \in \mathbb{F}_{2^n}.$$

The sum of a linear function and of a constant is called an *affine function*.

Let F be a function from $\mathbb{F}_{2^n}$ to itself and A_1, $A_2 : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be affine permutations. The functions F and $A_1 \circ F \circ A_2$ are then called *affine equivalent*. Affine equivalent functions have the same algebraic degree (i.e. the algebraic degree is *affine invariant*).

As recalled in the Introduction, we say that the functions F and F' are *extended affine equivalent* if $F' = A_1 \circ F \circ A_2 + A$ for some affine permutations A_1, A_2 and an affine function A. If F is not affine, then F and F' have again the same algebraic degree.

Two mappings F and F' from $\mathbb{F}_{2^n}$ to itself are called Carlet-Charpin-Zinoviev equivalent (*CCZ-equivalent*) if the graphs of F and F', that is, the subsets $G_F = \{(x, F(x)) \mid x \in \mathbb{F}_{2^n}\}$ and $G_{F'} = \{(x, F'(x)) \mid x \in \mathbb{F}_{2^n}\}$ of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$, are affine equivalent. Hence, F and F' are CCZ-equivalent if and only if there exists an affine automorphism $\mathcal{L} = (L_1, L_2)$ of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ such that

$$y = F(x) \Leftrightarrow L_2(x,y) = F'(L_1(x,y)).$$

Note that since $\mathcal{L}$ is a permutation then the function $L_1(x, F(x))$ has to be a permutation too (see [8]). As shown in [17], EA-equivalence is a particular case of CCZ-equivalence and any permutation is CCZ-equivalent to its inverse.

For a function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and any elements $a, b \in \mathbb{F}_{2^n}$ we denote

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

F is called a *differentially δ-uniform* function if $\max_{a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}} \delta_F(a,b) \leq \delta$. Note that $\delta \geq 2$ for any function over $\mathbb{F}_{2^n}$. Differentially 2-uniform mappings are called *almost perfect nonlinear*.

For any function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ we denote

$$\lambda_F(a,b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{tr}(bF(x)+ax)}, \qquad a, b \in \mathbb{F}_{2^n},$$

where $\mathrm{tr}(x) = x + x^2 + x^4 + ... + x^{2^{n-1}}$ is the trace function from $\mathbb{F}_{2^n}$ into $\mathbb{F}_2$. The set $\Lambda_F = \{\lambda_F(a, b) : a, b \in \mathbb{F}_{2^n}, b \neq 0\}$ is called the *Walsh spectrum* of the function F and the multiset $\{|\lambda_F(a, b)| : a, b \in \mathbb{F}_{2^n}, b \neq 0\}$ is called the *extended Walsh spectrum* of F. The value

$$\mathcal{NL}(F) = 2^{n-1} - \frac{1}{2} \max_{a\in\mathbb{F}_{2^n}, b\in\mathbb{F}^*_{2^n}} |\lambda_F(a, b)|$$

equals the *nonlinearity* of the function F. The nonlinearity of any function F satisfies the inequality

$$\mathcal{NL}(F) \leq 2^{n-1} - 2^{\frac{n-1}{2}}$$

([18, 35]) and in case of equality F is called *almost bent* or *maximum nonlinear.*

Obviously, AB functions exist only for n odd. It is proven in [18] that every AB function is APN and its Walsh spectrum equals $\{0, \pm 2^{\frac{n+1}{2}}\}$. If n is odd, every APN mapping which is quadratic (that is, whose algebraic degree equals 2) is AB [17], but this is not true for nonquadratic cases: the Dobbertin and the inverse APN functions are not AB (see [15, 17]). When n is even, the inverse function x^{2^n-2} is a differentially 4-uniform permutation [33] and has the best known nonlinearity [30], that is $2^{n-1} - 2^{\frac{n}{2}}$ (see [15, 21]). This function has been chosen as the basic S-box, with $n = 8$, in the Advanced Encryption Standard (AES), see [19]. A comprehensive survey on APN and AB functions can be found in [16].

It is shown in [17] that, if F and G are CCZ-equivalent, then F is APN (resp. AB) if and only if G is APN (resp. AB). More generally, CCZ-equivalent functions have the same differential uniformity and the same extended Walsh spectrum (see [11]). Further invariants for CCZ-equivalence are given in [25] (see also [20]) in terms of group algebras. Let $G = \mathbb{F}_2[\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}]$ be the group algebra of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ over $\mathbb{F}_2$. It consists of the formal sums

$$\sum_{g\in G} a_g g$$

where $a_g \in \mathbb{F}_2$. If S is a subset of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ then it can be identified with the element $\sum_{s\in S} s$ of G. For any APN mapping F we denote

$$\Delta_F = \{(a, b) : F(x) + F(x + a) = b \text{ has 2 solutions}\} \subset \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} .$$

The dimensions of the ideals of G generated by Δ_F and by the graph G_F of F are called Δ- and Γ-ranks, respectively. According to [25] (and also [20]), Δ- and Γ-ranks of a function are CCZ-invariant.

3 Constructions of differentially 4-uniform quadratic mappings

As recalled in the Introduction, different methods for constructing APN (or differentially 4-uniform) functions are presented in [6, 20, 25, 32]. In [25] it is shown that one of the ways to construct APN polynomials is to consider linear combinations of two different

Gold power functions. Using this approach two quadratic APN binomials on $\mathbb{F}_{2^{10}}$ and $\mathbb{F}_{2^{12}}$, which are CCZ-inequivalent to power maps, are introduced in [25]. The APN binomial of the field $\mathbb{F}_{2^{12}}$ has been proven in [8, 9] for being part of infinite sequences of quadratic APN binomials (given in Table 2 by the first and the second cases) while the APN function of the field $\mathbb{F}_{2^{10}}$ from [25] is not explained yet by any infinite family.

Another approach for constructing quadratic APN polynomials CCZ-inequivalent to power functions is introduced in [6]. This approach is based on the fact that for any APN function F and any function G the function $F(x) + \mathrm{tr}(G(x))$ has differential uniformity at most 4. The third class of APN polynomials presented in Table 2 is obtained by application of this method.

A third approach, given in [20], is to consider quadratic hexanomials of the type

$$F(x) = x(Ax^2 + Bx^q + Cx^{2q}) + x^2(Dx^q + Ex^{2q}) + Gx^{3q} \tag{1}$$

over $\mathbb{F}_{2^{2m}}$ with $q = 2^m$ as good candidates for being differentially 4-uniform. This approach gives new examples of quadratic APN functions over $\mathbb{F}_{2^6}$ and $\mathbb{F}_{2^8}$ which are CCZ-inequivalent to power functions [20]. Besides, the infinite family of APN functions introduced in the next section and presented by the fourth case in Table 2 is based on construction (1). It should be noted that similar approach was used to construct new quadratic APN quadrinomials over $\mathbb{F}_{2^6}$ in [32].

Below we suggest natural generalizations of the method from [20], but first let us recall the arguments leading to the construction (1). Let a function F be defined by (1). Since F is quadratic then in order to determine its differential uniformity it is enough to know the numbers of solutions of the equations $F(x + a) + F(x) + F(a) = 0$ for all nonzero elements a of $\mathbb{F}_{2^{2m}}$. We get

$$\begin{array}{rcl} f_1 & = & F(x+a) + F(x) + F(a) = a_1x + a_2x^2 + a_3x^q + a_4x^{2q} = 0 \\ f_2 & = & a_2^q f_1 + a_4 f_1^q = b_1x + b_2x^2 + b_3x^q = 0 \\ f_3 & = & b_3^2 f_1 + a_3b_3f_2 + a_4f_2^2 = c_1x + c_2x^2 + c_3x^4 = 0. \end{array}$$

Hence, if either c_1, c_2 or c_3 is different from 0 then F can have differential uniformity at most 4. In practice this condition on coefficients is very important. Indeed, the construction (1) gives all quadratic functions on the field $\mathbb{F}_{2^4}$ and we have checked by running a computer that only about 3/4 of them are differentially 4-uniform. For the field F_{2^6} only about 18/41 of all functions generated by (1) are differentially 4-uniform.

Let us now consider the construction

$$\begin{aligned} F'(x) = x(Ax^2 + Bx^4 + Cx^q + Dx^{2q} + Ex^{4q}) + x^2(Gx^4 + Hx^q + Ix^{2q} + Jx^{4q}) \\ +x^4(Kx^q + Lx^{2q} + Mx^{4q}) + x^q(Nx^{2q} + Px^{4q}) + Qx^{2q+4q}. \end{aligned}$$

For the function F' and for any nonzero elements a of $\mathbb{F}_{2^{2m}}$ we get

$$\begin{array}{rcl} f'_1 & = & F(x+a) + F(x) + F(a) = a'_1x + a'_2x^2 + a'_3x^4 + a'_4x^q + a'_5x^{2q} + a'_6x^{4q} = 0 \\ f'_2 & = & a'^q_3 f'_1 + a'_6 f'^q_1 = b'_1x + b'_2x^2 + b'_3x^4 + b'_4x^q + b'_5x^{2q} = 0 \\ f'_3 & = & b'_3f'_1 + a'_3f'_2 = c'_1x + c'_2x^2 + c'_3x^q + c'_4x^{2q} + c'_5x^{4q} = 0 \\ f'_4 & = & c'^q_5 f'_2 + b'_3 f'^q_3 = d'_1x + d'_2x^2 + d'_3x^q + d'_4x^{2q} = 0. \end{array}$$

Thus, if some of the coefficients d'_2, d'_3, d'_4 are different from 0 then we see that f'_4 has the same form as f_1. Therefore, applying the Dillon method to $f_1 = f'_4$, we get that if some of the coefficients d'_2, d'_3, d'_4, and some of the coefficients c_1, c_2, c_3, are different from 0 then F' is differentially 4-uniform. Obviously, the probability that we can prove this way that the function F' is differentially 4-uniform is less than in the case of construction (1) since we have an additional condition (on coefficients d'_2, d'_3, d'_4). And actually, we checked by computer investigation that only about 1/4 of the quadratic functions on the field $\mathbb{F}_{2^6}$ are differentially 4-uniform (while all of them have the same form as F').

Obviously, construction (1) can be further generalized. For any i we denote

$$F^{(i)}(x) = \sum_{0 \le t < j \le i} a_{tj} x^{2^t + 2^j} + \sum_{0 \le t, j \le i} b_{tj} x^{2^t + 2^j q} + \sum_{0 \le t < j \le i} c_{tj} x^{q(2^t + 2^j)}$$

and consider $F^{(i)}$ over $\mathbb{F}_{2^{2m}}$ with $m \ge i + 1$. Obviously, the cases $i = 1, 2$ correspond to the functions F and F'. For arbitrary i, using induction, we get that, under a condition on the coefficients translating that no relation obtained in the process completely vanishes, the function $F^{(i)}$ is differentially 4-uniform. Note that all quadratic functions have the form $F^{(i)}(x)$ for $i = m - 1$. But clearly, with increasing i the probability that we can prove this way that $F^{(i)}$ is differentially 4-uniform decreases since the number of conditions on coefficients grows. Nevertheless, we exhibit in the next section two subcases where these constructions succeed in providing differentially 4-uniform polynomials, and we can even deduce two new infinite classes of APN quadratic functions.

4 New infinite classes of APN functions

Functions whose nonzero derivatives are all 2^k-to-1 mappings (i.e. reach any value either 0 or 2^k times) are studied in [10]. The simplest examples of such functions over $\mathbb{F}_{2^n}$ are x^{2^i+1} when $\gcd(i, n) = k$. The following theorems give new classes of such functions - of APN functions when $k = 1$.

4.1 Trinomials

Theorem 1 *Let m and i be any integers, $q = 2^m$, $n = 2m$, $\gcd(i, m) = k$ and $c, b \in \mathbb{F}_{2^n}$ be such that $c^{q+1} = 1$, $c \notin \{\lambda^{(2^i+1)(q-1)}, \lambda \in \mathbb{F}_{2^n}\}$, $cb^q + b \neq 0$. Then all the nonzero derivatives of the function*

$$F(x) = x^{2^{2i} + 2^i} + bx^{q+1} + cx^{q(2^{2i} + 2^i)}$$

are 2^k-to-1 mappings of $\mathbb{F}_{2^n}$.

Proof. Since F is quadratic, then for any nonzero a in $\mathbb{F}_{2^n}$ the function $F(x + a) + F(x)$ is 2^k-to-1 if and only if the equation

$$f_1 = F(x+a) + F(x) + F(a) = ba^q x + a^{2^{2i}} x^{2^i} + a^{2^i} x^{2^{2i}} + bax^q + ca^{2^{2i}q} x^{2^i q} + ca^{2^i q} x^{2^{2i} q} = 0$$

has 2^k solutions. This equation implies

$$f_1 + cf_1^q = (cb^q + b)(ax^q + a^q x) = 0$$

and, since $cb^q + b \neq 0$, then $x = au$, $u \in \mathbb{F}_q$. The equation $f_1 = 0$ becomes

$$(a^{2^{2i}+2^i} + ca^{q(2^{2i}+2^i)})(u^{2^i} + u^{2^{2i}}) = 0.$$

The condition $c \notin \{\lambda^{(2^i+1)(q-1)}, \lambda \in \mathbb{F}_{2^n}\}$ implies that $a^{2^{2i}+2^i} + ca^{q(2^{2i}+2^i)} \neq 0$. Hence, if $\gcd(i, m) = k$ then $F(x + a) + F(x)$ is 2^k-to-one for any nonzero a. □

Clearly, for k equal 1 and 2 Theorem 1 gives differentially 2- and 4-uniform functions respectively.

Corollary 1 *Let m be any integer, $q = 2^m$, $n = 2m$, i be such that $\gcd(i, m) = 1$, and $c, b \in \mathbb{F}_{2^n}$ be such that $c^{q+1} = 1$, $c \notin \{\lambda^{(2^i+1)(q-1)}, \lambda \in \mathbb{F}_{2^n}\}$, $cb^q + b \neq 0$. Then the function*

$$F(x) = x^{2^{2i}+2^i} + bx^{q+1} + cx^{q(2^{2i}+2^i)}$$

is APN on $\mathbb{F}_{2^n}$.

Note that vectors c, b satisfying the hypotheses of Theorem 1 do exist for every odd m and i. Indeed, an element c such that $c^{q+1} = 1$ and $c \notin \{\lambda^{(2^i+1)(q-1)}, \lambda \in \mathbb{F}_{2^n}\}$ exists because for i odd $2^i + 1$ is divisible by 3 and $3(q - 1)$ divides $q^2 - 1$ and we can take for c any $(q-1)$-th power of a primitive element which is not the $3(q-1)$-th power of an element of the field and b clearly exists too (take for instance $b = 1$). When $i = 1$ this sufficient condition on m is also necessary since if m is even then $\gcd(3(q - 1), q^2 - 1) = q - 1$, so there does not exist such c.

4.2 Hexanomials

Theorem 2 *Let n be any even integer, $q = 2^{n/2}$, $\gcd(i, n/2) = k$, and $c, s \in \mathbb{F}_{2^n}$ be such that $s \notin \mathbb{F}_q$. If the equation*

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

has no solution x such that $x^{q+1} = 1$, and in particular if the polynomial $X^{2^i+1} + cX^{2^i} + c^q X + 1$ is irreducible over $\mathbb{F}_{2^n}$, then all the nonzero derivatives of the function

$$F(x) = x(x^{2^i} + x^q + cx^{2^i q}) + x^{2^i}(c^q x^q + sx^{2^i q}) + x^{(2^i+1)q}$$

are 2^k-to-1 mappings of $\mathbb{F}_{2^n}$.

Proof. Since F is quadratic then for any nonzero a the function $F(x+a)+F(x)$ is 2^k-to-1 if and only if the equation $F(x + a) + F(x) + F(a) = 0$ has 2^k solutions.

We have

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

$$(a^{2^i}+a^q+ca^{2^iq})x+(a+c^qa^q+sa^{2^iq})x^{2^i}+(a+c^qa^{2^i}+a^{2^iq})x^q+(ca+sa^{2^i}+a^q)x^{2^iq}$$

and

$$(F(x+a)+F(x)+F(a))^q=$$

$$(a^{2^iq}+a+c^qa^{2^i})x^q+(a^q+ca+s^qa^{2^i})x^{2^iq}+(a^q+ca^{2^iq}+a^{2^i})x+(c^qa^q+s^qa^{2^iq}+a)x^{2^i}.$$

The sum of this two expressions equals $(s+s^q)(a^{2^iq}x^{2^i}+a^{2^i}x^{2^iq})$. Hence, since $s+s^q\neq 0$ then $F(x+a)+F(x)+F(a)=0$ and $x\neq 0$ imply $x^{q-1}=a^{q-1}$, that is, $x=ua$ where $u\in\mathbb{F}_q^*$. Replacing x by ua, we get

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

$$(u^{2^i}a^{2^i}+ua^q+cu^{2^i}a^{2^iq})a+(ua+c^qua^q+su^{2^i}a^{2^iq})a^{2^i}+(ua+c^qu^{2^i}a^{2^i}+u^{2^i}a^{2^iq})a^q$$

$$+(cua+su^{2^i}a^{2^i}+ua^q)a^{2^iq}=(u+u^{2^i})(a^{2^i+1}+a^{(2^i+1)q}+ca^{2^iq+1}+c^qa^{2^i+q}).$$

The equation $u+u^{2^i}=0$ has 2^k solutions. We deduce that $F(x+a)+F(x)$ is 2^k-to-1 if the equation $x^{2^i+1}+x^{(2^i+1)q}+cx^{2^iq+1}+c^qx^{2^i+q}=0$ admits no nonzero solution or, equivalently, the equation $x^{(2^i+1)(q-1)}+cx^{2^i(q-1)}+c^qx^{q-1}+1=0$ has no solutions, or in other words, if the equation

$$y^{2^i+1}+cy^{2^i}+c^qy+1=0$$

has no solution y such that $y^{q+1}=1$. This happens (for instance) when the polynomial $X^{2^i+1}+cX^{2^i}+c^qX+1$ is irreducible over $\mathbb{F}_{2^n}$. □

Obviously, for the special case $k=2$, Theorem 2 gives differentially 4-uniform functions and for $k=1$, it gives a class of APN functions.

Corollary 2 *Let n be any even integer, $q=2^{n/2}$, $\gcd(i,n/2)=1$, and $c,s\in\mathbb{F}_{2^n}$ be such that $s\notin\mathbb{F}_q$. If the equation*

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

has no solution x such that $x^{q+1}=1$, and in particular if the polynomial $X^{2^i+1}+cX^{2^i}+c^qX+1$ is irreducible over $\mathbb{F}_{2^n}$, then the function

$$F(x)=x(x^{2^i}+x^q+cx^{2^iq})+x^{2^i}(c^qx^q+sx^{2^iq})+x^{(2^i+1)q}$$

is APN on $\mathbb{F}_{2^n}$.

The class of APN functions of Corollary 2 depends on existence of elements $c\in\mathbb{F}_{2^n}$ for which the polynomial $x^{2^i+1}+cx^{2^i}+c^qx+1$ is irreducible over $\mathbb{F}_{2^n}$. We checked with a computer that for $i=1$ such elements always exist at least for all even n, $6\leq n\leq 1000$, not divisible by 3. In case n divisible by 6, $6\leq n\leq 1000$, such elements exist at least for 140 out of 166 checked fields. We also checked that for $6\leq n\leq 26$ the number of elements c for which the polynomial is irreducible is in average 3/10-th of all elements.

4.3 Their inequivalence with power functions

The Dobbertin APN functions have unique Walsh spectra which are different from the Walsh spectra of quadratic APN functions (see [14, 34]). Since the extended Walsh spectrum of a function is invariant under CCZ-equivalence then we can make the following conclusion.

Proposition 1 *The functions of Corollaries 1 and 2 are CCZ-inequivalent to the Dobbertin APN functions.*

The APN functions from Corollaries 1 and 2 are CCZ-inequivalent to power functions at least for $n = 6$. Indeed, their Γ-ranks equal 1146, while the only APN power function x^3 on $\mathbb{F}_{2^6}$ has the Γ-rank 1104.

Proposition 2 *The functions of Corollaries 1 and 2 are CCZ-inequivalent to power functions on $\mathbb{F}_{2^6}$.*

Acknowledgement

The authors are indebted to John Dillon for nice observations.

References

[1] T. Berger, A. Canteaut, P. Charpin and Y. Laigle-Chapuy. On almost perfect nonlinear functions over F_2^n. *IEEE Trans. Inform. Theory*, vol. 52, no. 9, Sept. 2006.

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

[3] E. Biham and A. Shamir. Differential Cryptanalysis of DES-like Cryptosystems. *Journal of Cryptology*, vol. 4, No.1, pp. 3-72, 1991.

[4] M. Brinkman and G. Leander. On the classification of APN functions up to dimension five. To appear in the proceedings of WCC 2007.

[5] L. Budaghyan. The simplest method for constructing APN polynomials EA-inequivalent to power functions. Submitted, available at http://eprint.iacr.org/2007/058

[6] L. Budaghyan, C. Carlet, G. Leander. Constructing new APN functions from known ones. Preprint, available at http://eprint.iacr.org/2007/063

[7] L. Budaghyan, C. Carlet, G. Leander. Another class of quadratic APN binomials over $\mathbb{F}_{2^n}$: the case n divisible by 4. Submitted, available at http://eprint.iacr.org/2006/428.pdf

[8] L. Budaghyan, C. Carlet, G. Leander. A class of quadratic APN binomials inequivalent to power functions. Submitted, available at http://eprint.iacr.org/2006/445.pdf

[9] L. Budaghyan, C. Carlet, P. Felke, G. Leander. An infinite class of quadratic APN functions which are not equivalent to power mappings. *Proceedings of the IEEE International Symposium on Information Theory 2006*, Seattle, USA, Jul. 2006.

[10] L. Budaghyan and A. Pott. On Differential Uniformity and Nonlinearity of Functions. Submitted, 2006.

[11] L. Budaghyan, C. Carlet, A. Pott. New Classes of Almost Bent and Almost Perfect Nonlinear Functions. *IEEE Trans. Inform. Theory*, vol. 52, no. 3, pp. 1141-1152, March 2006.

[12] L. Budaghyan, C. Carlet, A. Pott. New Constructions of Almost Bent and Almost Perfect Nonlinear Functions. *Proceedings of the Workshop on Coding and Cryptography 2005*, P. Charpin and Ø. Ytrehus eds, pp. 306-315, 2005.

[13] A. Canteaut, P. Charpin and H. Dobbertin. A new characterization of almost bent functions. *Fast Software Encryption 99, LNCS* 1636, L. Knudsen edt, pp. 186-200. Springer-Verlag, 1999.

[14] A. Canteaut, P. Charpin and H. Dobbertin. Binary m-sequences with three-valued crosscorrelation: A proof of Welch's conjecture. *IEEE Trans. Inform. Theory*, 46 (1), pp. 4-8, 2000.

[15] A. Canteaut, P. Charpin, 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), pp. 105-138, 2000.

[16] C. Carlet. Vectorial (multi-output) Boolean Functions for Cryptography. Chapter of the monography *Boolean Methods and Models*, Y. Crama and P. Hammer eds, Cambridge University Press, to appear soon. Preliminary version available at http://www-rocq.inria.fr/codes/Claude.Carlet/pubs.html

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

[18] F. Chabaud and S. Vaudenay. Links between differential and linear cryptanalysis, *Advances in Cryptology -EUROCRYPT'94, LNCS*, Springer-Verlag, New York, 950, pp. 356-365, 1995.

[19] J. Daemen and V. Rijmen. AES proposal: Rijndael. http://csrc.nist.gov/encryption/aes/rijndael/Rijndael.pdf, 1999.

[20] J. F. Dillon. APN Polynomials and Related Codes. *Polynomials over Finite Fields and Applications*, Banff International Research Station, Nov. 2006.

[21] H. Dobbertin. One-to-One Highly Nonlinear Power Functions on $GF(2^n)$. *Appl. Algebra Eng. Commun. Comput.* 9 (2), pp. 139-152, 1998.

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

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

[24] H. Dobbertin. Almost perfect nonlinear power functions over $GF(2^n)$: a new case for n divisible by 5. D. Jungnickel and H. Niederreiter eds. *Proceedings of Finite Fields and Applications FQ5*, Augsburg, Germany, Springer, pp. 113-121, 2000.

[25] Y. Edel, G. Kyureghyan and A. Pott. A new APN function which is not equivalent to a power mapping. *IEEE Trans. Inform. Theory*, vol. 52, no. 2, pp. 744-747, Feb. 2006.

[26] R. Gold. Maximal recursive sequences with 3-valued recursive crosscorrelation functions. *IEEE Trans. Inform. Theory*, 14, pp. 154-156, 1968.

[27] H. Hollmann and Q. Xiang. A proof of the Welch and Niho conjectures on crosscorrelations of binary m-sequences. *Finite Fields and Their Applications 7*, pp. 253-286, 2001.

[28] 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*, vol. 673, Berlin, Springer-Verlag, pp. 180-194, 1993.

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

[30] G. Lachaud and J. Wolfmann. The Weights of the Orthogonals of the Extended Quadratic Binary Goppa Codes. *IEEE Trans. Inform. Theory*, vol. 36, pp. 686-692, 1990.

[31] M. Matsui. Linear cryptanalysis method for DES cipher. *Advances in Cryptology-EUROCRYPT'93, LNCS*, Springer-Verlag, pp. 386-397, 1994.

[32] N. Nakagawa and S. Yoshiara. A construction of differentially 4-uniform functions from commutative semifields of characteristic 2. Preprint.

[33] K. Nyberg. Differentially uniform mappings for cryptography, *Advances in Cryptography, EUROCRYPT'93, LNCS*, Springer-Verlag, New York, 765, pp. 55-64, 1994.

[34] K. Nyberg. S-boxes and Round Functions with Controllable Linearity and Differential Uniformity. *Proceedings of Fast Software Encryption 1994, LNCS* 1008, pp. 111-130, 1995.

[35] V. Sidelnikov. On mutual correlation of sequences. *Soviet Math. Dokl.*, 12, pp. 197-201, 1971.