Generalization of a class of APN binomials to Gold-like functions

D. Davidova[1] N. Kaleyski

[1]Department of Informatics, University of Bergen,
7803 NO-5020 Bergen, Norway
Diana.Davidova@uib.no,
Nikolay.Kaleyski@uib.no

Abstract. In 2008 Budaghyan, Carlet and Leander generalized a known instance of an APN function over the finite field $\mathbb{F}_{2^{12}}$ and constructed two new infinite families of APN binomials over the finite field $\mathbb{F}_{2^n}$, one for n divisible by 3, and one for n divisible by 4. By relaxing conditions, the family of APN binomials for n divisible by 3 was generalized to a family of differentially 2^t-uniform functions in 2012 by Bracken, Tan and Tan; in this sense, the binomials behave in the same way as the Gold functions. In this paper, we show that when relaxing conditions on the APN binomials for n divisible by 4, they also behave in the same way as the Gold function x^{2^s+1} (with s and n not necessarily coprime). As a counterexample, we also show that a family of APN quadrinomials obtained as a generalization of a known APN instance over $\mathbb{F}_{2^{10}}$ cannot be generalized to functions with 2^t-to-1 derivatives by relaxing conditions in a similar way.

Keywords: almost perfect nonlinear, Boolean functions, differential uniformity, Walsh transform, Walsh spectrum

1 Introduction

Let n, m be natural numbers. A *vectorial Boolean* (n, m)*-function*, or simply an (n, m)*-function*, or vectorial Boolean function, is a mapping from the n-dimensional vector space $\mathbb{F}_2^n$ over the finite field $\mathbb{F}_2 = \{0, 1\}$ to the m-dimensional vector space $\mathbb{F}_2^m$. Since the extension field $\mathbb{F}_{2^n}$ can be identified with an n-dimensional vector space over $\mathbb{F}_2$, (n, m)-functions can be seen as functions between the Galois fields $\mathbb{F}_{2^n}$ and $\mathbb{F}_{2^m}$. Vectorial Boolean functions have many applications in mathematics and computer science. In cryptography, they are the basic building blocks of block ciphers, and the choice of functions directly influences the security of the cipher. In order to construct cryptographically secure ciphers, it is necessary to understand what properties such functions need to possess in order to resist various types of cryptanalytic attacks, and to find methods for constructing functions having these desirable properties. In our work, we mostly concentrate on the case when $n = m$, i.e. when the number of input and output bits is the same. A comprehensive survey on (n, m)-functions can be found in [4, 8].

One of the most powerful attacks against block ciphers is differential cryptanalysis, introduced by Biham and Shamir [1]. The attack is based on studying how the difference in two inputs to a function affects the difference in the corresponding outputs. The resistance to differential attacks of an (n, m)-function is measured by a property called its differential uniformity. The lower the differential uniformity, the more resistant the cryptosystem is to differential attacks. The class of almost perfect nonlinear (APN) functions is defined as the class of (n, n)-functions having the best possible differential uniformity, and thus provides optimal security against differential cryptanalysis.

Another powerful attack against block ciphers is linear cryptanalysis, introduced by Matsui [12]. The property of a function which measures the resistance to this kind of attack is called nonlinearity. The nonlinearity $\mathcal{NL}(F)$ of an (n, m)-function F is defined to be the minimum Hamming distance between any component of F and any affine $(n, 1)$-function. An upper bound on the nonlinearity of any (n, n)-function can be derived, and the class of almost bent (AB) functions is defined as the class of those functions that meet this bound with equality and therefore provide the best possible resistance to linear attacks.

Recall that the Gold functions are APN power functions over $\mathbb{F}_{2^n}$ of the form x^{2^s+1} for some natural number s satisfying $\gcd(s, n) = 1$. Relaxing the condition to $\gcd(s, n) = t$ for some positive integer t, the functions of the form $F(x) = x^{2^s+1}$ become differentially 2^t-uniform, with all their derivatives $D_aF(x) = F(x)+F(a+x)$ for $a \neq 0$ being 2^t-to-1 functions. These functions are permutations if and only if $n/\gcd(s, n) = n/t$ is odd [13], and are $(2^t + 1)$–to–1 functions otherwise. Their nonlinearity is $2^{n-1} - 2^{(n+t)/2}$ when n/t is odd, and $2^{n-1} - 2^{(n+2t)/2}$ otherwise.

In 2008, two infinite families of (n, n)-APN binomials inequivalent to power functions were introduced in [5] for values of n divisible by 3 or by 4 as generalizations of a known sporadic APN instance over $\mathbb{F}_{2^{12}}$ [11]. These were the first known infinite families of APN functions that are inequivalent to power functions. It was later shown in 2012 that the family of APN binomials for n divisible by 3 can be generalized to functions with 2^t-to-1 derivatives (for some positive integer t) with nonlinearity equal to $2^{n-1} - 2^{(n+t)/2}$ for $n + t$ even, and $2^{n-1} - 2^{(n+t-1)/2}$ for $n + t$ odd by relaxing conditions [3]. Thus, the APN binomials for n divisible by 3 behave in the same way as the Gold functions from the point of view of differential uniformity, nonlinearity and properties of the image set.

In this paper we show that the second class of APN binomials from [5] (for n divisible by 4) also behaves in the same way as the Gold functions in this respect. We note that all the constructed functions (much like the APN binomials) are quadratic, and are therefore not directly suitable for cryptographic use in practice. Nonetheless, the vast majority of known APN functions are given by a quadratic representation, but contain representatives of higher algebraic degrees in their CCZ-equivalence class. We also consider the family of APN quadrinomials constructed by generalizing a known APN instance over $\mathbb{F}_{2^{10}}$ [7] and computationally verify that they provide a counterexample to this approach,

in the sense that they cannot be generalized to functions with 2^t-to-1 derivatives by relaxing conditions in a similar way for any even dimension n in the range $6 \leq n \leq 14$.

The paper is structured as follows. In Section 2, we recall the basic definitions and results that we use throughout our work. In Section 3, we compute the differential uniformity of the generalized families of binomials; an upper bound on their nonlinearity is then derived in Section 4. Section 5, in which we computationally show that the APN quadrinomials constructed in [7] cannot be generalized to 2^t-uniform functions over $\mathbb{F}_{2^n}$ with $6 \leq n \leq 14$, concludes the paper.

2 Preliminaries

Let n be a positive integer. Then $\mathbb{F}_{2^n}$ denotes the finite field with 2^n elements, and $\mathbb{F}_{2^n}^*$ denotes its multiplicative group. For any positive integer k dividing n, the trace function Tr_k^n is the mapping from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^k}$ defined by $\mathrm{Tr}_k^n(x) = \sum_{i=0}^{\frac{n}{k}-1} x^{2^{ik}}$. For $k = 1$, the function $\mathrm{Tr}_1^n : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is called the *absolute trace* over $\mathbb{F}_{2^n}$ and is denoted simply by $\mathrm{Tr}_n(x)$, or by $\mathrm{Tr}(x)$ if the dimension n is clear from context.

Let n and m be positive integers. An (n, m)-*function* is any function F from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$. For any (n, m)-function F and for any $a \in \mathbb{F}_{2^n}$, the function $D_aF(x) = F(x + a) + F(x)$ is called the *derivative of F in the direction a*. Let $\delta_F(a, b)$ denote the number of solutions of the equation $D_aF(x) = b$ for some $a \in \mathbb{F}_{2^n}$ and $b \in \mathbb{F}_{2^m}$. The multiset $\{\delta_F(a, b) : a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^m}\}$ is called the *differential spectrum* of F. The *differential uniformity* of F is the largest value in its differential spectrum. We say that F is *differentially δ-uniform* if its differential uniformity is at most δ. The differential uniformity of any (n, m)-function is clearly always even, since if $x \in \mathbb{F}_{2^n}$ is a solution to $D_aF(x) = b$ for some $a \in \mathbb{F}_{2^n}$ and $b \in \mathbb{F}_{2^m}$, then so is $x + a$. The lowest possible differential uniformity of any function is thus 2. A function with differential uniformity equal to 2 is called *almost perfect nonlinear (APN)*. Since a low differential uniformity corresponds to a strong resistance to differential cryptanalysis, APN functions provide optimal security against this type of attack.

A *component function* of an (n, m)-function F is any function of the form $x \mapsto \mathrm{Tr}_m(cF(x))$ for $c \in \mathbb{F}_{2^m}^*$. The component functions are clearly $(n, 1)$-functions. The nonlinearity $\mathcal{NL}(F)$ of F is the minimum Hamming distance between any component function of F and any affine $(n, 1)$-function, i.e. any function $a : \mathbb{F}_{2^n} \to \mathbb{F}_2$ satisfying $a(x) + a(y) + a(z) = a(x + y + z)$ for all $x, y, z \in \mathbb{F}_{2^n}$. Recall that the Hamming distance between two $(n, 1)$-functions f and g is the number of inputs $x \in \mathbb{F}_{2^n}$ for which $f(x) \neq g(x)$.

An important tool for analyzing any (n, m)-function F is the so-called Walsh transform. The *Walsh transform of F* is the function $W_F : \mathbb{F}_{2^m} \times \mathbb{F}_{2^n} \to \mathbb{Z}$ defined as $W_F(a, b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_m(aF(x)) + Tr_n(bx)}$.

The nonlinearity of an (n, m)-function F can be expressed as $\mathcal{NL}(F) = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_{2^m}^*, b \in \mathbb{F}_{2^n}} |W_F(a, b)|$. The nonlinearity of any (n, n)-function is bounded from above by $2^{n-1} - 2^{(n-1)/2}$ [10]. Functions attaining this bound are called *almost bent (AB)*. Clearly, AB functions exist only for odd values of n; when n is even, functions with nonlinearity $2^{n-1} - 2^{n/2}$ are known, and it is conjectured that this value is optimal in the even case. Nonlinearity measures the resistance to linear cryptanalysis; the higher the nonlinearity, the better. Thus, AB functions provide optimal security against linear cryptanalysis when n is odd. Furthermore, all AB functions are necessarily APN [10], so that AB functions are optimal with respect to differential cryptanalysis as well.

Due to the huge number of (n, m)-functions for non-trivial values of n and m, they are typically classified up to some notion of equivalence. The most general known equivalence relation which preserves differential uniformity (and hence APN-ness) is Carlet-Charpin-Zinoviev (or CCZ) equivalence [6, 9]. We say that two (n, m)-functions F and F' are *CCZ-equivalent* if there is an affine permutation $\mathcal{A}$ of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$ that maps the graph $\mathcal{G}(F) = \{(x, F(x)) : x \in \mathbb{F}_{2^n}\}$ of F to the graph $\mathcal{G}(F')$ of F'. A special case of CCZ-equivalence is extended affine (or EA) equivalence. We say that F and F' are *EA-equivalent* if there are affine permutations A_1 and A_2 of $\mathbb{F}_{2^m}$ and $\mathbb{F}_{2^n}$, respectively, and an affine (n, m)-function A such that $F' = A_1 \circ F \circ A_2 + A$.

In [5], Budaghyan, Carlet and Leander introduced the following two infinite families of APN binomials:

1. For $n = 3k$:
$$F_3(x) = x^{2^s+1} + w^{2^k-1} x^{2^{ik}+2^{mk+s}}, \tag{1}$$
where s and k are positive integers such that $s \leq 4k - 1$, $\gcd(k, 3) = \gcd(s, 3k) = 1$, $i = sk \mod 3$, $m = 3 - i$ and w is a primitive element of the field $\mathbb{F}_{2^n}$.
2. For $n = 4k$:
$$F_4(x) = x^{2^s+1} + w^{2^k-1} x^{2^{ik}+2^{mk+s}}, \tag{2}$$
where s and k are positive integers such that $s \leq 4k - 1$, $\gcd(k, 2) = \gcd(s, 2k) = 1$, $i = sk \mod 4$, $m = 4 - i$ and w is a primitive element of the field $\mathbb{F}_{2^n}$.

The first class of APN binomials (for n divisible by 3) are permutations if and only if k is odd.

As we show below, if the condition of k being odd is omitted, the binomials for n divisible by 4 are EA-equivalent to the Gold functions. Indeed, let k be even. Then $i = sk \mod 4$ is also even. If $i = 2$, then

$$F(x) = x^{2^s+1} + w^{2^k-1} x^{2^{ik}+2^{mk+s}} = x^{2^s+1} + w^{2^k-1} x^{2^{2k}+2^{2k+s}} =$$
$$x^{2^s+1} + w^{2^k-1} x^{2^{2k}(1+2^s)} = x^{2^s+1} + w^{2^k-1} (x^{2^s+1})^{2^{2k}}$$

which is EA-equivalent to x^{2^s+1} since $x \mapsto x+w^{2^k-1}x^{2^{2k}}$ is a linear permutation. Indeed, if $x+w^{2^k-1}x^{2^{2k}} = y+w^{2^k-1}y^{2^{2k}}$ and $x \neq y$, then we must have $w^{1-2^k} = (x+y)^{2^{2k}-1}$ which is impossible since $2^{2k}-1$ is a multiple of 5 under the hypothesis, whereas 2^k-1 is not.

In the same manner, if $i = 0$, we get

$$F(x) = x^{2^s+1} + w^{2^k-1}x^{2^{ik}+2^{mk+s}} = x^{2^s+1} + w^{2^k-1}x^{1+2^s} = \quad x^{2^s+1}\Big(1+w^{2^k-1}\Big).$$

The complete Walsh spectra of the functions F_3 and F_4 were determined in [2].

As previously mentioned, relaxing the conditions allows the functions F_3 to be generalized to a family of 2^t-differentially uniform functions in the same way as the Gold functions [3]. In this paper, we show how the family F_4 can be generalized to functions with 2^t-to-1 derivatives in a similar way. Further, we provide a counterexample to the question of whether this construction can be used to generalize any family of quadratic APN functions to a family of 2^t-uniform functions: for the family of quadrinomials from [7], we computationally verify that relaxing conditions does not lead to functions with 2^t-to-1 derivatives for $t > 1$ over $\mathbb{F}_{2^n}$ for any $6 \leq n \leq 14$.

For background on APN functions and cryptographic Boolean functions, we refer the reader to [4] or [8].

3 Differential uniformity

In the following theorem, we show that by relaxing the condition $\gcd(s, 2k) = 1$ in (2) to $\gcd(s, 2k) = t$ for some positive integer t, we obtain functions over $\mathbb{F}_{2^{4k}}$ all of whose derivatives are 2^t-to-1 functions.

Theorem 1. *Let s, k, t be positive integers and let $n = 4k$. Let $\gcd(s, 2k) = t$, $2 \nmid k$, $i = sk \mod 4$, $m = 4 - i$, and w be a primitive element of $\mathbb{F}_{2^n}$. Then all derivatives D_aF for $a \in \mathbb{F}_{2^n}^*$ of the function*

$$F(x) = wx^{2^s+1} + w^{2^k}x^{2^{ik}+2^{mk+s}} \tag{3}$$

are 2^t-to-1 functions. In particular, F is differentially 2^t-uniform.

Proof. We first show that for i even, F is EA-equivalent to x^{2^s+1}. To see this, consider two cases depending on the value of i. First, suppose $i = 2$. Then

$$F(x) = wx^{2^s+1} + w^{2^k}x^{2^{2k}+2^{2k+s}} = wx^{2^s+1} + w^{2^k}(x^{2^s+1})^{2^{2k}}$$

which is EA-equivalent to x^{2^s+1} since $x \mapsto wx+w^{2^k}x^{2^{2k}}$ is a linear permutation. Indeed, suppose that $wx+w^{2^k}x^{2^{2k}} = wy+w^{2^k}y^{2^{2k}}$ for some two distinct elements $x, y \in \mathbb{F}_{2^n}$; then $(x+y)^{2^{2k}-1} = w^{1-2^k}$ which is a contradiction since the exponent on the left-hand side is a multiple of three, while the one on the right-hand side

is not. Finally, note that the derivatives of x^{2^s+1} are all 2^t-to-1 functions since $\gcd(s, 4k) = \gcd(s, 2k) = t$.

If $i = 0$, then

$$F(x) = wx^{2^s+1} + w^{2^k}x^{1+2^{4k+s}} = wx^{2^s+1} + w^{2^k}x^{1+2^s} = x^{2^s+1}\left(w + w^{2^k}\right),$$

which is EA-equivalent to x^{2^s+1} (as w is a primitive element, we have $w + w^{2^k} \neq 0$), and hence all of its derivatives are 2^t-to-1 under the conditions on s, t and k.

We now consider the case of i odd. Both possibilities for i produce functions in the same EA-equivalence class. For $i = 1$, the function (3) takes the form

$$F(x) = wx^{2^s+1} + w^{2^k}x^{2^k+2^{3k+s}}. \tag{4}$$

Consider the function F' defined by

$$F'(x) = F(x)^{2^{3k}} = \left(wx^{2^s+1} + w^{2^k}x^{2^k+2^{3k+s}}\right)^{2^{3k}} = wx^{2^{2k+s}+1} + w^{2^{3k}}x^{2^{3k}(2^s+1)}.$$

Clearly, F' is EA-equivalent to F. From the condition $ks = 1 \mod 4$ we get $k \mod 4 = s \mod 4$, i.e. $2k + s = 3s \mod 4$, hence $(2k + s)k = 3sk = 3 \mod 4$. Thus, denoting $2k + s$ by s', we get $F'(x) = wx^{2^{s'}+1} + w^{2^{-k}}x^{2^{3k}+2^{k+s'}}$, which is precisely the function from (3) for $i = 3$.

It is thus enough to prove the theorem for $i = 3$, i.e. for the function $F(x) = wx^{2^s+1} + w^{2^k}x^{2^{3k}+2^{k+s}}$.

The derivatives of F are 2^t-to-1 functions if and only if the equation $F(x) + F(x + v) = u$ has either 0 or 2^t solutions for any $u, v \in \mathbb{F}_2^n, v \neq 0$. The left-hand side of this equality takes the form

$$\begin{aligned}
&F(x) + F(x + v) = \\
&wx^{2^s+1} + w^{2^k}x^{2^{3k}+2^{k+s}} + w(x + v)^{2^s+1} + w^{2^k}(x + v)^{2^{3k}+2^{k+s}} = \\
&wx^{2^s+1} + w^{2^k}x^{2^{3k}+2^{k+s}} + wx^{2^s+1} + wv^{2^s+1} + wx^{2^s}v + wxv^{2^s} + w^{2^k}x^{2^{3k}+2^{k+s}} + \\
&w^{2^k}v^{2^{3k}+2^{k+s}} + w^{2^k}x^{2^{3k}}v^{2^{k+s}} + w^{2^k}v^{2^{3k}}x^{2^{k+s}} = \\
&wv^{2^s+1} + wx^{2^s}v + wxv^{2^s} + w^{2^k}v^{2^{3k}+2^{k+s}} + w^{2^k}x^{2^{3k}}v^{2^{k+s}} + w^{2^k}v^{2^{3k}}x^{2^{k+s}} = \\
&w^{2^k}v^{2^{3k}+2^{k+s}}\left(\left(\frac{x}{v}\right)^{2^{3k}} + \left(\frac{x}{v}\right)^{2^{k+s}}\right) + wv^{2^s+1}\left(\left(\frac{x}{v}\right)^{2^s} + \left(\frac{x}{v}\right)\right) + wv^{2^s+1} + \\
&w^{2^k}v^{2^{3k}+2^{k+s}}.
\end{aligned}$$

Dividing the last expression by wv^{2^s+1} and substituting vx for x, we get a linear expression in x:

$$a\left(x^{2^{3k}} + x^{2^{k+s}}\right) + \left(x^{2^s} + x\right) + 1 + a,$$

where $a = w^{2^k-1}v^{2^{3k}+2^{k+s}-(2^s+1)}$. So, $F(x) + F(x + v) = u$ has 0 or 2^t solutions if and only if the kernel of the linear map

$$\Delta_a(x) = a\left(x^{2^{3k}} + x^{2^{k+s}}\right) + \left(x^{2^s} + x\right)$$

has 2^t elements. Consider the equation $\Delta_a(x) = 0$. We use Dobbertin's multivariate method and follow the computations from Theorem 2 of [5]. Let $b = a^{2^k}$ and $c = b^{2^k}$. We get that

$$\Delta_a(x) = 0 \text{ if and only if } ab\Big(bc+1\Big)^{2^s+1}\Big(x^{2^{2s}} + x^{2^s}\Big) = 0,$$

assuming that $P(a) = c(ab+1)^{2^s+1} + a^{2^s}(bc+1)^{2^s+1} \neq 0$.

We now show that $bc + 1 \neq 0$. Clearly, $bc + 1 = 0$ if and only if $ab + 1 = 0$. Suppose $ab = 1$, i.e. $a^{2^k+1} = 1$. From

$$\Big(2^{3k} + 2^{k+s} - (2^s+1)\Big)\Big(2^k+1\Big) = (2^{2k}-1)(2^k+2^s) \mod (2^{4k}-1)$$

we get

$$1 = a^{2^k+1} = \Big(w^{2^k-1}v^{2^{3k}+2^{k+s}-(2^s+1)}\Big)^{2^k+1} = w^{2^{2k}-1}v^{(2^{2k}-1)(2^k+2^s)} = \Big(wv^{2^k+2^s}\Big)^{2^{2k}-1},$$

hence $wv^{2^k+2^s}$ is a $(2^{2k}+1)$-st power of an element from $\mathbb{F}_{2^n}$. On the other hand, from $ks = 3 \mod 4$ and $2 \nmid k$ we have that k and s are odd, and $k \neq s \mod 4$, which means that $k - s = 2p$ for some odd p. Thus, $2^k + 2^s = 2^s(2^{k-s}+1) = 2^s(2^{2p}+1)$. Since p is odd, we have $5 \mid 2^{2p}+1$, and therefore $u^{2^k+2^s}$ is the fifth power of an element of the field, while $wu^{2^k+2^s}$ is not. Thus $wu^{2^k+2^s}$ is also not a $(2^{2k}+1)$-st power. Hence, we get a contradiction, and so we must have $ab + 1 \neq 0$ and hence $bc + 1 \neq 0$. Therefore, we have

$$\Delta_a(x) = 0 \text{ if and only if } x^{2^{2s}} + x^{2^s} = 0$$

when $P(a) \neq 0$.

By the statement of Theorem 1, k is odd and $sk = 3 \mod 4$, so that s is also odd, and from $\gcd(s, 2k) = t$ it follows that $\gcd(s, 4k) = t$. Therefore the equation $x^{2^{2s}} + x^{2^s} = 0$, which is equivalent to $x^{2^s} = 1$, has exactly $2^{\gcd(s,4k)} = 2^t$ solutions.

So we only have to show that $P(a) = c(ab+1)^{2^s+1} + a^{2^s}(bc+1)^{2^s+1}$ does not vanish.

Assume $P(a) = 0$, i.e.

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

We have that $\frac{c}{a^{2^s}}$ is the third power of an element of the field since $3 \mid 2^s+1, 2^n-1$ (since s is odd and n is even). On the other hand,

$$\frac{c}{a^{2^s}} = a^{2^{2k}-2^s} = a^{2^s(2^{2k-s}-1)} = \Big(w^{2^k-1}v^{2^{3k}+2^{k+s}-(2^s+1)}\Big)^{2^s(2^{2k-s}-1)} = w^{(2^k-1)2^s(2^{2k-s}-1)}v^{(2^{3k}+2^{k+s}-(2^s+1))2^s(2^{2k-s}-1)}$$

and $2^{3k} + 2^{k+s} - (2^s + 1) = 2^s(2^{3k-s} - 1) + (2^{k+s} - 1)$ is divisible by 3 because $3 \mid 2^{3k-s} - 1$ and $3 \mid 2^{k+s} - 1$ due to k and s being odd. But since k and $2k - s$ are odd, we have $3 \nmid 2^k - 1$ and $3 \nmid 2^{2k-s} - 1$, which means that $w^{(2^k-1)2^s(2^{2k-s}-1)}$ is not a third power, therefore $\frac{c}{a^{2^s}}$ is not a third power either, and we get a contradiction.

As the following proposition illustrates, the binomials from (3) also behave in the same way as the Gold functions from the point of view of bijectivity.

Proposition 1. *A function of the form* (3) *is a permutation if and only if it is EA-equivalent to a* 2^t*-differentially uniform permutation of the form* x^{2^s+1} *for some positive integer* s*.*

Proof. Recall that the power function x^{2^s+1} over $\mathbb{F}_{2^n}$ is 2^t-uniform for some positive integer t if and only if $\gcd(s, n) = t$, and it is a permutation if and only if n/t is odd.

Let $F(x) = wx^{2^s+1} + w^{2^k}x^{2^{ik}+2^{mk+s}}$ be a function satisfying the conditions of Theorem 1. If F is a permutation, then $4k/\gcd(s, 4k)$ is odd. Indeed, assume that F is a permutation and $4k/\gcd(s, 4k)$ is even. Since k is odd, we have that $\gcd(s, 4k)$ should be odd or $\gcd(s, 4k) = 2 \mod 4$. If $\gcd(s, 4k)$ is odd, then so is s, and therefore $3 \mid 2^s + 1$. Since $i = (sk \mod 4)$ and s, k are odd, then i is an odd number, and hence $(m - i)k + s$ is also odd; hence $3 \mid 2^{ik}(1 + 2^{(m-i)k+s}) = 2^{ik} + 2^{mk+s}$. Thus, for any $\gamma \in \mathbb{F}_{2^2}$, we have $F(\gamma x) = F(x)$. On the other hand, if $\gcd(s, 4k) = 2 \mod 4$, then s is even, and therefore i is also even due to $i = sk \mod 4$. Hence, as we discussed in the proof of Theorem 1, F is EA-equivalent to x^{2^s+1} which is not a permutation since $4k/\gcd(s, 4k)$ is even. Therefore $4k/\gcd(s, 4k)$ is necessarily odd if F is a permutation. However, when $4k/\gcd(4k, s)$ is odd, $\gcd(4k, s)$ is divisible by 4, and therefore s is also divisible by 4 since k is odd. This means that F is EA-equivalent to a 2^t-differentially uniform permutation of the form x^{2^l+1} for some positive integer l.

4 Magnitude of the Walsh coefficients

In following theorem, we compute an upper bound on the absolute values of the Walsh coefficients of the functions from (3). In the proof we make use of the following result.

Lemma 1 ([14]). *Let* n, l, d *be positive integers such that* $\gcd(n, s) = 1$ *and let* $G(x) = \sum_{i=0}^{d} a_i x^{li} \in \mathbb{F}_{2^n}[x]$*. Then the equation* $G(x) = 0$ *has at most* 2^d *solutions.*

We are now ready to present the main result of this section.

Theorem 2. *Let* s, k, t *be positive integers and let* $n = 4k$*. Let* $\gcd(s, 2k) = t$*,* $2 \nmid k$*,* $i = sk \mod 4$*,* $m = 4 - i$ *and let* w *be a primitive element of* $\mathbb{F}_{2^n}$*. Then the Walsh coefficients of the function* F *from* (3) *satisfy*

$$|W_F(a, b)| \leq 2^{2k+t}$$

for any $a \in \mathbb{F}_{2^n}^*$ *and* $b \in \mathbb{F}_{2^n}$*.*

Proof. For simplicity, instead of $F(x) = wx^{2^s+1} + w^{2^k}x^{2^{ik}+2^{mk+s}}$, we consider the EA-equivalent function $F'(x) = x^{2^s+1} + \alpha x^{2^{ik}+2^{mk+s}}$, where $\alpha = w^{2^k-1}$.

We are going to prove the theorem for $i = 3$, since as we already observed in the proof of Theorem 1, if i is even, the function $F(x)$ is EA-equivalent to a Gold-like differentially 2^t-uniform function; and if i is odd, the functions that we obtain for $i = 1$ and for $i = 3$ are EA-equivalent.

We have

$$W^2_{F'}(a,b) = \sum_x \sum_y (-1)^{\mathrm{Tr}(ax+ay+bF'(x)+bF'(y))}.$$

Substituting $x + y$ for y, we get

$$W^2_{F'}(a,b) = \sum_x \sum_y (-1)^{\mathrm{Tr}(ax+a(x+y)+bF'(x)+bF'(x+y))}.$$

By straightforward calculations, the exponent from the previous expression becomes

$$\begin{aligned}
&\mathrm{Tr}\Big(ax + a(x+y) + bF'(x) + bF'(x+y)\Big) = \\
&\mathrm{Tr}\Big(ay + b\Big(x^{2^s+1} + \alpha x^{2^{3k}+2^{k+s}} + (x+y)^{2^s+1} + \alpha(x+y)^{2^{3k}+2^{k+s}}\Big)\Big) = \\
&\mathrm{Tr}\Big(ay + by^{2^s+1} + b\alpha y^{2^{k+s}+2^{3k}}\Big) + \mathrm{Tr}\Big(bx^{2^s}y + bxy^{2^s} + b\alpha x^{2^{3k}}y^{2^{k+s}} + b\alpha y^{2^{3k}}x^{2^{k+s}}\Big) = \\
&\mathrm{Tr}\Big(ay + by^{2^s+1} + b\alpha y^{2^{k+s}+2^{3k}}\Big) + \mathrm{Tr}(x\mathcal{L}(y)),
\end{aligned}$$

where $\mathcal{L}(y) = (by)^{2^{-s}} + by^{2^s} + (b\alpha)^{2^{-3k}}y^{2^{s-2k}} + (b\alpha)^{2^{3k-s}}y^{2^{2k-s}} = (by)^{2^{-s}} + by^{2^s} + (b\alpha)^{2^{2k}}y^{2^{s+2k}} + (b\alpha)^{2^{3k-s}}y^{2^{2k-s}}$ is a linear function.

Thus

$$W^2_{F'}(a,b) = 2^n \sum_{\{y|\mathcal{L}(y)=0\}} (-1)^{\mathrm{Tr}(ay+by^{2^s+1}+b\alpha y^{2^{k+s}+2^{3k}})}.$$

The next step is to show that the cardinality of the kernel of $\mathcal{L}(y)$ is at most 2^{2t}, where $t = \gcd(2k, s)$. Following the computations of [2], we have

$$b^{2^{-s+2k}}\mathcal{L}(y) + (b\alpha)^{2^{3k-s}}\mathcal{L}^{2^{2k}}(y) = 0 \text{ and } b^{2^{2k}}\mathcal{L}(y) + (b\alpha)^{2^k}\mathcal{L}^{2^{2k}}(y) = 0,$$

from where we get

$$Ay^{2^s} + By^{2^{-s}} + Cy^{2^{s+2k}} = 0, \tag{5}$$

$$B^{2^s}y^{2^s} + A^{2^{2k}}y^{2^{-s}} + Cy^{2^{-s+2k}} = 0, \tag{6}$$

where

$$\begin{aligned}
A &= b^{2^{-s+2k}+1} + (b\alpha)^{2^{-k}+2^{3k-s}} \neq 0, \\
B &= b^{2^{-s}+2^{-s+2k}} + (b\alpha)^{2^{k-s}+2^{3k-s}}, \text{ and} \\
C &= b^{2^{-s+2k}+2^k}\alpha^{2^k} + b^{2^{2k}+2^{3k-s}}\alpha^{2^{3k-s}} \neq 0,
\end{aligned}$$

with $B = 0$ if and only if B^{2^s-1} is a cube.

Assume that $B \neq 0$, i.e. B^{2^s-1} is not a cube. Then from (5) and (6) we get

$$B^{2^{2s}}C^{2^{-s}}y^{2^{2s}} + C^{2^{-s}}A^{2^{2k+s}}y + B^{2^{-s}}C^{2^s}y^{2^{-2s}} + A^{2^{-s}}C^{2^s}y = 0.$$

Denote the last expression by $G(y)$. For some $v \neq 0$ in the kernel of $G(y)$, consider the expression $G_v(y) = yG(y) + vG(v) + (y+v)G(y+v)$, i.e.

$$C^{2^s}B^{2^{-s}}\left(y^{2^{-2s}}v + v^{2^{-2s}}y\right) + C^{2^{-s}}B^{2^{2s}}\left(y^{2^{2s}}v + v^{2^{2s}}y\right).$$

Note that the kernel of $\mathcal{L}(y)$ is contained in that of $G_v(y)$. Then from $G_v(y) = 0$ we get

$$C^{2^{-s}-2^s}B^{2^{2s-1}}\left(y^{2^{-2s}}v + v^{2^{-2s}}y\right)^{2^{2s}-1} = B^{2^s-1}.$$

If $y^{2^{-2s}}v + v^{2^{-2s}}y = 0$, i.e. $yv^{-1} = (yv^{-1})^{2^{2s}}$, then $yv^{-1} \in \mathbb{F}_{\gcd(2s,4k)} = \mathbb{F}_{2^{2t}}$ and therefore $\mathcal{L}(y) = 0$ has exactly 2^{2t} solutions. Otherwise, if $y^{2^{-2s}}v + v^{2^{-2s}}y$ does not vanish, then the right-hand side of the previous equation is not a cube by our assumption, while the left-hand side is. Hence, $\mathcal{L}(y) = 0$ has exactly 2^{2t} solutions, where $t = \gcd(2k, s)$.

Suppose now that $B = 0$. Following the computations of [2], the equation $\mathcal{L}(y) = 0$ becomes

$$\left(b + (bw)^{2^k}v^{2^{2k+s}-2^s}\right)y^{2^s} + \left(b^{2^{-s}} + (bw)^{2^{3k-s}}v^{2^{2k-s}-2^{-s}}\right)y^{2^{-s}} = 0.$$

If both coefficients (in front of y^{2^s} and in front of $y^{2^{-s}}$) in the above equation are nonzero, then raising both sides to the power 2^s, we get

$$\left(b + (bw)^{2^k}v^{2^{2k+s}-2^s}\right)^{2^s}y^{2^{2s}} + \left(b^{2^{-s}} + (bw)^{2^{3k-s}}v^{2^{2k-s}-2^{-s}}\right)^{2^s}y = 0.$$

Note that $2s = 2t\frac{s}{t}$ and $\gcd(\frac{s}{t}, 4k) = 1$. Then, applying Lemma 1, we get that $\mathcal{L}(y) = 0$ has at most 2^{2t} solutions. If exactly one of the coefficients is not zero, then the equation will have exactly one solution, namely $y = 0$. If both coefficients are equal to zero, then raising them to the power of 2^s and of 2^{-s}, and adding these powers together, we get $v^{2^{2k}-1} = b^{2^{3k}-2^{k-s}}w^{-2^{k-s}} = b^{1-2^{3k}}w^{-2^{3k}}$ which implies $C = 0$, a contradiction.

Thus, the kernel of $\mathcal{L}(y)$ consists of at most 2^{2t} elements, where $t = \gcd(2k, s)$, and therefore $|W_F^2(a, b)| \leq 2^n 2^{2t}$ and $|W_F(a, b)| \leq 2^{2k+t}$.

The next corollary immediately follows from Theorem 2.

Corollary 1. *Let s, k, t be positive integers and let $n = 4k$. Let $\gcd(s, 2k) = t$, $2 \nmid k$, $i = sk \mod 4$, $m = 4 - i$ and let w be a primitive element of $\mathbb{F}_{2^n}$. Then the nonlinearity of the function F from (3) satisfies*

$$\mathcal{NL}(F) \leq 2^{n-1} - 2^{2k+t-1}.$$

5 A counterexample: generalizing a family of APN quadrinomials to 2^t-uniform functions

As discussed above, both families of APN binomials from [5] can be generalized to functions all of whose derivatives are 2^t-to-1 by relaxing conditions; furthermore, the two families are obtained as generalizations of a previously unclassified sporadic APN instance over $\mathbb{F}_{2^{12}}$. Another sporadic APN instance, this time over $\mathbb{F}_{2^{10}}$, was recently also generalized into an infinite family [7]. This immediately raises the question of whether the same approach, i.e. relaxing conditions in order to obtain functions with 2^t-to-1 derivatives, could be applied to the latter family. In this section, we summarize our experimental results, which suggest that this is impossible.

The functions in the infinite family from [7] are defined over $\mathbb{F}_{2^n}$ with $n = 2m$ with m odd such that $3 \nmid m$, and have the form

$$F(x) = x^3 + \beta(x^{2^i+1})^{2^k} + \beta^2(x^3)^{2^m} + (x^{2^i+1})^{2^{m+k}}, \tag{7}$$

where k is a non-negative integer, and β is a primitive element of $\mathbb{F}_{2^2}$. It is shown that the function in (7) is APN for $i = m-2$ and $i = (m-2)^{-1} \mod n$, as well as for $i = m$ and $i = m-1$ (however, the last two values yield functions that are trivially EA-equivalent to known ones).

We computationally go through all functions of the form

$$F(x) = x^{2^j+1} + \beta(x^{2^i+1})^{2^k} + \beta^2(x^{2^j+1})^{2^m} + (x^{2^i+1})^{2^{m+k}} \tag{8}$$

with $0 \leq i, j \leq n-1$ for all values of $n = 2m$ with $6 \leq n \leq 14$, disregarding the conditions of $3 \nmid m$ and of m being odd. For each such function, we test whether all of its derivatives are 2^t-to-1 functions for some positive integer t. We restrict ourselves to the cases $k = 0$ and $k = 1$, as the APN functions constructed for $k \in \{0, 1\}$ appear to exhaust all CCZ-equivalence classes [7].

Besides the already known APN functions, for $k = 0$, we only encounter functions with 2^t-to-1 derivatives when $j = i$, i.e. when all exponents are in the same cyclotomic coset. In the case of $k = 1$, the only exceptions are for $n = 12$ where each pair (j, i) with $2 \leq j, i \leq 12$ and i, j even yields a 2^2-to-1, i.e. 4-to-1 function. However, since we do not observe other such non-trivial functions for other dimensions n, this does not suggest that (7) can be generalized to 2^t-functions in general.

These computational results constitute convincing evidence that the quadrinomials of the form (7) cannot be generalized to 2^t-to-1 functions in the same way as the binomials from [5].

6 Conclusion

The APN binomial $x^3 + \alpha x^{258}$ over $\mathbb{F}_{2^{12}}$ was generalized in 2008 to two infinite APN families over $\mathbb{F}_{2^n}$, one for $3 \mid n$, and one for $4 \mid n$. The family for $3 \mid n$ was generalized to a family of functions with 2^t-to-1 derivatives in 2012 [3] by

relaxing conditions. We have shown that the same approach can be applied to the family for $4 \mid n$, and have computed the differential uniformity of the resulting functions. We have also given an upper bound on their nonlinearity, and have shown that this construction cannot be applied to any infinite family of quadratic APN functions by computationally verifying that the quadrinomial family from [7] constitutes a counterexample.

Acknowledgment

This research was supported by the Trond Mohn foundation (TMS).

References

1. Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems, J. Cryptol., vol. 4, no. 1, pp. 3–72 (1991).
2. Bracken, C., Byrne, C., Markin, N., Mcguire, G.: Fourier spectra of binomial APN functions, SIAM J., Discrete Math., vol. 23, no. 2, pp. 596–608 (2009).
3. Bracken, C., Tan, C., Tan Y.: Binomial differentially 4 uniform permutations with hight nonlinearity, Finite Fields and Their Applications, 18, pp. 537–546 (2012).
4. Budaghyan, L.: Construction and Analysis of Cryptographic Functions, Springer Verlag (2015).
5. Budaghyan, L., Carlet, C., Leander G.: Two classes of quadratic APN binomials inequivalent to power functions, IEEE Transactions on Information Theory, vol. 54, no. 9, pp. 4218-4229 (2008).
6. Budaghyan, L., Carlet, C., Pott, A.: New classes of almost bent and almost perfect nonlinear functions, IEEE Trans. Inform. Theory, vol.52, no.3, pp.1141–1152 (2006).
7. Budaghyan, L., Helleseth, T., Kaleyski, N.: A new family of APN quadrinomials, IEEE Trans. Inform. Theory, 2020, early access article.
8. Carlet, C.: Vectorial (multi-output) Boolean Functions for Cryptography, Chapter of the monography *Boolean Methods and Models*, In: Crama Y., and Hammer P. (eds), Cambridge University Press, to appear soon. Preliminary version available at http://www-rocq.inria.fr/codes/Claude.Carlet/pubs.html
9. Carlet, C., Charpin, P., Zinoviev, V.: Codes, bent functions and permutations suitable for DES-like cryptography, Design, Codes and Cryptography, vol. 15, no. 2, pp.125–156 (1998).
10. Chabaud, F., Vaudenay, S.: Links between differential and linear cryptanalysis, Advances in Cryptology, Eurocrypt'94, In: Lecture Notes in Comput.Sci., vol. 950, pp. 356–365 (1995).
11. Edel, Y., Kyureghyan, G., Pott, A.: A new APN function which is not equivalent to a power mappings, IEEE Trans. Inf. Theory, vol. 52, no.2, pp. 744–747 (2006).
12. Matsui, M.: Linear cryptanalysis methods for DES cipher, Advances in Cryptology, Eurocrypt'93, In: Lecture Notes in Comput.Sci., vol. 765, pp. 386–397 (1993).
13. Nyberg, K.: Differentially uniform mappings for cryptography, Eurocrypt'93, In: Lecture Notes in Comput.Sci., vol.765, pp. 55-64 (1994).
14. Trachtenberg, H. M.: On the Cross–Correlation Functions of Maximal Linear Sequences , Ph.D. dissertation, University of Southern California, Los Angeles (1970).