Another class of quadratic APN binomials over $\mathbb{F}_{2^n}$: the case n divisible by 4

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

Abstract

We exhibit an infinite class of almost perfect nonlinear quadratic binomials from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ with $n = 4k$ and k odd. We prove that these functions are CCZ-inequivalent to known APN power functions when $k \neq 1$. In particular it means that for $n = 12, 20, 28$, they are CCZ-inequivalent to any power function.

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 almost perfect nonlinear (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 solutions (it is also called differentially 2-uniform). Vectorial Boolean functions used as S-boxes in block ciphers must have low differential uniformity to prevent from the differential cryptanalysis (see [4, 31]). In this sense APN functions are optimal. The notion of APN function is closely connected to the notion of almost bent (AB) function. A function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is called AB if the minimum Hamming distance between all Boolean functions $v \cdot F$, $v \in \mathbb{F}_2^n \setminus \{0\}$ (where "$\cdot$" denotes the usual inner product in $\mathbb{F}_2^n$, note that any other choice of an inner product would lead to the same notion) and all affine Boolean functions on $\mathbb{F}_2^n$ is maximal (this distance is called the nonlinearity of F and this maximum equals $2^{n-1} - 2^{\frac{n-1}{2}}$). AB functions oppose an optimum resistance to the linear cryptanalysis (see [30, 15]). Besides, every AB function is APN [15], and in case n odd any quadratic function is APN if and only if it is AB [14].

Until recently the only known constructions of APN and AB functions were EA-equivalent to power functions over finite fields. Recall that functions F and F' are called extended affine equivalent (EA-equivalent) if $F' = A_1 \circ F \circ A_2 + A$, where the mappings

[*]Department of Mathematics, University of Trento, I-38050 Povo (Trento), ITALY; e-mail: lilia.b@mail.ru

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

[‡]GRIM, University Toulon, BP 132, 83957 La Garde Cedex, FRANCE; e-mail: Gregor.Leander@rub.de

A, A_1, A_2 are affine, and where A_1, A_2 are permutations. 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 [11, 12, 24, 26, 28, 31]).

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

Functions	Exponents d	Conditions	Proven in
Gold	$2^i + 1$	$\gcd(i, n) = 1$	[24, 31]
Kasami	$2^{2i} - 2^i + 1$	$\gcd(i, n) = 1$	[27, 28]
Welch	$2^t + 3$	$n = 2t + 1$	[20]
Niho	$2^t + 2^{\frac{t}{2}} - 1$, t even $2^t + 2^{\frac{3t+1}{2}} - 1$, t odd	$n = 2t + 1$	[19]
Inverse	$2^{2t} - 1$	$n = 2t + 1$	[3, 31]
Dobbertin	$2^{4t} + 2^{3t} + 2^{2t} + 2^t - 1$	$n = 5t$	[21]

When using S-boxes EA-equivalent to power functions the advantage is the low implementation complexity in hardware environments. On the other hand the properties of power functions could be exploited in an attack (see [1]). A first well known property of a power permutation F is that all its component functions $\mathrm{tr}(cF)$, $c \in \mathbb{F}_{2^n}^*$, are affine equivalent. A second consequence is that the rich algebraic structure of the field $\mathbb{F}_{2^n}$ can be extensively used, probably in a simpler manner for a power function than for a polynomial with many terms. The impact of the choice of power functions on algebraic attacks is another open question [16]. Probably, some of the potential weaknesses of S-boxes based on power functions can be avoided by using S-boxes EA-inequivalent or even CCZ-inequivalent (see below) to power mappings.

Applying the stability properties studied in [14] and more recently called CCZ-equivalence (cf. definition at Section 2), classes of APN functions EA-inequivalent to power functions are constructed in [8, 9]. They are presented in Table 2. When n is odd these functions are also AB. However they are, by construction, CCZ-equivalent to Gold mappings.

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

Functions	Conditions	Alg. degree
$x^{2^i+1} + (x^{2^i} + x + \mathrm{tr}(1) + 1)\,\mathrm{tr}(x^{2^i+1} + x\,\mathrm{tr}(1))$	$n \geq 4$ $\gcd(i, n) = 1$	3
$[x + \mathrm{tr}_{n/3}(x^{2(2^i+1)} + x^{4(2^i+1)}) + \mathrm{tr}(x)\,\mathrm{tr}_{n/3}(x^{2^i+1} + x^{2^{2i}(2^i+1)})]^{2^i+1}$	n divisible by 6 $\gcd(i, n) = 1$	4
$x^{2^i+1} + \mathrm{tr}_{n/m}(x^{2^i+1}) + x^{2^i}\,\mathrm{tr}_{n/m}(x) + x\ \mathrm{tr}_{n/m}(x)^{2^i}$ $+[\mathrm{tr}_{n/m}(x)^{2^i+1} + \mathrm{tr}_{n/m}(x^{2^i+1}) + \mathrm{tr}_{n/m}(x)]^{\frac{1}{2^i+1}}(x^{2^i} + \mathrm{tr}_{n/m}(x)^{2^i} + 1)$ $+[\mathrm{tr}_{n/m}(x)^{2^i+1} + \mathrm{tr}_{n/m}(x^{2^i+1}) + \mathrm{tr}_{n/m}(x)]^{\frac{2^i}{2^i+1}}(x + \mathrm{tr}_{n/m}(x))$	$m \neq n$ n odd n divisible by m $\gcd(i, n) = 1$	$m + 2$

The first examples of APN functions CCZ-inequivalent to power mappings are introduced in [23]. These are two quadratic binomials:

- $x^3 + wx^{36}$ over $\mathbb{F}_{2^{10}}$, where w has the order 3 or 93,
- $x^3 + wx^{528}$ over $\mathbb{F}_{2^{12}}$, where w has the order 273 or 585.

The second of these two functions has been proven being part of an infinite sequence of quadratic APN binomials given in Table 3 (see [6, 7]) while the first function from [23] is not explained yet by any infinite family.

Table 3
Known APN functions CCZ-inequivalent to power functions on $\mathbb{F}_{2^n}$.

	Functions	Conditions	Proven in
The case n divisible by 3	$x^{2^s+1} + wx^{2^{ik}+2^{mk+s}}$	$n = 3k$, $\gcd(k, 3) = \gcd(s, 3k) = 1$ $k \geq 4$, $i = sk \mod 3$, $m = 3 - i$ w has the order $2^{2k} + 2^k + 1$	[6, 7]
The case n divisible by 4	$x^{2^s+1} + wx^{2^{ik}+2^{mk+s}}$	$n = 4k$, $\gcd(k, 2) = \gcd(s, 2k) = 1$ $k \geq 3$, $i = sk \mod 4$, $m = 4 - i$ w has the order $2^{3k} + 2^{2k} + 2^k + 1$	Theorem 1 of the present paper

The class of functions from Table 3 which corresponds to the case n divisible by 3 is constructed in [6, 7]. It is proven that these functions are APN for n even and in case n odd they are AB permutations [6, 7]. Until now this case has been the only known class of APN functions CCZ-inequivalent to power mappings. The present paper introduces a new infinite family of quadratic APN binomials which corresponds to the case n divisible by 4 in Table 3. It is proven (in [6] for n divisible by 3 and in the present paper for n divisible by 4) that all these functions are EA-inequivalent to power functions and CCZ-inequivalent to the Gold and Kasami mappings. This implies that for n even they are CCZ-inequivalent to all known APN functions, and for $n = 12, 15, 20, 24, 28$ they are CCZ-inequivalent to any power mappings. We conjecture CCZ-inequivalence of these functions to any power functions for all $n \geq 12$.

Though quadratic APN functions are used in some Feistel ciphers (see for instance [34, 35]) functions of low algebraic degree are not the best choices for S-boxes (see [5]). However, the APN functions from Table 3 can be viewed as the first necessary steps to construct maximum nonlinear S-boxes of a larger algebraic degree CCZ-inequivalent to power functions. Note that, applying CCZ-equivalence to quadratic APN functions it is possible to construct nonquadratic APN mappings CCZ-inequivalent to power functions. The existence of APN functions CCZ-inequivalent to power functions and to quadratic functions is still an open problem.

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 $\mathbb{F}_{2^n}$ 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, $0 \le k \le 2^n - 1$, 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, $d^\circ(F) = \max_{0 \le i \le n-1, c_i \neq 0} w_2(i)$ (see [14]).

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* 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 $\{(x, F(x)) \mid x \in \mathbb{F}_{2^n}\}$ and $\{(x, F'(x)) \mid x \in \mathbb{F}_{2^n}\}$ 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 [6]). As shown in [14], 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

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

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 $\max_{a\in\mathbb{F}_{2^n}^*, b\in\mathbb{F}_{2^n}} \delta_F(a,b) \leq \delta$. 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 $tr(x) = x + x^2 + x^4 + ... + x^{2^{n-1}}$ 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

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

([15, 33]) and in case of equality F is called *almost bent* or *maximum nonlinear.*

It is shown in [14] that, if F and G are CCZ-equivalent, then F is APN (resp. AB) if and only if G is APN (resp. AB). More general, CCZ-equivalent functions have the same differential uniformity and the same extended Walsh spectrum (see [8]).

Obviously, AB functions exist only for n odd. It is proven in [15] 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 [14], but this is not true for nonquadratic cases: the Dobbertin and the inverse APN functions are not AB (see [12, 14]). When n is even, the inverse function x^{2^n-2} is a differentially 4-uniform permutation [31] and has the best known nonlinearity [29], that is $2^{n-1} - 2^{\frac{n}{2}}$ (see [12, 18]). This function has been chosen as the basic S-box, with $n = 8$, in the Advanced Encryption Standard (AES), see [17]. A comprehensive survey on APN and AB functions can be found in [13].

3 A new family of APN functions

Theorem 1 *Let s and k be positive integers such that $s \leq 4k-1$, $\gcd(k,2) = \gcd(s,2k) = 1$, and $i = sk \mod 4$, $m = 4-i$, $n = 4k$. If $w \in \mathbb{F}_{2^n}^*$ has the order $2^{3k}+2^{2k}+2^k+1$ then the function $F(x) = x^{2^s+1} + wx^{2^{ik}+2^{mk+s}}$ is APN on $\mathbb{F}_{2^n}$.*

Proof. Since w has the order $2^{3k}+2^{2k}+2^k+1$ then $w = \alpha^{2^k-1}$ for some primitive element α of $\mathbb{F}_{2^n}^*$. We have to show that for every $u,v \in \mathbb{F}_{2^n}$, $u \neq 0$, the equation

$$F(x) + F(x+u) = v \tag{1}$$

has at most 2 solutions. We have

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

As this is a linear equation in x it is sufficient to study the kernel. To simplify notation we denote

$$
a=\alpha^{2^k-1}u^{2^{ik}+2^{mk+s}-2^s-1}.
$$

After replacing x by ux and dividing by u^{2^s+1}, we see the equation (1) admits 0 or 2 solutions for every $u\in\mathbb{F}_{2^n}^*$ if and only if, denoting

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

the equation $\Delta_a(x)=0$ has the only solutions 0 and 1.

From now on we consider the cases $i=1$ and $i=3$ separately.

Case 1 $(i=3, m=1)$**:** If we denote $y=x^{2^k}$, $z=y^{2^k}$, $t=z^{2^k}$ and $b=a^{2^k}$, $c=b^{2^k}$, $d=c^{2^k}$ the equation $\Delta_a(x)=0$ can be rewritten as

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

Since $2^{ik}+2^{mk+s}-2^s-1=2^{3k}+2^{k+s}-2^s-1=(2^k-1)(2^{2k}+2^k+2^s+1)$ then the element a is always a (2^k-1)-th power and thus $abcd=1$. Considering also the conjugated equations we derive the following system of equations

$$
\begin{array}{lllll}
f_1= & \Delta_a(x) & =a(t+y^{2^s})+x^{2^s}+x & =0 \\
f_2= & f_1^{2^k} & =b(x+z^{2^s})+y^{2^s}+y & =0 \\
f_3= & f_2^{2^k} & =c(y+t^{2^s})+z^{2^s}+z & =0 \\
f_4= & abcf_3^{2^k} & =z+x^{2^s}+abc(t^{2^s}+t) & =0.
\end{array}
$$

The aim is now to eliminate y, z and t from these equations to get an equation in x only. First we compute

$$
\begin{aligned}
R_1 &= bcf_1+abcf_2+abf_3+f_4 \\
&= ab(bc+1)z^{2^s}+(ab+1)z+(bc+1)x^{2^s}+bc(ab+1)x
\end{aligned}
$$

and

$$
\begin{aligned}
R_2 &= cf_1^{2^s}+a^{2^s}c(f_2^{2^s}+f_2)+a^{2^s}f_3 \\
&= a^{2^s}b^{2^s}cz^{2^{2s}}+a^{2^s}(bc+1)z^{2^s}+a^{2^s}z+cx^{2^{2s}}+c(ab+1)^{2^s}x^{2^s}+a^{2^s}bcx
\end{aligned}
$$

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

$$\begin{aligned} R_3 &= cR_1^{2^s} + (bc+1)^{2^s} R_2 \\ &= (c(ab+1)^{2^s} + a^{2^s}(bc+1)^{2^s+1})z^{2^s} + a^{2^s}(bc+1)^{2^s} z + c(ab+1)^{2^s} x^{2^s} + a^{2^s} bc(bc+1)^{2^s} x. \end{aligned}$$

Using equations R_1 and R_3 we can eliminate z^{2^s} by computing

$$\begin{aligned} R_4 &= ab(bc+1)R_3 + (c(ab+1)^{2^s} + a^{2^s}(bc+1)^{2^s+1})R_1 \\ &= P(a)(z + (bc+1)x^{2^s} + bcx), \end{aligned}$$

where

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

Below we shall show that $P(a) \neq 0$, thus we can denote

$$R_5 = \frac{R_4}{P(a)} = z + (bc+1)x^{2^s} + bcx.$$

Computing

$$\begin{aligned} R_6 &= R_1 + ab(bc+1)R_5^{2^s} \\ &= (ab+1)z + ab(bc+1)^{2^s+1}x^{2^{2s}} + (ab^{2^s+1}c^{2^s}+1)(bc+1)x^{2^s} + bc(ab+1)x \end{aligned}$$

we finally get our desired equation

$$\begin{aligned} R_7 &= (ab+1)R_5 + R_6 \\ &= ab(bc+1)^{2^s+1}\left(x^{2^{2s}} + x^{2^s}\right). \end{aligned}$$

Obviously if x is a solution of $\Delta_a(x) = 0$ then $R_7(x) = 0$. For $P(a) \neq 0$ and $bc+1 \neq 0$ this is equivalent to $x = 0, 1$. Thus to prove the theorem we have to show that $P(a)$ and $bc+1$ do not vanish for elements a fulfilling the equation

$$a = \alpha^{2^k-1} u^{2^{3k}+2^{k+s}-2^s-1}. \tag{2}$$

Assume $bc = 1$, that is, $a^{2^{2k}+2^k} = 1$ or equivalently $a^{2^k+1} = 1$. We have

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

because

$$(2^{3k} + 2^{k+s} - 2^s - 1)(2^k+1) \equiv (2^{2k}-1)(2^k+2^s) \bmod (2^{4k}-1).$$

Since $a^{2^k+1} = 1$ then $\alpha u^{2^k+2^s}$ should be $(2^{2k}+1)$-th power of an element of the field. We have

$$2^k + 2^s = 2^s(2^{k-s}+1) = 2^s(2^{2p}+1)$$

with some p odd. Indeed, $ks \mod 4 = 3$, then

$$k \mod 4 \neq s \mod 4$$

for odd k, s, and $k - s = 2p$ for some p odd.

Numbers $2^{2p} + 1$ and $2^{2k} + 1$ are divisible by 5 because p, k are odd. We get that $u^{2^k+2^s}$ is fifth power of an element of the field and $\alpha u^{2^k+2^s}$ is not (since α is a primitive element). Therefore $\alpha u^{2^k+2^s}$ is not $(2^{2k} + 1)$-th power of an element of the field. A contradiction.

Let $c(ab + 1)^{2^s+1} + a^{2^s}(bc + 1)^{2^s+1} = 0$. Since $bc + 1 \neq 0$ then $ab + 1 \neq 0$ and we get

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

Note that since n is even and s is odd then $2^n - 1$ and $2^s + 1$ are divisible by 3. Therefore c/a^{2^s} is third power of an element of the field. We have

$$c/a^{2^s} = a^{2^{2k}-2^s} = a^{2^s(2^{2k-s}-1)}$$

and

$$2^{3k} + 2^{k+s} - 2^s - 1 = 2^s(2^{3k-s} - 1) + (2^{k+s} - 1).$$

The numbers $2^{3k-s} - 1$ and $2^{k+s} - 1$ are divisible by 3 since $3k - s$ and $k + s$ are even. On the other hand $2^k - 1$ and $2^{2k-s} - 1$ are not divisible by 3 since k and $2k - s$ are odd. We get

$$a^{2^s(2^{2k-s}-1)} = \alpha^{2^s(2^{2k-s}-1)(2^k-1)} u^{2^s(2^{2k-s}-1)(2^{3k}+2^{k+s}-2^s-1)}.$$

Obviously c/a^{2^s} is not third power of an element of the field and therefore it is not (2^s+1)-th power. A contradiction.

Case 2 ($i = 1, m = 3$)**:** Since $2^{ik} + 2^{mk+s} - 2^s - 1 = 2^k + 2^{3k+s} - 2^s - 1 = (2^k - 1)(1 + 2^{2k+s} + 2^{k+s} + 2^s)$ then a is always a $(2^k - 1)$-th power and thus again $abcd = 1$.

In this case the equation $\Delta_a(x) = 0$ can be transformed into the following system of equations

$$\begin{aligned} f_1 = &\quad a(y + t^{2^s}) + x^{2^s} + x = &\quad 0 \\ f_2 = &\quad b(z + x^{2^s}) + y^{2^s} + y = &\quad 0 \\ f_3 = &\quad c(t + y^{2^s}) + z^{2^s} + z = &\quad 0 \\ f_4 = &\quad x + z^{2^s} + abc(t^{2^s} + t) = &\quad 0. \end{aligned}$$

We get

$$\begin{aligned}
R_1 &= bcf_1 + abcf_2 + abf_3 + f_4 \\
&= (ab+1)z^{2^s} + ab(bc+1)z + bc(ab+1)x^{2^s} + (bc+1)x, \\
R_2 &= c^{2^s} f_1 + ac^{2^s}(f_2^{2^s} + f_2) + af_3^{2^s} \\
&= az^{2^{2s}} + a(bc+1)^{2^s} z^{2^s} + abc^{2^s} z + ab^{2^s} c^{2^s} x^{2^{2s}} + c^{2^s}(ab+1)x^{2^s} + c^{2^s} x, \\
R_3 &= aR_1^{2^s} + (ab+1)^{2^s} R_2 \\
&= a(bc+1)^{2^s} z^{2^s} + abc^{2^s}(ab+1)^{2^s} z + (a(bc+1)^{2^s} + c^{2^s}(ab+1)^{2^s+1})x^{2^s} + c^{2^s}(ab+1)^{2^s} x, \\
R_4 &= (ab+1)R_3 + a(bc+1)^{2^s})R_1 \\
&= P(a)(abz + (ab+1)x^{2^s} + x),
\end{aligned}$$

where

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

Assuming that $P(a) \neq 0$ we continue

$$\begin{aligned}
R_5 &= \frac{R_4}{P(a)} = abz + (ab+1)x^{2^s} + x, \\
R_6 &= a^{2^s} b^{2^s} R_1 + (ab+1)R_5^{2^s} \\
&= a^{2^s+1} b^{2^s+1}(bc+1)z + (ab+1)^{2^s+1} x^{2^{2s}} + (a^{2^s} b^{2^s+1} c + 1)(ab+1)x^{2^s} + a^{2^s} b^{2^s}(bc+1)x, \\
R_7 &= a^{2^s} b^{2^s}(bc+1)R_5 + R_6 \\
&= (ab+1)^{2^s+1}\left(x^{2^{2s}} + x^{2^s}\right).
\end{aligned}$$

We see now that the equation $\Delta_a(x) = 0$ has the only solutions 0 and 1 if $P(a) \neq 0$ and $ab+1 \neq 0$.

Assume that $ab = 1$, that is, $a^{2^k+1} = 1$. We have

$$(2^k + 2^{3k+s} - 2^s - 1)(2^k + 1) \equiv (2^{2k} - 1)(2^{k+s} + 1) \bmod (2^{4k} - 1)$$

and

$$a^{2^k+1} = \left(\alpha^{2^k-1} u^{2^k + 2^{3k+s} - 2^s - 1}\right)^{2^k+1} = \left(\alpha u^{2^{k+s}+1}\right)^{2^{2k}-1}.$$

Because $a^{2^k+1} = 1$, the element $\alpha u^{2^{k+s}+1}$ should be $(2^{2k}+1)$-th power of an element of the field. Since $ks \mod 4 = 1$ then $k \mod 4 = s \mod 4$ and $2^{k+s} + 1 = 2^{2p} + 1$ for some p odd. Thus $2^{k+s} + 1$ and $2^{2k} + 1$ are divisible by 5. Therefore $\alpha u^{2^{k+s}+1}$ is not fifth power of an element of the field and then it is not $(2^{2k}+1)$-th power. A contradiction.

Let $c^{2^s}(ab+1)^{2^s+1} + a(bc+1)^{2^s+1} = 0$. Since $ab+1 \neq 0$ then

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

We show that the element $c^{2^s}/a = a^{2^{2k+s}-1}$ is not third power of an element of the field. A contradiction.

Indeed, for n even and s odd the numbers 2^s+1 and 2^n-1 are divisible by 3. On the other hand

$$a^{2^{2k+s}-1} = \left(\alpha^{2^k-1}u^{2^k+2^{3k+s}-2^s-1}\right)^{2^{2k+s}-1} = \alpha^{(2^k-1)(2^{2k+s}-1)}u^{(2^k+2^{3k+s}-2^s-1)(2^{2k+s}-1)}$$

and

$$2^k+2^{3k+s}-2^s-1 = 2^s(2^{k-s}-1)+(2^{3k+s}-1).$$

Since $2^{k-s}-1$ and $2^{3k+s}-1$ are divisible by 3 then $u^{(2^k+2^{3k+s}-2^s-1)(2^{2k+s}-1)}$ is third power of an element of the field. The number $(2^k-1)(2^{2k+s}-1)$ is not divisible by 3 because k and $2k+s$ are odd. Therefore, $a^{2^{2k+s}-1}$ is not third power of an element of the field. $\square$

4 On CCZ-inequivalence of the introduced APN functions to power functions

To prove CCZ-inequivalence of APN functions of Theorem 1 to the Gold and Kasami functions we use results from [6].

Theorem 2 ([6]) *Let n be a positive integer and let s,j,q be three nonzero elements of $\mathbb{Z}/n\mathbb{Z}$ such that $q\neq\pm s$, $j\neq\pm s,\pm q,2s,s\pm q$. 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 $\mathbb{F}_{2^n}$.*

Theorem 3 ([6]) *Let n be a positive integer and r,s,q be three nonzero elements of $\mathbb{Z}/n\mathbb{Z}$ and j an element of $\mathbb{Z}/n\mathbb{Z}$ such that $s\neq\pm q$, $j\neq s-r$, $j\neq -r$, $j+q\neq s-r$, $j+q\neq -r$. If for $a\in\mathbb{F}_{2^n}^*$ the function $F(x)=x^{2^s+1}+ax^{2^j(2^q+1)}$ is APN on $\mathbb{F}_{2^n}$ and it is CCZ-equivalent to the function $G(x)=x^{2^r+1}$ then F and G are EA-equivalent.*

Theorem 4 ([6]) *Let n be a positive integer and r,s,q,j be nonzero elements of $\mathbb{Z}/n\mathbb{Z}$ such that $\gcd(r,n)=1$, $n>4$, $s\neq\pm q$, $s\neq\pm 3q$, $q\neq\pm 3s$, $s\neq\pm j$, $q\neq\pm j$, $3q+j\neq 0$, $j+q\neq\pm s$, $j\neq s+q$, $2q\neq\pm j$, $2q\neq s-j$, $2s\neq j$, $2s\neq j+q$. Then for $a\in\mathbb{F}_{2^n}^*$ the functions $F(x)=x^{2^s+1}+ax^{2^j(2^q+1)}$ and $K(x)=x^{4^r-2^r+1}$ are CCZ-inequivalent on $\mathbb{F}_{2^n}$.*

Proposition 1 *The function F of Theorem 1 is EA-inequivalent to power functions when $k\geq 3$.*

Proof. The function F satisfies the conditions of Theorem 2. If $i=1$ then $j=k$ and $q=2k+s$. The conditions $q\neq\pm s$, $j\neq\pm s,\pm q,\pm 2s,s\pm q$ are satisfied when $k\geq 3$ because k,s are odd, $n=4k$, $\gcd(s,4k)=1$. The same is with the case $i=3$. $\square$

Proposition 2 *The function F of Theorem 1 is CCZ-inequivalent to the Gold mappings when $k\geq 3$.*

Proof. The proof is based on Proposition 1 and Theorem 3. Let $i = 1$, then $j = k$ and $q = 2k + s$ satisfy the conditions $q \neq \pm s, j \neq s - r, j \neq -r, j + q \neq s - r, j + q \neq -r$ for any r satisfying $1 \leq r < n/2$ and $\gcd(r, n) = 1$. Indeed, $q = \pm s$ is in contradiction with $\gcd(s, 4k) = 1$, $n = 4k$. If $k = s - r$ then it contradicts to the fact that k is odd and $s - r$ is even. If $k = -r$ then it would contradict to $\gcd(r, 4k) = 1$. If $3k + s = s - r$ then $3k = -r$ and $\gcd(r, k) \neq 1$, a contradiction. If $3k + s = -r$ then $s + r = k$ while s, r, k are odd. By Theorem 3 and Proposition 1 the function F is CCZ-inequivalent to x^{2^r+1}. For the case $i = 3$ the proof is similar. $\square$

Proposition 3 *The function F of Theorem 1 is CCZ-inequivalent to the Kasami mappings when $k \geq 3$.*

Proof. Obviously, when $k \geq 3$ the function F satisfies the conditions of Theorem 4 because k, s are odd, $n = 4k$, $\gcd(s, 4k) = 1$. $\square$

If n is even then for any quadratic APN mapping F the number $2^{n/2}$ divides all the values in the Walsh spectrum of F (see [32]). Besides, it is proven in [11] that $2^{\frac{2n}{5}+1}$ cannot be a divisor of all the values in the Walsh spectrum of the Dobbertin function. Since the extended Walsh spectrum of a function is invariant under CCZ-equivalence then we can make the following conclusion from Propositions 1-3.

Corollary 1 *The function F of Theorem 1 is CCZ-inequivalent to all known power APN functions when $k \geq 3$.*

For $n = 12, 20, 28$ Corollary 1 implies that the introduced APN binomials are CCZ-inequivalent to all power functions. When $n \geq 20$ and n is not divisible by 3 then the function F is CCZ-inequivalent to all known APN functions.

Problem 1 *Construct APN polynomials CCZ-inequivalent to power functions and to quadratic functions.*

References

[1] *AES Security Report.* C. Cid and H. Gilbert eds., http://www.ecrypt.eu.org/documents/D.STVL.2-1.0.pdf, 2006.

[2] 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.

[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] A. Biryukov, C. De Canniere. Block Ciphers and Systems of Quadratic Equations. *Proceedings of Fast Software Encryption 2003, Lecture Notes in Computer Science* 2887, pp. 274-289, 2003.

[6] L. Budaghyan, C. Carlet, G. Leander. A class of quadratic APN binomials inequivalent to power functions, submitted.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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

[14] 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.

[15] 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.

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

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

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

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

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

[21] 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.

[22] 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.

[23] 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.

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

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

[26] 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.

[27] 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.

[28] 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.

[29] 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.

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

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

[32] 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.

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

[34] E. Takeda. Misty1. *Submission to NESSIE*, Sept. 2000. http://www.cryptonessie.org/workshop/submissions.html

[35] *Third Generation Partnership Project.* 3GPP KASUMI evaluation report. Tech. rep., *Security Algorithms Group of Experts (SAGE)*, 2001. http://www.3gpp.org/TB/other/algorithms/KASUMI_Eval_rep_v20.pdf