On equivalence between some families of APN functions

Lilya Budaghyan, Marco Calderini, and Irene Villa

Department of informatics, University of Bergen
{lilya.budaghyan, marco.calderini, irene.villa}@uib.no

Abstract. We prove that two families among the known APN polynomial functions are equivalent to the hexanomials family introduced by Budaghyan and Carlet in 2008. By that we reduce the list of known families of APN functions to those strictly inequivalent to each other.

Keywords: CCZ-equivalence, EA-equivalence, APN, Boolean functions

1 Introduction

Let n and m be two positive integers, an (n, m)-function, or vectorial Boolean function, is a function F from the finite field $\mathbb{F}_{2^n}$ with 2^n elements to the finite field $\mathbb{F}_{2^m}$ with 2^m elements. When $m = 1$ such functions are simply called Boolean functions. Boolean functions and vectorial Boolean functions have been intensively studied due to the large number of applications both in mathematics and computer science. In particular, they have a crucial role in the design of secure cryptographic primitives, such as block ciphers. In this context, vectorial Boolean functions are also called S-boxes.

The differential attack, introduced by Biham and Shamir [1], is among the most efficient attacks on block cipher. To measure the resistance of an S-box to this attack, in [15], Nyberg introduced the notion of *differential uniformity*. A vectorial Boolean function F is called differentially δ-uniform if the equation $F(x) + F(x + a) = b$ has at most δ solutions for any non-zero a and for all b. The smallest possible values for δ is 2, and functions achieving such differential uniformity are called *almost perfect nonlinear* (APN).

Boolean function used in cryptography must have low differential uniformity. For this reason, functions with low differential uniformity, and in particular APN functions are an important domain of research for symmetric cryptography.

The differential uniformity, and thus the APN property, is preserved by some transformations of functions, which define equivalence relations between vectorial Boolean functions. Two of these equivalence notions are, the extended affine equivalence (EA-equivalence) and Carlet-Charpin-Zinoviev equivalence (CCZ-equivalence). EA-equivalence is a particular case of CCZ-equivalence, which is the more general known equivalence relation preserving the differential uniformity.

An important aspect of the study and the analysis of APN functions, and vectorial Boolean functions in general, is their classification with respect to these equivalence relations. Classifications of APN functions is a hard problem and a complete classification is only known for $n \leq 5$ [5]. There are only few infinite classes of APN functions known and among them six are power functions. In recent years, some newly constructed families of APN polynomials have not been checked for equivalence to already known classes.

In this work we reduce the list of known families of polynomial APN functions by excluding all equivalent cases. Indeed, we show that the class of trinomial APN functions introduced in [7] and the class of multinomials studied in [2] are equivalent. Finally we show that both these classes can be reduced to the hexanomials introduced in [7]. According to the table of all CCZ-inequivalent functions which arise from known APN families (in dimensions up to 11) [12], the remained families of APN functions are pairwise inequivalent in general. We present a complete list of the known families of APN polynomials, which are pairwise CCZ-inequivalent, in Table 3.

2 Preliminaries

Let $\mathbb{F}_{2^n}[x]$ be the univariate polynomial ring defined over $\mathbb{F}_{2^n}$. Any function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ can be represented by a univariate polynomial of degree at most $2^n - 1$ in $\mathbb{F}_{2^n}[x]$, that is

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

The algebraic degree of a function F is equal to the maximum 2-weight of the exponent i such that $c_i \neq 0$, where the *2-weight* of i is the (Hamming) weight of its binary representation. Functions of algebraic degree 1 are called *affine* and of degree 2 *quadratic*. Affine functions without the constant term are linear functions and they can be represented as $L(x) = \sum_{i=0}^{n-1} c_i x^{2^i}$.
We will denote the *trace function* from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ by $Tr_n^m(x) = \sum_{i=0}^{n/m-1} x^{2^{im}}$. When $m = 1$ we denote $Tr_n^1(x)$ by $Tr(x)$.

The *derivative* of F in the direction of $a \in \mathbb{F}_{2^n}^*$ is given by the function $D_aF(x) = F(x+a) + F(x)$. The function F is APN if for every $a \neq 0$ and every b in $\mathbb{F}_{2^n}$, the equation $D_aF(x) = b$ admits at most 2 solutions, or equivalently $|\mathrm{Im}(D_aF)| = 2^{n-1}$, where $\mathrm{Im}(F) = \{F(x) \,|\, x \in \mathbb{F}_{2^n}\}$ is the *image* of F.

There are several equivalence relations of functions for which the APN property is preserved. Two functions F and F' from $\mathbb{F}_{2^n}$ to itself are called:

- affine equivalent if $F' = A_1 \circ F \circ A_2$ where $A_1, A_2 : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are affine permutations;
- EA-equivalent if $F' = F'' + A$, where the map $A : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is affine and F'' is affine equivalent to F;

– CCZ-equivalent if there exists some affine permutation $\mathcal{L}$ of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ such that the image of the graph of F is the graph of F', that is, $\mathcal{L}(G_F) = G_{F'}$, where $G_F = \{(x, F(x)) : x \in \mathbb{F}_{2^n}\}$ and $G_{F'} = \{(x, F'(x)) : x \in \mathbb{F}_{2^n}\}$.

The affine equivalence is, obviously, included in the EA-equivalence, and EA-equivalence is a particular case of CCZ-equivalence [13]. Moreover, every permutation is CCZ-equivalent to its inverse [13].

There are six known infinite families of power APN functions presented in Table 1. Some results on CCZ-inequivalence between the functions in Table 1 were

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

Functions	Exponents d	Conditions	Degree
Golden	$2^i + 1$	$\gcd(i, n)$=1	2
Kasami	$2^{2i} - 2^i + 1$	$\gcd(i, n)$=1	i+1
Welch	$2^t + 3$	$n = 2t + 1$	3
Niho	$2^t + 2^{\frac{t}{2}} - 1$, t even $2^t + 2^{\frac{3t+1}{2}} - 1$, t odd	$n = 2t + 1$	$\frac{t+2}{2}$ t+1
Inverse	$2^{2t} - 1$	$n = 2t + 1$	$n - 1$
Dobbertin	$2^{4i} + 2^{3i} + 2^{2i} + 2^i - 1$	$n = 5i$	$i + 3$

proven in [9]. Recently, in both [16] and [14] Yoshiara and Dempwolff show that two APN power functions are CCZ-equivalent if and only if they are *cyclotomic-equivalent*, i.e. they are EA-equivalent or one is EA-equivalent to the inverse of the second one. Since the algebraic degree is preserved by the EA-equivalence, and families in Table 1 have different algebraic degree in general, then all these families differ up to CCZ-equivalence (although they can intersect in some particular cases).

There are also thirteen known infinite families of quadratic APN polynomials CCZ-inequivalent to power functions listed in Table 2.

3 Equivalence between known families

In this section we will show that families C3 and C11 in Table 2 are equivalent and they are included in family C4.

In [12], the authors present a table of all possible pairwise CCZ-inequivalent functions which can be derived from the known families of APN functions, up to dimension $n = 11$. According to this table, families C3 and C11 are the same on small dimensions and are contained in C4. Below we prove that this is actually true for all dimensions.

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

N°	Functions	Conditions	In
C1-C2	$x^{2^s+1} + u^{2^k-1}x^{2^{ik}+2^{mk+s}}$	$n = pk$, $\gcd(k,3)=\gcd(s,3k)=1$, $p \in \{3,4\}$, $i = sk \bmod p$, $m = p-i$, $n \geq 12$, u primitive in $\mathbb{F}_{2^n}^*$	[8]
C3	$x^{2^{2i}+2^i} + cx^{q+1} + dx^{q(2^{2i}+2^i)}$	$q = 2^m$, $n = 2m$, $\gcd(i,m)=1$, $\gcd(2^i+1, q+1) \neq 1$, $dc^q + c \neq 0$, $d \notin \{\lambda^{(2^i+1)(q-1)}, \lambda \in \mathbb{F}_{2^n}\}$, $d^{q+1} = 1$	[7]
C4	$x(x^{2^i} + x^q + cx^{2^i q}) + x^{2^i}(c^q x^q + sx^{2^i q}) + x^{(2^i+1)q}$	$q = 2^m$, $n = 2m$, $\gcd(i,m)=1$, $c \in \mathbb{F}_{2^n}$, $s \in \mathbb{F}_{2^n} \setminus \mathbb{F}_q$, $X^{2^i+1} + cX^{2^i} + c^q X + 1$ has no solution x s.t. $x^{q+1} = 1$	[7]
C5	$x^3 + a^{-1}Tr(a^3x^9)$	$a \neq 0$	[10]
C6	$x^3 + a^{-1}Tr_n^3(a^3x^9 + a^6x^{18})$	$3 \mid n$, $a \neq 0$	[11]
C7	$x^3 + a^{-1}Tr_n^3(a^6x^{18} + a^{12}x^{36})$	$3 \mid n$, $a \neq 0$	[11]
C8-C10	$ux^{2^s+1} + u^{2^k}x^{2^{-k}+2^{k+s}} + vx^{2^{-k}+1} + wu^{2^k+1}x^{2^s+2^{k+s}}$	$n = 3k$, $\gcd(k,3)=\gcd(s,3k)=1$, $v, w \in \mathbb{F}_{2^k}$, $vw \neq 1$, $3 \mid (k+s)$ u primitive in $\mathbb{F}_{2^n}^*$	[2, 3]
C11	$dx^{2^i+1} + d^q x^{q(2^i+1)} + cx^{q+1} + \sum_{s=1}^{m-1}\gamma_s x^{2^s(q+1)}$	$q = 2^m$, $n = 2m$, $\gcd(i,m)=1$, i, m odd, $c \notin \mathbb{F}_{2^m}$, $\gamma_s \in \mathbb{F}_{2^m}$, d not a cube	[2]
C12	$(x+x^q)^{2^i+1} + u'(ux+u^qx^q)^{(2^i+1)2^j} + u(x+x^q)(ux+u^qx^q)$	$q = 2^m$, $n = 2m$, $m \geq 2$ even, $\gcd(i,m) = 1$ and j even u primitive in $\mathbb{F}_{2^n}^*$, $u' \in \mathbb{F}_{2^m}$ not a cube	[17]
C13	$a^2x^{2^{2m+1}+1} + b^2x^{2^{m+1}+1} + ax^{2^{2m}+2} + bx^{2^m+2} + (c^2+c)x^3$	$n = 3m$, m odd $L(x) = ax^{2^{2m}} + bx^{2^m} + cx$ satisfies the conditions in Theorem 6.3 of [6]	[6]

3.1 C11 and C3 are equivalent

First of all, note that, for family C11, the conditions given in Table 2 that i is odd and d is not a cube are equivalent to request just $d \notin \{x^{2^i+1} : x \in \mathbb{F}_{2^{2m}}\}$ (if i is even we have no choice for d since in this case $\{x^{2^i+1} : x \in \mathbb{F}_{2^{2m}}\} = \mathbb{F}_{2^{2m}}$). Moreover, for family C3, we have that the coefficients c and d, satisfying the constrains of Table 2, exist if and only if $\gcd(2^i+1, 2^m+1) \neq 1$. This implies that m is odd, since i and m are coprime (it can be easily deduced from $\gcd(2^{2i}-1, 2^{2m}-1) = 2^{\gcd(2i,2m)} - 1 = 3$).

Consider the following function of C11 (without the sum component)

$$F(x) = cx^{2^m+1} + dx^{2^i+1} + d^{2^m}x^{2^m(2^i+1)}. \tag{1}$$

Since $c \in \mathbb{F}_{2^{2m}} \setminus \mathbb{F}_{2^m}$ we have $\mathbb{F}_{2^{2m}} = c\mathbb{F}_{2^m} \oplus \mathbb{F}_{2^m}$. Let us consider the linear permutation L such that over $c\mathbb{F}_{2^m}$ it is the identity map and over $\mathbb{F}_{2^m}$ it is given by the power linear function x^{2^i}. That is, for any $x_1, x_2 \in \mathbb{F}_{2^m}$, $L(cx_1 + x_2) = cx_1 + x_2^{2^i}$. Then,

$$\frac{L(F(x))}{d^{2^i}} = c' x^{2^m+1} + x^{2^{2i}+2^i} + d' x^{2^m(2^{2i}+2^i)},$$

with $c' = \dfrac{c}{d^{2^i}}$ and $d' = d^{2^i(2^m-1)}$. Since, $d \notin \{x^{2^i+1} : x \in \mathbb{F}_{2^{2m}}\}$ we have $d' \notin \{x^{(2^i+1)(2^m-1)} : x \in \mathbb{F}_{2^{2m}}\}$. Moreover, since $c \notin \mathbb{F}_{2^m}$

$$c'^{2^m} d' + c' = \frac{c^{2^m}}{d^{2^i}} + \frac{c}{d^{2^i}} \neq 0,$$

implying that F in (1) is equivalent to an APN function contained in C3.

Consider now the general formula of C11:

$$F(x) = cx^{2^m+1} + \sum_{l=1}^{m-1} \gamma_l x^{2^l(2^m+1)} + dx^{2^i+1} + d^{2^m} x^{2^m(2^i+1)}.$$

It is possible to reduce it to a function of the type (1).
Assume $1 \leq t \leq m-1$ be such that $\gamma_t \neq 0$. We know that, since $\gamma_t \in \mathbb{F}_{2^m}$, there exists a non-zero element λ_t such that $\gamma_t = \lambda_t^{2^t(2^m+1)}$. Applying the substitution $x \to \lambda_t^{-1} x$ we obtain an equivalent function with $\gamma_t = 1$.
Consider the following linear function with $w \in \mathbb{F}_{2^m}^*$ (we will study its permutation property later)

$$L(x) = (w + (c + c^{2^m})^{2^t})x + x^{2^t} + wx^{2^m} + x^{2^{m+t}}. \tag{2}$$

Let $u = dx^{2^i+1}$, then we obtain

$$\begin{aligned} L(F(x)) &= (w + (c + c^{2^m})^{2^t} + w)[u + u^{2^m}] + ((w + (c + c^{2^m})^{2^t})c + wc^{2^m})x^{2^m+1} \\ &\quad + (c + c^{2^m})^{2^t} x^{2^t(2^m+1)} + \sum_{l=1}^{m-1} \gamma_l (w + (c + c^{2^m})^{2^t} + w) x^{2^l(2^m+1)} \\ &= (c + c^{2^m})^{2^t}[u + u^{2^m}] + (w(c + c^{2^m}) + c(c + c^{2^m})^{2^t})x^{2^m+1} \\ &\quad + \sum_{l=1, l\neq t}^{m-1} \gamma_l (c + c^{2^m})^{2^t} x^{2^l(2^m+1)}. \end{aligned}$$

Hence

$$\frac{L(F(x))}{(c + c^{2^m})^{2^t}} = u + u^{2^m} + (w(c + c^{2^m})^{1-2^t} + c)x^{2^m+1} + \sum_{l=1, l\neq t}^{m-1} \gamma_l x^{2^l(2^m+1)}.$$

Let $c' = w(c + c^{2^m})^{1-2^t} + c$, also the condition on c' is satisfied since we have

$$\begin{aligned} c'^{2^m} + c' &= w^{2^m}(c + c^{2^m})^{1-2^t} + c^{2^m} + w(c + c^{2^m})^{1-2^t} + c \\ &= (c + c^{2^m}). \end{aligned}$$

Therefore, we managed, from the original formula of C11, to obtain a similar one in which the monomial $x^{2^t(2^m+1)}$ is not present any more and the rest of the components of the sum is left unchanged. Iterating this procedure we obtain a function of the form (1).

Now, we only need to show that $L(x)$ of Equation (2) is a permutation. We have that

$$L(x) = (x + x^{2^m})^{2^t} + w(x + x^{2^m}) + (c + c^{2^m})^{2^t} x.$$

Assume that $x \in \mathbb{F}_{2^m}$ then $L(x) = (c + c^{2^m})^{2^t} x$ is null if and only if $x = 0$. Otherwise consider $x \notin \mathbb{F}_{2^m}$ and let $y = x + x^{2^m} \in \mathbb{F}_{2^m}^*$, we have $L(x) = y^{2^t} + wy + (c + c^{2^m})^{2^t} x$. If $L(x) = 0$ then

$$x = \frac{y^{2^t} + wy}{(c + c^{2^m})^{2^t}}.$$

Since $w \in \mathbb{F}_{2^m}$ we have that the right hand-side belongs to $\mathbb{F}_{2^m}$ that leads to a contradiction. Therefore, L is a linear permutation.

Conversely, we have that C3 can be reduced to C11 reversing the computation done for (1). Indeed, let

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

be an APN function of C3, with c and d satisfying the constrains of C3.

Since $d^{2^m+1} = 1$, there exists d' such that $d'^{2^m-1} = d$. Moreover, since d is not in $\{x^{(2^i+1)(2^m-1)} : x \in \mathbb{F}_{2^{2m}}\}$ we have $d' \notin \{x^{(2^i+1)} : x \in \mathbb{F}_{2^{2m}}\}$. Multiplying it by d', we obtain

$$F'(x) = d'F(x) = d'cx^{2^m+1} + d'x^{2^i+1} + d'^{2^m} x^{2^m(2^i+1)}.$$

Since $c + c^{2^m} d \neq 0$ we have that $d'c + (d'c)^{2^m} = d'(c + c^{2^m} d) \neq 0$, so $d'c \notin \mathbb{F}_{2^m}$. Thus, $F'(x)$ is an element of C11 and we have the following result.

Lemma 1. *Families C3 and C11 are equivalent.*

3.2 Equivalence with hexanomials (family C4 Table 2)

In [7], the authors introduced a family of APN hexanomials. In particular the result is the following.

Theorem 1 ([7]). *Let n and i be any positive integers, $n = 2m$, $\gcd(i, m) = 1$, and $\bar{c}, \bar{d} \in \mathbb{F}_{2^n}$ be such that $\bar{d} \notin \mathbb{F}_{2^m}$. If the equation*

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

has no solution x such that $x^{2^m+1} = 1$, then the function

$$H(x) = \bar{d}x^{2^i(2^m+1)} + x^{(2^m+1)} + (x^{2^i+1} + x^{2^m(2^i+1)} + \bar{c}x^{2^{m+i}+1} + \bar{c}^{2^m}x^{2^i+2^m})$$

is APN.

We are going to show below that C3 and C11 are contained in C4. As proved in the previous section, we can consider only family C11 without the part $\sum_{\ell=1}^{m-1} \gamma_\ell x^{2^\ell(2^m+1)}$.

Consider now the function in C11 as in (1). We can transform it in a function as follows

$$F(x) = cx^{2^m+1} + x^{2^i(2^m+1)} + dx^{2^i+1} + d^{2^m}x^{2^m(2^i+1)}, \tag{3}$$

with $c \in \mathbb{F}_{2^{2m}} \setminus \mathbb{F}_{2^m}$ and $d \notin \{x^{2^i+1} : x \in \mathbb{F}_{2^{2m}}\}$. Indeed, using linear permutations as in (2), we can obtain from functions in form (3) all possible functions as in (1).

Consider a linear permutation of type $x + \gamma x^{2^m}$ ($\gamma^{2^m+1} \neq 1$). Evaluating $F(x + \gamma x^{2^m})$ and deleting terms of algebraic degree less than 2, we obtain

$$\left.\begin{array}{rl} \widetilde{F}(x) = & (c + c\gamma^{2^m+1})x^{2^m+1} + (1 + \gamma^{2^i(2^m+1)})x^{2^i(2^m+1)} \\ & +(d + d^{2^m}\gamma^{2^m(2^i+1)})x^{2^i+1} + (d^{2^m} + d\gamma^{2^i+1})x^{2^m(2^i+1)} \\ & +(d\gamma^{2^i} + d^{2^m}\gamma^{2^m})x^{2^{m+i}+1} + (d^{2^m}\gamma^{2^{m+i}} + d\gamma)x^{2^i+2^m} \end{array}\right\} = u$$

Now, using a similar linear permutation as for the sum $\sum_{\ell=1}^{m-1} \gamma_\ell x^{2^\ell(2^m+1)}$, it is possible to prove that we can delete the monomial $(1 + \gamma^{2^i(2^m+1)})x^{2^i(2^m+1)}$ since $(1+\gamma^{2^i(2^m+1)})$ and u are in $\mathbb{F}_{2^m}$. Now, denoting by $a = (d+d^{2^m}\gamma^{2^m(2^i+1)})$ and $b = (d\gamma^{2^i} + d^{2^m}\gamma^{2^m})$ we have

$$F'(x) = c'x^{2^m+1} + (ax^{2^i+1} + a^{2^m}x^{2^m(2^i+1)} + bx^{2^{m+i}+1} + b^{2^m}x^{2^i+2^m}), \tag{4}$$

where $c' \in \mathbb{F}_{2^{2m}} \setminus \mathbb{F}_{2^m}$ depends on the linear function applied for removing $(1 + \gamma^{2^i(2^m+1)})x^{2^i(2^m+1)}$.

Now, since i and m are odd and $\gcd(i, m) = 1$ we have that $x^{2^{m+i}+1}$ is a permutation of $\mathbb{F}_{2^n}$, which means that there exists $\lambda \in \mathbb{F}_{2^n}^*$ such that $\lambda^{2^{m+i}+1} = b$. Then, substituting $x \mapsto \lambda^{-1}x$ in (4) we obtain

$$F''(x) = \underbrace{c''x^{2^m+1}}_{c''\mathbb{F}_{2^m}} + \underbrace{\frac{a}{\lambda^{2^i+1}}x^{2^i+1} + \left(\frac{a}{\lambda^{2^i+1}}\right)^{2^m} x^{2^m(2^i+1)} + x^{2^{m+i}+1} + x^{2^i+2^m}}_{\mathbb{F}_{2^m}}.$$

Since $\mathbb{F}_{2^n} = c''\mathbb{F}_{2^m} \oplus \mathbb{F}_{2^m}$ we can perform the substitution $x \mapsto x^{2^{m-i}}$ and then apply a linear map L which is $x^{1/2^{m-i}}$ on $c''\mathbb{F}_{2^m}$ and the identity on $\mathbb{F}_{2^m}$. Thus, denoting by $c = (c'')^{1/2^{m-i}}$, we can obtain the equivalent function

$$\begin{aligned}\bar{F}(x) = L(F''(x^{2^{m-i}})) =& cx^{2^m+1} + \frac{a}{\lambda^{2^i+1}}x^{2^m+2^j} + \left(\frac{a}{\lambda^{2^i+1}}\right)^{2^m} x^{(2^{m+j}+1)} \\ &+ x^{2^j+1} + x^{2^m(2^j+1)},\end{aligned} \tag{5}$$

where $j = m - i$. Note that j is even and $\gcd(j, m) = 1$.

On the other hand, let i be an integer with $\gcd(i, m) = 1$ and consider a hexanomial

$$H(x) = \bar{d}x^{2^i(2^m+1)} + x^{(2^m+1)} + (x^{2^i+1} + x^{2^m(2^i+1)} + \bar{c}x^{2^{m+i}+1} + \bar{c}^{2^m}x^{2^i+2^m}).$$

Applying the linear permutation (as in (2)) $L(x) = (w+(\bar{d}+\bar{d}^{2^m})^{1/2^i})x+wx^{2^m} + x^{1/2^i} + x^{2^{m-i}}$ for some $w \in \mathbb{F}_{2^m}^*$, we obtain

$$H'(x)=\frac{L(H(x))}{(\bar{d}+\bar{d}^{2^m})^{1/2^i}}=\bar{d}'x^{2^i(2^m+1)} + (x^{2^i+1} + x^{2^m(2^i+1)} + \bar{c}x^{2^{m+i}+1} + \bar{c}^{2^m}x^{2^i+2^m}).$$

Since $\mathbb{F}_{2^{2m}} = \bar{d}'\mathbb{F}_{2^m} \oplus \mathbb{F}_{2^m}$ we can apply a linear permutation which is $x^{(1/2^i)}$ on $\bar{d}'\mathbb{F}_{2^m}$ and the identity on $\mathbb{F}_{2^m}$ in order to obtain the equivalent function

$$H''(x) = d''x^{2^m+1} + x^{2^i+1} + x^{2^m(2^i+1)} + \bar{c}x^{2^{m+i}+1} + \bar{c}^{2^m}x^{2^i+2^m}, \tag{6}$$

where $d'' = \bar{d}'^{(1/2^i)}$. Then, the family of the hexanomials can be expressed as pentanomials and the constrain on the coefficient $\bar{c}$ is the same of the hexanomials. Indeed, following the same steps of the proof in [7, Theorem 2], a function H'' as in (6), with $d'' \notin \mathbb{F}_{2^m}$ and i such that $\gcd(i, m) = 1$, is APN if and only if

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

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

Coming back to our function in (5), since $\bar{F}(x)$ is APN and $c'' \notin \mathbb{F}_{2^m}$, denoting $\bar{a} = \left(\frac{a}{\lambda^{2^i+1}}\right)^{2^m}$, we have that

$$x^{2^j+1} + \bar{a}x^{2^j} + \bar{a}^{2^m}x + 1 = 0$$

has no nonzero solution such that $x^{2^m+1} = 1$. So, the function $\bar{F}(x)$ is equivalent to a hexanomials.

Then we have proved the following result:

Theorem 2. *Families C3 and C11 coincide and they are included in C4. In particular, the hexanomials admit a representation in the following form*

$$H_i(x) = \bar{d}x^{2^m+1} + x^{2^i+1} + x^{2^m(2^i+1)} + \bar{c}x^{2^{m+i}+1} + \bar{c}^{2^m}x^{2^i+2^m},$$

with $\bar{d} \notin \mathbb{F}_{2^m}$ and $\bar{c}$ such that the equation

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

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

Moreover, when m is odd, a pentanomial $H_i(x)$ for i odd is equivalent to a pentanomial $H_j(x)$ (always in C4) with $j = m - i$ even.

Proof. We need to prove only that when m is odd the case i odd is equivalent to a pentanomial relative to the even case $j = m - i$. This can be done with the same steps used above to compute $\bar{F}(x)$ in (5) from $F''(x)$ of (4), with the only difference that in this case the coefficient a of $F''(x)$ is equal to 1.

In Table 3 we list all the known families of APN functions which are CCZ-inequivalent to power functions and that are pairwise CCZ-inequivalent to each other.

Table 3. Known classes of quadratic APN polynomial over $\mathbb{F}_{2^n}$ CCZ-inequivalent to power functions

N°	Functions	Conditions	In
F1-F2	$x^{2^s+1} + u^{2^k-1}x^{2^{ik}+2^{mk}+s}$	$n = pk$, $\gcd(k,3)= \gcd(s,3k)=1$, $p \in \{3,4\}$, $i = sk \bmod p$, $m = p - i$, $n \geq 12$, u primitive in $\mathbb{F}_{2^n}^*$	[8]
F3	$sx^{q+1} + x^{2^i+1} + x^{q(2^i+1)}$ $+cx^{2^iq+1} + c^q x^{2^i+q}$	$q = 2^m$, $n = 2m$, $\gcd(i,m)=1$, $c \in \mathbb{F}_{2^n}$, $s \in \mathbb{F}_{2^n} \setminus \mathbb{F}_q$, $X^{2^i+1} + cX^{2^i} + c^q X + 1$ has no solution x s.t. $x^{q+1} = 1$	[7]
F4	$x^3 + a^{-1}\,Tr(a^3x^9)$	$a \neq 0$	[10]
F5	$x^3 + a^{-1}\,Tr_n^3(a^3x^9 + a^6x^{18})$	$3\|n$, $a \neq 0$	[11]
F6	$x^3 + a^{-1}\,Tr_n^3(a^6x^{18} + a^{12}x^{36})$	$3\|n$, $a \neq 0$	[11]
F7-F9	$ux^{2^s+1} + u^{2^k}x^{2^{-k}+2^{k+s}}+$ $vx^{2^{-k}+1} + wu^{2^k+1}x^{2^s+2^{k+s}}$	$n = 3k$, $\gcd(k,3)= \gcd(s,3k)=1$, $v, w \in \mathbb{F}_{2^k}$, $vw \neq 1$, $3\|(k+s)$ u primitive in $\mathbb{F}_{2^n}^*$	[2, 3]
F10	$(x + x^q)^{2^i+1}+$ $u'(ux + u^qx^q)^{(2^i+1)2^j} +$ $u(x + x^q)(ux + u^qx^q)$	$q = 2^m$, $n = 2m$, $m \geq 2$ even, $\gcd(i,m) = 1$ and $j \geq 2$ even u primitive in $\mathbb{F}_{2^n}^*$, $u' \in \mathbb{F}_{2^m}$ not a cube	[17]
F11	$a^2x^{2^{2m+1}+1} + b^2x^{2^{m+1}+1}+$ $ax^{2^{2m}+2} + bx^{2^m+2} + (c^2+c)x^3$	$n = 3m$, m odd $L(x) = ax^{2^{2m}} + bx^{2^m} + cx$ satisfies the conditions in Theorem 6.3 of [6]	[6]

References

1. E. Biham, A. Shamir: *Differential Cryptanalysis of DES-like Cryptosystems.* J. Cryptology 4(1), 3-72 (1991)
2. C. Bracken, E. Byrne, N. Markin, G. McGuire: *New Families of Quadratic Almost Perfect Nonlinear Trinomials and Multinomials.* Finite Fields and Their Applications 14(3), 703–714 (2008)
3. C. Bracken, E. Byrne, N. Markin, and G. McGuire, *A Few More Quadratic APN Functions*, Cryptography and Communications, 3(1), 2011, pp. 43-53.
4. 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, 1993, pp. 65-76.
5. M. Brinkmann, G. Leander, *On the classification of APN functions up to dimension five.* Designs, Codes and Cryptography, 49(1-3), 273-288, 2008.
6. L. Budaghyan, M. Calderini, C. Carlet, R. Coulter, I. Villa, *Constructing APN functions through isotopic shift.* Cryptology ePrint Archive, Report 2018/769.
7. L. Budaghyan, C. Carlet: *Classes of Quadratic APN Trinomials and Hexanomials and Related Structures.* IEEE Trans. Inform. Theory 54(5), 2354-2357 (2008)
8. L. Budaghyan, C. Carlet, and G. Leander, *Two classes of quadratic APN binomials inequivalent to power functions*, IEEE Trans. Inform. Theory, 54(9), 2008, pp. 4218-4229.
9. L. Budaghyan, C. Carlet, G.Leander, *On inequivalence between known power APN functions.* In: Masnyk-Hansen, O., Michon, J.-F., Valarcher, P., J.-B.Yunes (Eds.) Proceedings of the conference BFCA'08, Copenhagen.
10. L. Budaghyan, C. Carlet, and G. Leander, *Constructing new APN functions from known ones*, Finite Fields and Their Applications, vol.15, issue 2, Apr. 2009, pp. 150-159.
11. L. Budaghyan, C. Carlet, and G. Leander, *On a construction of quadratic APN functions*, Proceedings of IEEE Information Theory workshop ITW'09, Oct. 2009, pp. 374-378.
12. Budaghyan L., Helleseth T., Li N., Sun B., *Some Results on the Known Classes of Quadratic APN Functions.* In: El Hajji S., Nitaj A., Souidi E. (eds) Codes, Cryptology and Information Security. C2SI 2017. Lecture Notes in Computer Science, vol 10194. Springer, Cham (2017)
13. C. Carlet, P. Charpin, and V. Zinoviev, *Codes, bent functions and permutations suitable for DES-like cryptosystems.* Designs, Codes and Cryptography 15.2 (1998): 125-156. Sci., vol. 5203, Springer-Verlag, Berlin, 2008, pp. 368–376.
14. U. Dempwolff, *CCZ equivalence of power functions*, submitted to Designs, Codes and Cryptography Mar. 2017
15. K. Nyberg, *Differentially uniform mappings for cryptography*, Advances in Cryptography, EUROCRYPT'93, Lecture Notes in Computer Science 765, 1994, pp. 55-64.
16. S. Yoshiara, *Equivalences of power APN functions with power or quadratic APN functions*, Journal of Algebraic Combinatorics, vol. 44, N. 3. Nov. 2016, pp. 561-585.
17. Y. Zhou and A. Pott. *A New Family of Semifields with 2 Parameters.* Advances in Mathematics, 234:43-60, 2013.