An infinite class of quadratic APN functions which are not equivalent to power mappings

Lilya Budaghyan,[*] Claude Carlet,[†] Patrick Felke,[‡] Gregor Leander[§]

Abstract

We exhibit an infinite class of almost perfect nonlinear quadratic polynomials from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ ($n \geq 12$, n divisible by 3 but not by 9). We prove that these functions are EA-inequivalent to any power function. In the forthcoming version of the present paper we will proof that these functions are CCZ-inequivalent to any Gold function and to any Kasami function, in particular for $n = 12$, they are therefore CCZ-inequivalent to power functions.

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

1 Introduction

Since the introduction by Biham and Shamir of differential attacks on block ciphers [4] and by Matsui of linear attacks [28], and since the introduction by Nyberg [30] of the related notion of almost perfect nonlinear (APN) mappings, and by Chabaud and Vaudenay of the notion of almost bent (AB) mappings [13], much work has been done on these two notions [1, 3, 5, 6, 7, 8, 11, 16, 17, 18, 19, 23, 24, 25]. A function $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ is called APN 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 two (that is, 0 or 2) solutions (it is also called differentially 2-uniform). A function F is called AB if the minimum Hamming distance between all Boolean functions $v \cdot F$, $v \neq 0$ (where "$\cdot$" denotes the usual inner product in $\mathbb{F}_2^n$) and all affine functions on $\mathbb{F}_2^n$ is maximum

[*]Institute of Algebra and Geometry, Otto-von-Guericke University Magdeburg, D-39016 Magdeburg, GERMANY; e-mail: lilya.budaghyan@student.uni-magdeburg.de.

[†]INRIA, Projet CODES, BP 105 - 78153, Le Chesnay Cedex, FRANCE; e-mail: claude.carlet@inria.fr; also member of the University of Paris 8.

[‡]Department of Mathematics, Ruhr-University, Bochum, D-44780 Bochum, GERMANY; e-mail: felke@itsc.ruhr-uni-bochum.de

[§]Department of Mathematics, Ruhr-University, Bochum, D-44780 Bochum, GERMANY; e-mail: leander@itsc.ruhr-uni-bochum.de

(this distance is called the nonlinearity of F and this maximum equals $2^{n-1} - 2^{\frac{n-1}{2}}$). A comprehensive survey on APN and AB functions can be found in [10].

Until recently, all known constructions of APN and AB functions happened to be EA-equivalent to power functions x^d (where x ranges over the finite field $\mathbb{F}_{2^n}$, identified as a vector space to $\mathbb{F}_2^n$). Recall that two functions F and F' are called *extended affine equivalent* (EA-equivalent) if $F' = A_1 \circ F \circ A_2 + A$, where the mappings A, A_1, A_2 are affine, and where A_1, A_2 are permutations. Table 1 (resp. Table 2) 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 is APN (resp. AB).

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

	Exponents d	Conditions	$w_2(d)$	Proven in
Gold functions	$2^i + 1$	$\gcd(i, n) = 1$	2	[22, 30]
Kasami functions	$2^{2i} - 2^i + 1$	$\gcd(i, n) = 1$	$i + 1$	[25, 26]
Welch function	$2^t + 3$	$n = 2t + 1$	3	[18]
Niho function	$2^t + 2^{\frac{t}{2}} - 1$, t even $2^t + 2^{\frac{3t+1}{2}} - 1$, t odd	$n = 2t + 1$	$(t + 2)/2$ $t + 1$	[17]
Inverse function	$2^{2t} - 1$	$n = 2t + 1$	$n - 1$	[3, 30]
Dobbertin function	$2^{4i} + 2^{3i} + 2^{2i} + 2^i - 1$	$n = 5i$	$i + 3$	[19]

Table 2
Known AB power functions x^d on $\mathbb{F}_{2^n}$, n odd.

	Exponents d	Conditions	Proven in
Gold functions	$2^i + 1$	$\gcd(i, n) = 1$	[22, 30]
Kasami functions	$2^{2i} - 2^i + 1$	$\gcd(i, n) = 1$	[26]
Welch function	$2^t + 3$	$n = 2t + 1$	[7, 8]
Niho function	$2^t + 2^{\frac{t}{2}} - 1$, t even $2^t + 2^{\frac{3t+1}{2}} - 1$, t odd	$n = 2t + 1$	[24]

Every AB function is APN [13]. The converse is not true in general since AB functions exist only when n is odd while APN functions exist for n even too. Besides, in the n odd case, the Dobbertin APN function is not AB as proven in [8]. Also, in this same case, 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 [11]). But, if n is odd again, every APN mapping which is quadratic (that is, whose algebraic degree equals 2) is AB.

When n is even, the inverse function x^{2^n-2} is a differentially 4-uniform permutation [30] and has the best known nonlinearity [27], that is $2^{n-1} - 2^{\frac{n}{2}}$ (see [8, 16]). This function has been chosen as the basic S-box, with $n = 8$, in the Advanced Encryption Standard (AES), see [15].

Several conjectures have been made on APN and AB functions. In particular, it had been conjectured (in different terms) that all APN functions are EA-equivalent to power functions and in [11] that all AB functions are EA-equivalent to permutations, and that all quadratic AB functions are EA-equivalent to Gold functions (this last conjecture has been restated for APN functions in [2]). Using the stability properties studied in [11] and more recently called CCZ-equivalence, a new infinite class of APN functions has been introduced in [5] and disproves the two first conjectures.

The new APN and AB functions introduced in [5] are, by construction, CCZ-equivalent to Gold functions. Hence, the problem of knowing whether there exist APN functions which would be CCZ-inequivalent to power functions remained open after their introduction. A recent paper [21] by Edel, Kyureghyan and Pott introduces two quadratic functions from $F_{2^{10}}$ (resp. $F_{2^{12}}$) to itself, which is proved to be CCZ-inequivalent to any power function. The exhibition of this function also disproves the third of the conjectures recalled above.

This (quadratic) function is isolated and this leaves open the question of knowing whether a whole infinite class of APN functions being not CCZ-equivalent to power functions can be exhibited.

In the present paper, we introduce an infinite class of quadratic functions on every number of variables n, divisible by 3, but not by 9. We show that, for $n \geq 12$, these functions are EA-inequivalent to power functions and, in the next version of this paper, CCZ-inequivalent to Gold and Kasami functions. This implies in particular that, for $n = 12$, they are CCZ-inequivalent to power functions.

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 1:

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

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 $\mathbb{F}_{2^n}$ being an n-dimensional vector space over $\mathbb{F}_2$, it 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 [11]).

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 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 introduction, we say that the functions F and F' are *extended affine equivalent* (EA-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.

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

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

and

$$\Delta_F = \{\delta_F(a,b) : a, b \in \mathbb{F}_2^n, a \neq 0\}.$$

F is called a *differentially δ-uniform* function if $\max_{a\in\mathbb{F}_2^{n*}, b\in\mathbb{F}_2^n} \delta_F(a,b) \leq \delta$, where $\mathbb{F}_2^{n*} = \mathbb{F}_2^n \setminus \{0\}$. For any $a, b \in \mathbb{F}_2^n$, the number $\delta_F(a,b)$ is even since if x_0 is a solution of the equation $F(x+a) + F(x) = b$ then $x_0 + a$ is a solution too. Hence, $\delta \geq 2$. Differentially 2-uniform mappings are called *almost perfect nonlinear.*

For any function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, the distribution of the values

$$\lambda_F(a,b) = \sum_{x\in\mathbb{F}_2^n} (-1)^{b\cdot F(x) + a\cdot x}, \qquad a, b \in \mathbb{F}_2^n,$$

does not depend on a particular choice of the inner product " $\cdot$ " in $\mathbb{F}_2^n$. If we identify $\mathbb{F}_2^n$ with $\mathbb{F}_{2^n}$ then we can take $x \cdot y = tr(xy)$, where $tr(x) = x + x^2 + x^4 + ... + x^{2^{n-1}}$ 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 F and 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

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

([13, 33]) and in case of equality F is called *almost bent* or *maximum nonlinear.* For any AB function F, the Walsh spectrum Λ_F equals $\{0, \pm 2^{\frac{m+1}{2}}\}$ as it is proven in [13].

For EA-equivalent functions F and F', we have $\Delta_F = \Delta_{F'}$, $\Lambda_F = \Lambda_{F'}$ and if F is a permutation then $\Delta_F = \Delta_{F^{-1}}$, $\Lambda_F = \Lambda_{F^{-1}}$ (see [11]).

Two mappings F and G from $\mathbb{F}_{2^n}$ to itself are called CCZ-equivalent if the graphs of F and G, that is, the subsets of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ of equations $y = F(x)$ and $y = G(x)$, are affine equivalent. Hence, F and G are CCZ-equivalent if and only if there exists an affine automorphism $L = (L_1, L_2)$ of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ such that

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

It has been shown in [11] that, if F and G are CCZ-equivalent, then F is APN (resp. AB) if and only if g is APN (resp. AB). As shown in [11] too, EA-equivalence is a particular case of CCZ-equivalence.

3 A new family of APN functions

The following theorem will prove the APN property for an large class of quadratic binomial functions. The functions for which we proof the non equivalence to power functions are a special case of the functions covered by this theorem and are described in corollary 1.

Theorem 1 *Let s and k be positive integers and $t \in \{1, 2\}$, $i = 3 - t$. Furthermore let $d = 2^{ik} + 2^{tk+s} - (2^s + 1)$,*

$$g_1 = \gcd(2^n - 1, d/(2^k - 1))$$

and

$$g_2 = \gcd(2^k - 1, d/(2^k - 1)).$$

If $g_1 \neq g_2$ then the function

$$\begin{array}{rcl} F : \mathbb{F}_{2^{3k}} & \to & \mathbb{F}_{2^{3k}} \\ x & \mapsto & \alpha^{2^k-1} x^{2^{ik}+2^{tk+s}} + x^{2^s+1} \end{array}$$

where α is a primitive element in $\mathbb{F}^*_{2^{3k}}$ is almost perfect nonlinear (APN).

Proof. Let $n = 3k$ and $L = \mathbb{F}_{2^n}$. We have to show that for every $c, e \in L$ and $c \neq 0$ the equation

$$F(x) + F(x + c) = e$$

has at most 2 solutions. We have

$$\begin{aligned} F(x) + F(x+c) &= \alpha^{2^k-1}\left(x^{2^{ik}+2^{tk+s}} + (x+c)^{2^{ik}+2^{tk+s}}\right) + x^{2^s+1} + (x+c)^{2^s+1} \\ &= \alpha^{2^k-1} c^{2^{ik}+2^{tk+s}} \left(\left(\frac{x}{c}\right)^{2^{ik}} + \left(\frac{x}{c}\right)^{2^{tk+s}}\right) \\ &\quad + c^{2^s+1}\left(\left(\frac{x}{c}\right)^{2^s} + \left(\frac{x}{c}\right)\right) \\ &\quad + \alpha^{2^k-1} c^{2^{ik}+2^{tk+s}} + c^{2^s+1} \end{aligned} \tag{1}$$

As this is a linear equation in x it is sufficient to study the kernel. Note furthermore that

$$c^{2^{ik}+2^{tk+s}-(2^s+1)} = c^{(2^k-1)(2^{k+s}+2^s+1-2^k(2^s-1)(i-1))}$$

(this can be checked separately for $i=1$ and $i=2$). To simplify notation we define:

$$a := \left(\alpha c^{2^{k+s}+2^s+1-2^k(2^s-1)(i-1)}\right)^{2^k-1}.$$

After replacing x by cx and dividing by c^{2^s+1}, we finally see that Equation (1) admits 0 or 2 solutions for every $c \in L^*$ if and only if, denoting:

$$\Delta_a(x) = a\left(x^{2^{ik}} + x^{2^{tk+s}}\right) + x^{2^s} + x,$$

the equation $\Delta_a(x) = 0$ has at most two zeros or, equivalently, that the only solutions are $x = 0$ and $x = 1$.

From now on we consider the cases $i = 1$ and $i = 2$ separately.

Case 1 $(t = 1, i = 2)$**:** The following step can be seen as a very basic application of the multivariate method introduced by Dobbertin [20]. If we denote $y = x^{2^k}$, $z = y^{2^k}$ and $b = a^{2^k}$, $c = b^{2^k}$ the equation $\Delta_a(x) = 0$ can be rewritten as

$$a(z + y^{2^s}) + (x^{2^s} + x) = 0$$

As stated before, a is always a $(2^k - 1)$-th power and thus

$$abc = 1.$$

Considering also the conjugated equations we derive the following system of equations

$$\begin{aligned} f_1 = \quad & a(z + y^{2^s}) + x^{2^s} + x = \quad 0 \\ f_2 = \quad & b(x + z^{2^s}) + y^{2^s} + y = \quad 0 \\ f_3 = \quad & \tfrac{1}{ab}(y + x^{2^s}) + z^{2^s} + z = \quad 0 \end{aligned}$$

The aim now is eliminating y and z from these equations and finally getting an equation in x only. First we compute

$$\begin{aligned} R_1 &= b(f_1)^{2^s} + a^{2^s} f_2 \\ &= a^{2^s} b y^{2^{2s}} + a^{2^s} y^{2^s} + a^{2^s} y + b x^{2^{2s}} + b x^{2^s} + a^{2^s} b x \end{aligned}$$

and

$$\begin{aligned} R_2 &= \frac{1}{a(b+1)}\left(bf_1 + af_2 + abf_3\right) \\ &= y^{2^s} + \frac{a+1}{ab+a} y + \frac{1}{a} x^{2^s} + \frac{ab+b}{ab+a} x \end{aligned}$$

to eliminate z. To eliminate $y^{2^{2s}}$ we compute

$$\begin{aligned} R_3 &= R_1 + a^{2^s} b (R_2)^{2^s} \\ &= \frac{a^{2^s}(b+1)^{2^s} + (a+1)^{2^s} b}{(b+1)^{2^s}} y^{2^s} + a^{2^s} y + \frac{a^{2^s} b^{2^s+1} + b}{b^{2^s}+1} x^{2^s} + a^{2^s} bx \end{aligned}$$

Using equations R_2 and R_3 we can eliminate y^{2^s} by computing

$$\begin{aligned} R_4 &= R_3 + \frac{a^{2^s}(b+1)^{2^s} + (a+1)^{2^s} b}{(b+1)^{2^s}} R_2 \\ &= P(a)(y + (b+1)x^{2^s} + bx) \end{aligned}$$

where

$$P(a) = \frac{(ab)^{2^s+1} + (ab)^{2^s} + a^{2^s} b + a^{2^s} + ab + b}{(b+1)^{2^s+1} a}.$$

Computing

$$\begin{aligned} R_5 &= (R_4)^{2^s} + P(a)^{2^s} R_2 \\ &= P(a)^{2^s} \left(\frac{a+1}{ab+a} y + (b^{2^s}+1) x^{2^{2s}} + \frac{ab^{2^s}+1}{a} x^{2^s} + \frac{ab+b}{ab+a} x \right) \end{aligned}$$

we finally get our desired equation

$$\begin{aligned} R_6 &= \frac{a+1}{ab+a} P(a)^{2^s-1} R_4 + R_5 \\ &= P(a)^{2^s} (b+1) \left(x^{2^{2s}} + x^{2^s} \right) \end{aligned}$$

Obviously if x is a solution of $\Delta_a(x) = 0$ then $R_6(x) = 0$. For $P(a)^{2^s}(b+1) \neq 0$ this is equivalent to $x = 0, 1$. Thus to prove the theorem we have to show that $P(a)$ does not vanish for elements a fulfilling the equation

$$a = \left(\alpha c^{2^k+2^s+1} \right)^{2^k-1} \tag{2}$$

Note that, if a satisfies (2), then a is not a (2^k+2^s+1)-th power. Indeed, $g_2 = \gcd(2^k - 1, 2^k+2^s+1)$ is always a divisor of $g_1 = \gcd(2^n-1, 2^k+2^s+1)$. And if a fulfilling (2) is a (2^k+2^s+1)-th power, then α is a (g_1/g_2)-th power. But as (g_1/g_2) is a nontrivial divisor of 2^n-1 this contradicts that α is a primitive element.

Consequently we want to show, that if $P(a) = 0$ then a is a (2^k+2^s+1)-th power. But for $\alpha \notin \mathbb{F}_2$ the equation $P(a) = 0$ is equivalent to

$$a = \left(\frac{a+1}{c+1} \right)^{2^s+1} c^{2^s+1} \left(\frac{b+1}{a+1} \right) a,$$

as can easily be seen by expansion and using that $c = 1/ab$. Note that the right hand side is always a (2^k+2^s+1)-th power. This proves the first case.

Case 2 $(t = 2, i = 1)$**:** In this case the equation $\Delta_a(x) = 0$ can be transformed into the following system of equations.

$$\begin{aligned} a(y + z^{2^s}) + (x + x^{2^s}) &= 0 \\ b(z + x^{2^s}) + (y + y^{2^s}) &= 0 \\ \frac{1}{ab}(x + y^{2^s}) + (z + z^{2^s}) &= 0. \end{aligned}$$

Again eliminating y and z similarly as before we get this time

$$P(a)^{2^s}\left(x^{2^{2s}} + x^{2^s}\right) = 0,$$

with

$$P(a) = (ab)^{2^s+1} + (ab)^{2^s} + ab^{2^s} + ab + a + b^{2^s}.$$

Using similar arguments as before it suffices in this case to show that if $P(a) = 0$ then a is a $(2^{k+s} + 2^s + 1)$-th power. For this, note that for $a \notin \mathbb{F}_2$ the equation $P(a) = 0$ is equivalent to

$$a^{2^s} = \left(\frac{a+1}{c+1}\right)^{2^s+1} c^{2^s+1}\left(\frac{b+1}{a+1}\right)^{2^s} a^{2^s}$$

and the right hand side is always a $(2^{k+s} + 2^s + 1)$-th power. □

From this theorem we get the following corollary as a special case.

Corollary 1 *Let s and k be positive integers such that $\gcd(k, 3) = \gcd(s, 3k) = 1$, and $i = sk \mod 3$, $t = 2i \mod 3$, $n = 3k$. Then the function*

$$\begin{aligned} F : \mathbb{F}_{2^{3k}} &\rightarrow \mathbb{F}_{2^{3k}} \\ x &\mapsto \alpha^{2^k-1}x^{2^{ik}+2^{tk+s}} + x^{2^s+1} \end{aligned}$$

where α is a primitive element in $\mathbb{F}^*_{2^{3k}}$ is almost perfect nonlinear (APN).

Proof. We only have to verify that in this case the greatest common divisors

$$g_1 = \gcd(2^n - 1, 2^{k+s} + 2^s + 1 - 2^k(2^s - 1)(i - 1))$$

and

$$g_2 = \gcd(2^k - 1, 2^{k+s} + 2^s + 1 - 2^k(2^s - 1)(i - 1))$$

are not the same. Indeed g_1 is always divisible by 7 while g_2 is always coprime to 7. □

It should be noted that the theorem covers a larger class of APN functions as can be seen by checking the conditions on the greatest common divisors for small values of k and s.

4 On the CCZ-inequivalence between the introduced APN functions and the Gold and the Kasami functions

Below we prove the EA-inequivalence between the APN functions introduced in Corollary 1 and all power functions.

Theorem 2 *Let n be a positive integer and let s, j, q be three nonzero elements of $\mathbb{Z}/n\mathbb{Z}$ such that $q \neq s, -s$. Then the function $F(x) = x^{2^s+1} + ax^{2^j(2^q+1)}$ with $a \in \mathbb{F}_{2^n}^*$ is EA inequivalent to power functions on $\mathbb{F}_{2^n}$ if one of the following conditions holds:*

1. $j \neq s, q, -s, -q, 2s, s+q, s-q$;
2. $j \neq s, q, -s, -q, s-q, -s-q, -2q$;
3. $j \neq 2s-q, s, -q, s-2q, s-q, q+s, 2s$;
4. $j \neq 2s-q, s, -q, s-2q, s-q, -s-q, -2q$.

Proof. Suppose the function $x^{2^s+1} + ax^{2^j(2^q+1)}$ is EA equivalent to x^{2^t+1} on $\mathbb{F}_{2^n}$ for some nonzero $t \in \mathbb{Z}/n\mathbb{Z}$. Then, there exist affine permutations L_1, L_2 and an affine function L' such that $L_1(x^{2^s+1}) + L_1(ax^{2^j(2^q+1)}) = (L_2(x))^{2^t+1} + L'(x)$. Expressing $L_1(x)$, $L_2(x)$ and $L'(x)$ as sums of linearized polynomials and constants and reducing the resulting exponents modulo $2^n - 1$ leads to an equation whose degree is at most $2^{n-1} + 2^{n-2}$ (since the 2-weights of the exponents are at most 2) and which has 2^n solutions. Hence the equation must be an identity.

Since the functions are quadratic, we can assume without loss of generality that L_1 and L_2 are linear: $L_1(x) = \sum_{m\in\mathbb{Z}/n\mathbb{Z}} b_m x^{2^m}$, $L_2(x) = \sum_{p\in\mathbb{Z}/n\mathbb{Z}} c_p x^{2^p}$. Then we get

$$\sum_{m\in\mathbb{Z}/n\mathbb{Z}} b_m x^{2^m(2^s+1)} + \sum_{m\in\mathbb{Z}/n\mathbb{Z}} b_m a^{2^m} x^{2^{m+j}(2^q+1)} = \sum_{l,p\in\mathbb{Z}/n\mathbb{Z}} c_p c_l^{2^t} x^{2^{l+t}+2^p} + L'(x). \tag{3}$$

On the left hand side of the identity (3) we have only items of the type $x^{2^m(2^s+1)}$, $x^{2^{m+j}(2^q+1)}$, with some coefficients. Therefore this must be true also for the right hand side of the identity.

We shall show that under some conditions on s, j, q, the equality above is satisfied only if $b_m = 0$ for every $m \in \mathbb{Z}/n\mathbb{Z}$. A contradiction.

If $b_m \neq 0$ for some m, then the coefficients of the items $x^{2^m(2^s+1)}$ and $x^{2^{m+j}(2^q+1)}$ are not zero on the left hand side of the identity (3) since $q \neq s, -s$. Hence this is also true for the right hand side of (3), that is,

$$c_m c_{m+s-t}^{2^t} \neq c_{m+s} c_{m-t}^{2^t}, \tag{4}$$

$$c_{m+j} c_{m+j+q-t}^{2^t} \neq c_{m+j+q} c_{m+j-t}^{2^t}. \tag{5}$$

The items of the type $x^{2^m+2^{m+j}}$ are missing in the left hand side of (3) when $j \neq s, q, -s, -q$. And we have no item of the kind $x^{2^{m+j}+2^{m+s}}$ in the left hand side of (3) when $j - s \neq s, q, -s, -q$, that is, $j \neq 2s, s+q, s-q$.

Thus, if these conditions are satisfied, then from the right hand side of (3) we get the following equalities with $c_m, c_{m+s-t}^{2^t}, c_{m+s}, c_{m-t}^{2^t}, c_{m+j}, c_{m+j-t}^{2^t}$:

$$c_m c_{m+j-t}^{2^t} = c_{m+j} c_{m-t}^{2^t}, \tag{6}$$

$$c_{m+j} c_{m+s-t}^{2^t} = c_{m+s} c_{m+j-t}^{2^t}. \tag{7}$$

Assume $c_{m+j-t}, c_{m+s-t} \neq 0$. If $c_{m-t} \neq 0$ then we get from (4), (6), (7):

$$c_m c_{m-t}^{-2^t} \neq c_{m+s} c_{m+s-t}^{-2^t},$$

$$c_m c_{m-t}^{-2^t} = c_{m+j} c_{m+j-t}^{-2^t},$$

$$c_{m+j} c_{m+j-t}^{-2^t} = c_{m+s} c_{m+s-t}^{-2^t},$$

and we come to a contradiction. If $c_{m-t} = 0$ then from (6) and since $c_{m+j-t} \neq 0$ we get $c_m = 0$. But $c_{m-t} = c_m = 0$ contradicts (4). Therefore, either c_{m+j-t} or c_{m+s-t} equals 0.

Assume first that $c_{m+j-t} = 0$. Then from (5) we get $c_{m+j} \neq 0$; then from (6), (7) we get $c_{m+s-t} = c_{m-t} = 0$, that is in contradiction with (4). Therefore, $c_{m+j-t} \neq 0$.

Assume now that $c_{m+s-t} = 0$. Then from (4) we get $c_{m+s} \neq 0$; then from (7) we get $c_{m+j-t} = 0$. Then from (5) we get $c_{m+j} \neq 0$ and we arrive to the contradiction $c_{m+s-t} = c_{m-t} = 0$ as above.

Therefore, if $j \neq s, q, -s, -q, 2s, s+q, s-q$ then F is EA inequivalent to quadratic power functions. Since F is quadratic and EA transformation does not change the degree of a function then F is EA inequivalent to any power function.

Using similar arguments we get below other conditions on s, q, j which are also sufficient.

We have no items of the kind $x^{2^{m+j+q}+2^m}$ in the left hand side of (3) when $j+q$ and $j+q-n$ are different from $s, q, n-s, n-q$, that is, $j \neq s-q, -s-q, -2q$. Thus, if $j \neq s, q, -s, -q, s-q, -s-q, -2q$ then we have the equality (6) and the items of the type $x^{2^{m+j+q}+2^m}$ are missing also in the right hand side of (3) and we get the following equality

$$c_m c_{m+j+q-t}^{2^t} = c_{m+j+q} c_{m-t}^{2^t}. \tag{8}$$

Let $c_{m+j+q-t}, c_{m+j-t} \neq 0$. If also $c_{m-1} \neq 0$ then we get from (5), (6), (8)

$$c_{m+j} c_{m+j-t}^{-2^t} \neq c_{m+j+q} c_{m+j+q-t}^{-2^t},$$

$$c_m c_{m-t}^{-2^t} = c_{m+j} c_{m+j-t}^{-2^t},$$

$$c_m c_{m-t}^{-2^t} = c_{m+j+q} c_{m+j+q-t}^{-2^t},$$

and we come to a contradiction. If $c_{m-t} = 0$ then it follows from (6) that $c_m = 0$. But $c_m = c_{m-t} = 0$ contradicts (4). Therefore, either $c_{m+j+q-t} = 0$ or $c_{m+j-t} = 0$.

If $c_{m+j-t} = 0$ then $c_{m+j}, c_{m+j+q-t} \neq 0$ by (5). Since $c_{m+j-t} = 0$ and $c_{m+j} \neq 0$ then it follows from (6) that $c_{m-t} = 0$. Since $c_{m+j+q-t} \neq 0$ and $c_{m-t} = 0$ then $c_m = 0$ by (8). But $c_{m-t} = c_m = 0$ contradicts (4).

If $c_{m+j+q-t} = 0$ then from (5) we get $c_{m+j+q}, c_{m+j-t} \neq 0$. Since $c_{m+j+q-t} = 0$ and $c_{m+j+q} \neq 0$ then $c_{m-t} = 0$ from (8). We have $c_m = 0$ from (6) since $c_{m+j-t} \neq 0$ and $c_{m-t} = 0$. But $c_m = c_{m-t} = 0$ contradicts (4).

Thus, if $j \neq s, q, -s, -q, s-q, -s-q, -2q$ then the function F is EA inequivalent to power functions.

The proofs of the third and the fourth claim of the theorem are similar. We have the following equality if $j \neq 2s-q, s, -q, s-2q$

$$c_{m+s}c^{2^t}_{m+j+q-t} = c_{m+j+q}c^{2^t}_{m+s-t}. \tag{9}$$

The equalities (7) and (9) lead to the condition $j \neq 2s-q, s, -q, s-2q, s-q, q+s, 2s$ which is sufficient for F to be EA inequivalent to power functions. The same is true when we consider the equalities (8) and (9) with the condition $j \neq 2s-q, s, -q, s-2q, s-q, -s-q, -2q$. $\square$

Theorem 3 *Let s and k be positive integers such that $k \geq 4$, $s \leq 3k-1$, $\gcd(k,3) = \gcd(s,3k) = 1$, and $i = sk \mod 3$, $t = 2i \mod 3$, $n = 3k$. Then the function $F(x) = x^{2^s+1} + ax^{2^{ik}+2^{tk+s}}$ with $a \in \mathbb{F}^*_{2^n}$ is EA inequivalent to power functions on $\mathbb{F}_{2^n}$.*

Proof. Let s and k be positive integers such that $k \geq 4$, $\gcd(k,3) = \gcd(s,3k) = 1$, and $i = sk \mod 3$, $t = 2i \mod 3$, $n = 3k$. Then the function $F(x) = x^{2^s+1} + ax^{2^{ik}+2^{tk+s}}$, $a \in \mathbb{F}^*_{2^n}$, satisfies the conditions of 1.) of Theorem 2. Indeed, if $i = 1$ then

$$2^{ik}+2^{tk+s} \mod (2^{3k}-1) = 2^k+2^{2k+s} \mod (2^{3k}-1) = \begin{cases} 2^k(2^{k+s}+1) & \text{if } s < k \\ 2^{s-k}(2^{2k-s}+1) & \text{if } k < s < 2k \\ 2^k(2^{s-2k}+1) & \text{if } s > 2k \end{cases}.$$

If $0 < s < k$ then in terms of Theorem 2 we have $j = k$, $q = k+s$. Obviously, $k \not\equiv s, q, -s, -q, s-q, q+s, 2s \equiv s, k+s, 3k-s, 2k-s, -k, k+2s, 2s, 2s-3k, 2s-2k, 2k \mod n$ since $k \geq 4$ and $\gcd(k,3) = \gcd(s,3k) = 1$.
If $k < s < 2k$ then $j = s-k$, $q = 2k-s$ and $s-k \not\equiv s, q, -s, -q, s-q, q+s, 2s \mod n$.
If $s > 2k$ then $j = k$, $q = s-2k$ and $k \not\equiv s, q, -s, -q, s-q, q+s, 2s \mod n$.

In case $i = 2$ we have

$$2^{ik}+2^{tk+s} \mod (2^{3k}-1) = 2^{2k}+2^{k+s} \mod (2^{3k}-1) = \begin{cases} 2^{k+s}(2^{k-s}+1) & \text{if } s < k \\ 2^{2k}(2^{s-k}+1) & \text{if } k < s < 2k \\ 2^{s-2k}(2^{4k-s}+1) & \text{if } 2k < s \end{cases}.$$

If $s < k$ then $j = k+s$, $q = k-s$ and using the conditions $k \geq 4$ and $\gcd(k,3) = \gcd(s,3k) = 1$ we get $k+s \not\equiv s, q, -s, -q, s-q, q+s, 2s \mod n$.

If $k < s < 2k$ then $j = 2k$, $q = s - k$ and $2k \not\equiv s, q, -s, -q, s - q, q + s, 2s \mod n$.
If $s > 2k$ then $j = s - 2k$, $q = 4k - s$ and $s - 2k \not\equiv s, q, -s, -q, s - q, q + s, 2s \mod n$.

Obviously, in all cases the condition $q \not\equiv s, -s \mod n$ is satisfied. Hence, the function F is EA inequivalent to power functions by Theorem 2. $\square$

Corollary 2 *Let s and k be positive integers such that $s \leq 3k-1$, $\gcd(k, 3) = \gcd(s, 3k) = 1$, and $i = sk \mod 3$, $t = 2i \mod 3$, $n = 3k$. If $a \in \mathbb{F}_{2^n}$ has the order $2^{2k} + 2^k + 1$ then the function $F(x) = x^{2^s+1} + ax^{2^{ik}+2^{tk+s}}$ is AB on $\mathbb{F}_{2^n}$ when n is odd and APN when n is even and it is EA inequivalent to power mappings.*

In a next version of the present paper, we shall show that, except in particular cases, the new APN functions introduced here are not CCZ-equivalent to the Gold functions nor to the Kasami functions.

5 Conclusion

We have introduced an infinite class of APN (and AB if n is odd) quadratic functions which we conjecture CCZ-inequivalent to power functions, and therefore, new, up to CCZ-equivalence. In the next version of this paper we will show that they are CCZ-inequivalent to Gold and Kasami functions. This implies that, for $n = 12$, they are indeed CCZ-inequivalent to power functions. We leave two open problems:
- proving that the functions introduced in the present paper are CCZ-inequivalent to power functions for every $n \geq 12$;
- finding classes of non-quadratic APN functions which would be CCZ-inequivalent to all known APN functions (or even, CCZ-inequivalent to power functions).

References

[1] T. Bending, D. Fon-Der-Flaass. Crooked functions, bent functions and distance-regular graphs. *Electron. J. Comb.*, 5(R34), 14, 1998.

[2] T. Berger, A. Canteaut, P. Charpin and Y. Laigle-Chapuy. On almost perfect nonlinear mappings over F_2^n. Proceedings of International Symposium on Information Theory ISIT 2005.

[3] 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.

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

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

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

[7] 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.

[8] 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.

[9] C. Carlet. Boolean Functions for Cryptography and Error Correcting Codes. Chapter of the monography *Boolean Methods and Models*, Y. Crama and P. Hammer eds, Cambridge University Press, to appear (winter 2005-2006).

[10] C. Carlet. Vectorial Boolean Functions for Cryptography. Chapter of the monography *Boolean Methods and Models*, Y. Crama and P. Hammer eds, Cambridge University Press, to appear (winter 2005-2006).

[11] 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.

[12] C. Carlet and C. Ding. Highly Nonlinear Mappings. *Special Issue "Complexity Issues in Coding and Cryptography", dedicated to Prof. Harald Niederreiter on the occasion of his 60th birthday, Journal of Complexity* 20, pp. 205-244, 2004.

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

[14] N. Courtois and J. Pieprzyk. Cryptanalysis of block ciphers with overdefined systems of equations. *Advances in cryptology–ASIACRYPT 2002, Lecture Notes in Computer Science* 2501, pp. 267-287, Springer, 2003.

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

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

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

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

[19] 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.

[20] H. Dobbertin, Uniformly representable permutation polynomials, T. Helleseth, P.V. Kumar and K. Yang eds. *in the Proceedings of "Sequences and their applications–SETA '01"*, Springer Verlag, London, 2002, 1-22.

[21] Y. Edel, G. Kyureghyan and A. Pott. A new APN function which is not equivalent to a power mapping. Preprint, 2005, http://arxiv.org/abs/math.CO/0506420

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

[23] T.Helleseth and D. Sandberg. Some power mappings with low differential uniformity. *Applic. Alg. Eng., Commun. Comput.*, vol.8, pp. 363-370, 1997.

[24] 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.

[25] 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, Lecture Notes in Computer Science*, vol. 673, Berlin, Springer-Verlag, pp. 180-194, 1993.

[26] 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.

[27] 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.

[28] M. Matsui. Linear cryptanalysis method for DES cipher. *Advances in Cryptology-EUROCRYPT'93, Lecture Notes in Computer Science*, Springer-Verlag, pp. 386-397, 1994.

[29] K. Nyberg. On the construction of highly nonlinear permutations. *Advances in Cryptography, EUROCRYPT'92, Lecture Notes in Computer Science*, Springer-Verlag, 658, pp. 92-98, 1993.

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

[31] K. Nyberg. S-boxes and Round Functions with Controllable Linearity and Differential Uniformity. *Proceedings of Fast Software Encryption 1994, Lecture Notes in Computer Science* 1008, pp. 111-130, 1995.

[32] A. Pott. Nonlinear functions in Abelian groups and relative difference sets. *Discrete Applied Math.* 138, pp. 177-193, 2004.

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

[34] H. M. Trachtenberg. On the cross-correlation functions of maximal linear recurring sequences. PhD Thesis, University of Southern California, 1970.