Componentwise APNness, Walsh uniformity of APN functions and cyclic-additive difference sets

Claude Carlet

LAGA, Department of Mathematics, University of Paris 8
(and Paris 13 and CNRS), Saint–Denis cedex 02, France.
E-mail: claude.carlet@univ-paris8.fr

Abstract. In the preprint [Characterizations of the differential uniformity of vectorial functions by the Walsh transform, IACR ePrint Archive 2017/516], the author has, for each even positive δ, characterized in several ways differentially δ-uniform functions by equalities satisfied by their Walsh transforms. These characterizations generalize the well-know characterization of APN functions by the fourth moment of their Walsh transform. We introduce two notions which are related to these characterizations: (1) that of componentwise APN (CAPN) (n,n)-function, which is a stronger version of APNness related to the characterization by the fourth moment, and is defined as follows: the arithmetic mean of $W_F^4(u,v)$ when u ranges over $\mathbb{F}_2^n$ and v is fixed nonzero in $\mathbb{F}_2^n$ equals 2^{2n+1}, and (2) that of componentwise Walsh uniform (CWU) (n,m)-function ($m=n$, resp. $m=n-1$), which is a stronger version of APNness (resp. of differential 4-uniformity) related to one of the new characterizations, and is defined as follows: the arithmetic mean of $W_F^2(u_1,v_1)W_F^2(u_2,v_2)W_F^2(u_1+u_2,v_1+v_2)$ when u_1,u_2 range independently over $\mathbb{F}_2^n$ and v_1,v_2 are fixed nonzero and distinct in $\mathbb{F}_2^m$, equals 2^{3n}. We observe that CAPN functions can exist only if n is odd, that every plateaued function is CAPN if and only if it is AB and that APN power permutations are CAPN. We show that any APN function whose component functions are partially-bent (in particular, every quadratic APN function) is CWU, but we show also that other APN functions like Kasami functions and the inverse of one of the Gold APN permutations are CWU. To prove these two more difficult results, we first show that the CWUness of APN power permutations is equivalent to a property which is similar to the difference set with Singer parameters property of the complement of $\Delta_F=\{F(x)+F(x+1)+1; x\in\mathbb{F}_{2^n}\}$, proved in the case of Kasami APN functions by Dillon and Dobbertin in [New cyclic difference sets with Singer parameters, FFA 2004]. This new property, that we call cyclic-additive difference set property, involves both operations of addition and multiplication and is more complex. We prove it in the case of the inverse of Gold function. In the case of Kasami functions, it seems difficult to find a direct proof, even by adapting the sophisticated proof by Dillon and Dobbertin of the cyclic difference set property. But the properties of plateaued APN functions proved recently by the author in [Boolean and vectorial plateaued functions, and APN functions, IEEE Transactions on Information Theory 2015] allow proving that, for APN power functions, the cyclic-additive difference set property is equivalent to the cyclic difference set property. The case n odd is then solved, but not the case n even since, in such case, F is not a permutation. Stronger properties proved in this same paper for the particular case of plateaued functions with unbalanced components allow proving in the same time that APN Kasami functions in even dimension are CWU and that their associated set Δ_F has the cyclic-additive difference set property. This provides as a side result a simple alternative proof of the difference set property with Singer parameters of the complement of the set Δ_F related to a Kasami APN function F in even dimension, since it is known that these functions are plateaued.

Keywords: Boolean function, vectorial function, Walsh–Hadamard transform, APN function, Kasami function, cyclic difference set.

1 Introduction

APN functions are those (n,n)-functions from the vector space $\mathbb{F}_2^n$ to itself (which can be identified with the field $\mathbb{F}_{2^n}$ since this field is an n-dimensional vector space over $\mathbb{F}_2$; this allows to define power functions $F(x)=x^d$), which contribute to an optimal resistance against the differential cryptanalyses of those block ciphers involving them as substitution boxes. The differential uniformity of a vectorial function $F:\mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ is the number $\delta_F = \max_{a\in\mathbb{F}_2^n, b\in\mathbb{F}_2^m, a\neq 0} |\{x\in\mathbb{F}_2^n; F(x)+F(x+a)=b\}|$. Function F is then called a differentially δ_F-uniform function. The best (minimal) value of δ_F when $m=n$ is 2. The function is then called almost perfect nonlinear (APN). A subclass of APN functions for n odd is that of almost bent (AB) (n,n)-functions, whose Walsh transform:

$$W_F(u,v)=\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)+u\cdot x}$$

(some inner products, both denoted by " $\cdot$ ", being chosen in $\mathbb{F}_2^n$ and $\mathbb{F}_2^m$) takes values 0 and $\pm 2^{\frac{n+1}{2}}$ only. Equivalently, AB functions are those (n,n)-functions whose component functions $v\cdot F$, $v\neq 0$, all lie at optimal Hamming distance $2^{n-1}-2^{\frac{n-1}{2}}$ from the set of affine functions. Any quadratic APN function in odd dimension n is AB (quadratic meaning that all the derivatives $D_aF(x)=F(x)+F(x+a)$ are affine). Surveys on APN and AB functions can be found in [1, 5]. Note that all known APN functions are given by expressions in the field $\mathbb{F}_{2^n}$. The inner product in this field can be taken equal to $u\cdot x = tr_1^n(ux)$, where tr_1^n is the absolute trace function $tr_1^n(x)=x+x^2+x^{2^2}+\cdots+x^{2^{n-1}}$.

In [7], the author has characterized differentially δ-uniform (n,m)-functions by equalities involving the values of their Walsh transform. For $\delta=2$, this characterization is by the fourth moment of the Walsh transform and is well-known: every (n,n)-function is APN if and only if:

$$\sum_{u,v\in\mathbb{F}_2^n; v\neq 0} W_F^4(u,v)=2^{3n+1}(2^n-1). \tag{1}$$

But for $\delta\geq 4$, the characterization is new. In fact, more than one characterization could be derived for each even value of $\delta\geq 2$. One of them is particularly interesting. It characterizes when $m=n-1$ the case $\delta=4$ (which is optimal for $m=n-1$) and the same characterization (up to a change of constant) happens to be also valid when $m=n$ for $\delta=2$ (also optimal):

Theorem 1.1 *[7] Every (n,n)-function F is APN if and only if:*

$$\sum_{\substack{u_1,u_2\in\mathbb{F}_2^n; v_1,v_2\in\mathbb{F}_2^m \\ v_1\neq 0, v_2\neq 0, v_1\neq v_2}} W_F^2(u_1,v_1)W_F^2(u_2,v_2)W_F^2(u_1+u_2,v_1+v_2)=2^{5n}(2^n-1)(2^n-2). \tag{2}$$

Theorem 1.2 *[7] Every $(n, n-1)$-function F is differentially 4-uniform if and only if:*

$$\sum_{\substack{u_1,u_2\in\mathbb{F}_2^n; v_1,v_2\in\mathbb{F}_2^m \\ v_1\neq 0, v_2\neq 0, v_1\neq v_2}} W_F^2(u_1,v_1)W_F^2(u_2,v_2)W_F^2(u_1+u_2,v_1+v_2) = 2^{5n}(2^{n-1}-1)(2^{n-1}-2). \tag{3}$$

In the present paper, we introduce two notions on (n, m)-functions. The first one is called componentwise APNness (CAPNness) and corresponds to a version of the characterization when $m = n$ of APN functions by Relation (1), in which the value on the left hand side is the same for every component function (i.e. the same when fixing v to any nonzero value). The second one is called componentwise Walsh uniformity (CWU) and corresponds to a version of the characterization when $m = n$ (resp. $m = n - 1$) of APN (resp. differentially 4-uniform) functions by Theorem 1.1 (resp. 1.2) in which the value on the left hand side is the same for every choice of two distinct component functions (i.e. the same when fixing $v_1 \neq 0$ and $v_2 \neq 0$ such that $v_1 \neq v_2$). The former property (CAPNness) implies APNness and we observe that it is shared by AB functions and power APN permutations (and then by all known APN functions in odd dimension). We also derive a characterization by character sums and deduce that CAPNness can be satisfied only for n odd; we leave open the determination of all CAPN functions and the related questions of determining if there exist CAPN functions which are neither AB nor power permutations, and APN functions in odd dimension which are not CAPN. The latter property (CWUness) implies APNness in the case of (n, n)-functions, and differential 4-uniformity in the case of $(n, n - 1)$-functions. We study those (n, n)-functions which are CWU. We show that all quadratic APN functions and more generally all APN functions whose component functions are partially-bent (definition recalled in Proposition 4.6) are CWU. We give a table for n between 3 and 11 of all the main known classes of non-quadratic APN functions, indicating if they are CWU. We observe in this table that most known APN functions are not CWU but, for $n \leq 11$, the compositional inverse of Gold function $x^{2^{\frac{n-1}{2}}+1}$ (n odd) is CWU (while its component functions are not all partially-bent) and all Kasami (also called Welch-Kasami) APN functions $F(x) = x^{4^i-2^i+1}$, $gcd(i, n) = 1$, are CWU while their components are not all partially-bent. Kasami APN functions are sometimes considered as behaving similarly to quadratic functions, even if they are not quadratic. For n odd, they have the form $G' \circ G^{-1}$ where G and G' are quadratic permutations and this property close to the CCZ-equivalence [9, 2] with quadratic functions has an incidence on the Walsh support, that is, on the positions where the Walsh transform takes values $\pm 2^{\frac{n+1}{2}}$. For n even, the similarity with quadratic functions is looser but, in both cases, Kasami functions are plateaued [20], that is, have Walsh transform $W_F(u, v)$ valued for every v in a set of the form $\{0, \pm\lambda_v\}$, like quadratic functions. The main results of this paper consist in proving that, for every odd n, the compositional inverse of Gold function $x^{2^{\frac{n-1}{2}}+1}$ is CWU and that, whatever is n, all Kasami APN functions are CWU. All

the other known (infinite classes of) non-quadratic power APN functions are not CWU for some (probably almost all) values of n.

In order to address the inverse of the Gold function above and Kasami APN permutations, we show that the CWU property of APN power pemutations is equivalent to a notion similar to the "cyclic difference set with Singer parameters property" proved by Dillon and Dobbertin [13] for the complement of the set $\Delta_F = \{F(x) + F(x+1) + 1; x \in \mathbb{F}_{2^n}\}$, but more complex since instead of involving only multiplication, it involves both multiplication and addition (see Definition 4.12). We call it the "cyclic-additive difference set with Singer-like parameters property". We prove it for the compositional inverse of the Gold function above (our proof is obtained by direct but complex calculations on character sums). In the case of Kasami functions, Dillon and Dobbertin's proof of the difference set with Singer parameters property for these functions is deduced from a sophisticated and elegant calculation of the Fourier transform of the indicator of the set $D_F = \{x^{\frac{1}{2^i+1}}; x \in \Delta_F\}$. It seems impossible to prove the cyclic-additive property by the same mean, but a result from [6], general to all plateaued (n,m)-functions, allows us to show that, for any plateaued power APN function, the cyclic-additive difference set property is equivalent to the cyclic difference set property. This solves the case of Kasami APN functions in odd dimension. For n even, the equivalence between CWU and cyclic-additive difference set property does not seem to be valid and another method is needed. A stronger result from [6], valid for those plateaued functions whose component functions are all unbalanced, allows us to show that all plateaued APN power functions are CWU and that the related sets Δ_F have the cyclic-additive difference set with Singer-like parameters property. This and the equivalence for plateaued APN power functions of the cyclic-additive difference set and cyclic difference set properties (which is valid also for n even) give a simple alternative proof to Dillon-Dobbertin's result. It suggests also that the situations when n is odd and n is even are of a probably different nature. All these results address the CWU property for (n,n)-functions. To partly address the case of $(n,n-1)$-functions, we show that if F is a CWU (n,n)-function and L is a surjective affine $(n,n-1)$-function, then $L \circ F$ is CWU, and more generally if F is a CWU (n,m)-function and L is a surjective affine (m,k)-function, then $L \circ F$ is CWU. This shows the existence of CWU $(n,n-1)$-functions; we leave open the search for other examples. We complete our paper with a conclusion which lists thirteen open questions raised by our results.

2 Preliminaries

For every vectorial (n,m)-function $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ (where $\mathbb{F}_2^n$ and $\mathbb{F}_2^m$ may be endowed with the field structure), we define $\delta_F = \max_{a \in \mathbb{F}_2^n, a \neq 0, z \in \mathbb{F}_2^m} |\{x \in \mathbb{F}_2^n; F(x) + F(x+a) = z\}|$, called the differential uniformity of F, and F is called *differentially δ-uniform*, see [18], if $\delta_F \leq \delta$. Such functions exist only if $\delta \geq 2^{n-m}$. Differentially 2^{n-m}-uniform (n,m)-functions, which are optimal with respect to differential uni-

formity, are called *perfect nonlinear* (PN). These functions are the same as bent (vectorial) functions, and exist if and only if n is even and $m \leq n/2$ (see [17]). For $m = n$, differentially 2-uniform functions are optimal and are called *almost perfect nonlinear* (APN). An (n, m)-function is called *plateaued* if, for every nonzero $v \in \mathbb{F}_2^m$, there exists a positive integer λ_v (called the *amplitude* of the component function $v \cdot F$) such that, for every $u \in \mathbb{F}_2^n$, the Walsh transform value $W_F(u, v)$ (whose definition has been recalled in introduction) belongs to $\{0, \pm\lambda_v\}$. Then λ_v is necessarily a power of 2 whose exponent is larger than or equal to $\frac{n}{2}$. An (n, n)-function is called *almost bent* (AB) if it is plateaued with the single amplitude $\lambda_v = 2^{\frac{n+1}{2}}$, $\forall v \neq 0$ (n odd). Another sub-class of the class of plateaued functions (which neither includes all AB functions nor, for n odd, is made of AB functions only) is that of those vectorial functions whose component functions $v \cdot F$, $v \neq 0$, are all partially-bent. A Boolean function f is called partially-bent if all its derivatives $D_a f(x) = f(x) + f(x + a)$, $a \neq 0$, are either constant or balanced, see [4]. Quadratic Boolean functions (that is, functions whose algebraic normal form $\sum_{I \subseteq \{1,\ldots,n\}} a_I \prod_{i \in I} x_i$; $a_I, x_i \in \mathbb{F}_2$, has degree at most 2, i.e. whose derivatives are all affine, or equivalently whose univariate polynomial representation $\sum_{i=0}^{2^n-1} a_i x^i$, $a_i, x \in \mathbb{F}_{2^n}$, has exponents with binary expansion of Hamming weight at most 2 when their coefficients are nonzero) are partially-bent. Quadratic vectorial functions (which have same definition, with $a_I \in \mathbb{F}_2^m$ instead of $\mathbb{F}_2$) are then a particular case of those vectorial functions whose components are partially-bent (since their components are quadratic). Characterizations of plateaued functions are given in [6, 15].

The Sidelnikov-Chabaud-Vaudenay (SCV) bound [11] states in the case $m = n$ that the nonlinearity $nl(F) = 2^{n-1} - \frac{1}{2} \max_{u \in \mathbb{F}_2^n, v \in \mathbb{F}_2^m, v \neq 0} |W_F(u, v)|$ of an (n, n)-function (which equals the minimum Hamming distance between all component functions and all affine Boolean functions over $\mathbb{F}_2^n$) is at most $2^{n-1} - 2^{\frac{n-1}{2}}$. This bound is tight for n odd. The functions which achieve it with equality are called AB functions. For every AB function and every $v \neq 0$, there are 2^{n-1} elements u such that $W_F^2(u, v) = 2^{n+1}$ and 2^{n-1} elements u such that $W_F^2(u, v) = 0$. This is a consequence of the Parseval relation (valid for any Boolean function f): $\sum_{u \in \mathbb{F}_2^n} W_f^2(u) = 2^{2n}$ (where $W_f(u) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+u \cdot x}$).

We shall need in proofs to use the *Fourier transform* $\widehat{\varphi}(a) = \sum_{x \in \mathbb{F}_2^n} \varphi(x)(-1)^{a \cdot x}$ of numerical functions φ over $\mathbb{F}_2^n$ and to apply the *inverse Fourier transform formula* $\sum_{a \in \mathbb{F}_2^n} \widehat{\varphi}(a)(-1)^{a \cdot b} = 2^n \varphi(b)$, for $b \in \mathbb{F}_2^n$, which shows that the Fourier transform is injective. In the case of a 2-variable function $\varphi(x, y)$ defined over $\mathbb{F}_2^n \times \mathbb{F}_2^m$, we have $\widehat{\varphi}(a, b) = \sum_{(x,y) \in \mathbb{F}_2^n \times \mathbb{F}_2^m} \varphi(x, y)(-1)^{a \cdot x + b \cdot y}$ and, for every $(c, d) \in \mathbb{F}_2^n \times \mathbb{F}_2^m$, $\sum_{(a,b) \in \mathbb{F}_2^n \times \mathbb{F}_2^m} \widehat{\varphi}(a, b)(-1)^{a \cdot c + b \cdot d} = 2^{n+m} \varphi(c, d)$. Note that in the case of a Boolean function f defined over $\mathbb{F}_2^n$, we have $\widehat{f}(a) = 2^{n-1} \delta_0(a) - \frac{1}{2} W_f(a)$, where δ_0 is the Dirac symbol.

Two functions are called *affine equivalent* if one is equal to the other, composed on the left and on the right by affine permutations (in the case of Boolean functions, it is enough to compose on the right only). More generally, they are called

extended affine equivalent (EA-equivalent) if one is affine equivalent to the other, added with an affine function. Still more generally, they are called *CCZ-equivalent* if their graphs $\{(x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \,|\, y = F(x)\}$ and $\{(x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \,|\, y = G(x)\}$ are affine equivalent, that is, if there exists an affine automorphism $A = (A_1, A_2)$ of $\mathbb{F}_2^n \times \mathbb{F}_2^n$ such that $y = F(x) \Leftrightarrow A_2(x, y) = G(A_1(x, y))$. A notion or a parameter is called EA-invariant (resp. CCZ-invariant) if it is preserved by EA equivalence (resp. CCZ equivalence). ABness, APNness and plateauedness with a single amplitude are CCZ-invariant. In particular, the compositional inverse of an APN (resp. AB) permutation is APN (resp. AB). The algebraic degree (the degree of the algebraic normal form, or equivalently, the maximum Hamming weight of exponents in the univariate representation of the function, see e.g. [5]) and plateauedness with several amplitudes are only EA-invariant.
Most known APN functions are power functions $F(x) = x^d$ over $\mathbb{F}_{2^n}$. Table 1 below gives all known values of exponents d such that the function x^d over $\mathbb{F}_{2^n}$ is APN (up to multiplying d by a power of 2 modulo $2^n - 1$, and to taking its inverse when it is co-prime with $2^n - 1$, that is, when the power function is a permutation). For n odd the Gold, Kasami, Welch and Niho APN functions from Table 1 are also AB.

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

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

3 Componentwise APNness

If we fix v to any nonzero value in the characterization of APN functions given by Relation (1), we obtain a notion which is more demanding than APNness. As far as we known, this rather natural notion has never been addressed in the literature.

Definition 3.1 *Let n be any positive integer and F any (n, n)-function. We call F* componentwise APN *(CAPN) if, given any nonzero v, its Walsh transform satisfies the equality:*

$$\sum_{u \in \mathbb{F}_2^n} W_F^4(u, v) = 2^{3n+1}. \tag{4}$$

Of course, we have:

$$\sum_{u\in\mathbb{F}_2^n} W_F^4(u,v) = 2^n \sum_{x,y,z\in\mathbb{F}_2^n} (-1)^{v\cdot(F(x)+F(y)+F(z)+F(x+y+z))}$$
$$= 2^n \sum_{a\in\mathbb{F}_2^n} \left(\sum_{x\in\mathbb{F}_2^n} (-1)^{v\cdot D_a F(x)} \right)^2 .$$

We observe that those CAPN plateaued functions are precisely the AB functions, since for a plateaued function F, denoting again by λ_v the amplitude of $v\cdot F$, we have according to Parseval's relation that $\sum_{u\in\mathbb{F}_2^n} W_F^4(u,v) = \lambda_v^2 \sum_{u\in\mathbb{F}_2^n} W_F^2(u,v) = 2^{2n}\lambda_v^2$ equals 2^{3n+1} if and only if $\lambda_v = 2^{\frac{n+1}{2}}$.
We also observe that if F is a power permutation, that is, identifying $\mathbb{F}_2^n$ with $\mathbb{F}_{2^n}$, if $F(x) = x^d$ for every $x \in \mathbb{F}_{2^n}$, where $(d, 2^n-1) = 1$, and if F is APN (equivalently, as shown by Dobbertin, if F is a power APN function and n is odd), then F is CAPN because, for every nonzero $\lambda \in \mathbb{F}_{2^n}$, we have $W_F(\lambda u, \lambda^d v) = W_F(u,v)$ and λ^d ranges over the whole multiplicative group $\mathbb{F}_{2^n}^*$. Hence, we have the easy:

Proposition 3.2 *Every plateaued function is CAPN if and only if it is AB. Every APN power permutation is CAPN.*

Recall that F is APN if and only if the size $|\{(x,y,z) \in \mathbb{F}_2^n;\ F(x)+F(y)+F(z)+F(x+y+z)=0\}|$ equals $3\cdot 2^{2n} - 2^{n+1}$. We have:

Proposition 3.3 *Let n be any positive integer and F any (n,n)-function. Then F is CAPN if and only if, for every $w \neq 0$, we have:*

$$|\{(x,y,z) \in \mathbb{F}_2^n;\ F(x)+F(y)+F(z)+F(x+y+z)=w\}| = 2^{2n} - 2^{n+1}.$$

Proof. Function F is CAPN if and only if, for every $v \in \mathbb{F}_2^n$, $\sum_{u\in\mathbb{F}_2^n} W_F^4(u,v) = 2^{3n+1} + (2^{4n} - 2^{3n+1})\,\delta_0(v)$ (where δ_0 has been defined in Section 2). Then applying the Fourier transform and using its injectivity, F is CAPN if and only if, for every $w \in \mathbb{F}_2^n$, $\sum_{v\in\mathbb{F}_2^n}(-1)^{v\cdot w}\sum_{u\in\mathbb{F}_2^n} W_F^4(u,v) = 2^{4n+1}\delta_0(w) + 2^{4n} - 2^{3n+1}$, that is, $|\{(x,y,z) \in \mathbb{F}_2^n;\ F(x)+F(y)+F(z)+F(x+y+z)=w\}| = 2^{2n+1}\delta_0(w) + 2^{2n} - 2^{n+1}$, since $\sum_{v\in\mathbb{F}_2^n}(-1)^{v\cdot w}\sum_{u\in\mathbb{F}_2^n} W_F^4(u,v) = 2^{2n}|\{(x,y,z) \in \mathbb{F}_2^n;\ F(x)+F(y)+F(z)+F(x+y+z)=w\}|$. The condition for $w=0$ (which is equivalent to APN-ness) is implied by the condition for all $w \neq 0$, since we have $\sum_{w\in\mathbb{F}_2^n} |\{(x,y,z) \in \mathbb{F}_2^n;\ F(x)+F(y)+F(z)+F(x+y+z)=w\}| = 2^{3n}$. This completes the proof. □

Corollary 3.4 *CAPN (n,n)-functions exist only for n odd.*

Proof. When $w \neq 0$, all sets $\{x,y,z,x+y+z\}$ such that $F(x)+F(y)+F(z)+F(x+y+z) = w$ are 2-dimensional affine spaces (note that $w \neq 0$ implies that x,y,z and $x+y+z$ are pairwise distinct). For each such 2-dimensional affine space E, there exist 4! triples (x,y,z) such that $E = \{x,y,z,x+y+z\}$. Each set $\{(x,y,z) \in$

$\mathbb{F}_2^n;\ F(x)+F(y)+F(z)+F(x+y+z)=w\}$ has then size divisible by 3. Hence, if F is CAPN, then 3 divides $2^{2n}-2^{n+1}$ and n is odd. □

According to Proposition 3.2 and to Corollary 3.4, all known APN functions are CAPN if n is odd and are not if n is even. Note also that Proposition 3.2 and Corollary 3.4 prove again that power APN functions cannot be permutations when n is even.

Remark 3.5 *As shown by van Dam and Fon-Der-Flaass in [19], an APN (n,n)-function is AB if and only if, for every $w\neq 0$ and every z in $\mathbb{F}_2^n$, the equation $F(x)+F(y)+F(z)+F(x+y+z)=w$ has 2^n-2 solutions. This (together with Proposition 3.3) gives again that every AB function is CAPN and shows that CAPNness is a notion intermediate between APNness and ABness. The fact that there exist APN functions which are not CAPN, and the fact that the inverse function $F(x)=x^{2^n-2}$, $x\in\mathbb{F}_{2^n}$, n odd, and Dobbertin function $F(x)=x^{2^{\frac{4n}{5}}+2^{\frac{3n}{5}}+2^{\frac{2n}{5}}+2^{\frac{n}{5}}-1}$, $x\in\mathbb{F}_{2^n}$, n odd divisible by 5, are CAPN, according to Proposition 3.2, but not AB (i.e. the number of solutions (x,y) of $F(x)+F(y)+F(z)+F(x+y+z)=w$ depends on z for some $w\neq 0$) show that the three notions are distinct.*
Another characterization of AB functions given in [5] is that F is AB if and only if the system $\begin{cases} x+y+z+t & =a \\ F(x)+F(y)+F(z)+F(t) & =b \end{cases}$ admits $3\cdot 2^{2n}-2^{n+1}$ solutions if $a=b=0$ (this is APNness), $2^{2n}-2^{n+1}$ solutions if $a=0$ and $b\neq 0$ (this is CAPNness), and $2^{2n}+2^{n+2}\gamma_F(a,b)-2^{n+1}$ solutions if $a\neq 0$, where $\gamma_F(a,b)$ equals 1 if the equation $F(x)+F(x+a)=b$ has solutions and 0 otherwise. Clearly, in the case of the two functions above, the system has the correct number of solutions when $a=0$ but not always when $a\neq 0$.

We leave open the very difficult question of determining all CAPN functions (doing so would solve in particular the problem of determining all AB functions) and the sub-questions of determining if there exist CAPN functions which are neither AB nor power permutations and APN functions in odd dimension which are not CAPN. Another interesting question is to determine whether the CAPNness of permutations is equivalent to the CAPNness of their compositional inverses, and more generally, whether CAPNness is CCZ-invariant. We leave these questions open as well. We have of course:

Proposition 3.6 *CAPNness is EA-invariant.*

Proof. Let F be an (n,n)-function, L,L' two linear permutations of $\mathbb{F}_2^n$, L'' a linear function from $\mathbb{F}_2^n$ to itself and $a,b,c\in\mathbb{F}_2^n$. We denote by L^* the adjoint operator of L. Then $W_{(L+a)\circ F\circ(L'+b)+(L''+c)}(u,v)=\pm\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot(L(F(L'(x)+b))+L''(x))+u\cdot x}=\pm\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot(L(F(x))+L''(L'^{-1}(x+b)))+u\cdot L'^{-1}(x+b)}$ is equal, up to a change of sign, to

$\sum_{x\in\mathbb{F}_2^n}(-1)^{L^*(v)\cdot F(x)+[(L''\circ L'^{-1})^*(v)+(L'^{-1})^*(u)]\cdot x}$, that is, to:

$$W_F((L''\circ L'^{-1})^*(v)+(L'^{-1})^*(u),L^*(v)).$$

Since L and L' are bijective, L^* and $(L'^{-1})^*$ are bijective. Hence, the mapping $(u,v)\mapsto((L''\circ L'^{-1})^*(v)+(L'^{-1})^*(u),L^*(v))$ is a permutation of $(\mathbb{F}_2^n)^2$ which maps $\mathbb{F}_2^n\times\{0\}$ to itself and every coset of $\mathbb{F}_2^n\times\{0\}$ to a coset of $\mathbb{F}_2^n\times\{0\}$. This completes the proof. □

4 Componentwise Walsh uniformity

We have seen in Theorems 1.1 and 1.2 that, for all APN (n,n)-functions and all differentially 4-uniform $(n,n-1)$-functions, the arithmetic mean of

$$W_F^2(u_1,v_1)W_F^2(u_2,v_2)W_F^2(u_1+u_2,v_1+v_2)$$

when u_1,u_2 range independently over $\mathbb{F}_2^n$ and v_1,v_2 are distinct nonzero and range over the image set of F equals 2^{3n}. We first observe that this property is still valid for APN (n,n)-functions when fixing one of the two elements v_1,v_2.

4.1 A characteristic property of APN functions more precise than Relation (2)

Proposition 4.1 *Every (n,n)-function is APN if and only if, for every $v_1\neq 0$:*

$$\sum_{\substack{u_1,u_2,v_2\in\mathbb{F}_2^n\\ v_2\neq 0,v_2\neq v_1}} W_F^2(u_1,v_1)W_F^2(u_2,v_2)W_F^2(u_1+u_2,v_1+v_2)=2^{5n}(2^n-2). \tag{5}$$

Proof. The condition is clearly sufficient, according to Theorem 1.1. Let us show that it is necessary. For every v_1,v_2, we have:

$$\sum_{u_1,u_2\in\mathbb{F}_2^n} W_F^2(u_1,v_1)W_F^2(u_2,v_2)W_F^2(u_1+u_2,v_1+v_2)=$$

$$2^{2n}\sum_{\substack{(x_1,y_1,x_2,y_2,x_3,y_3)\in(\mathbb{F}_2^n)^6\\ x_1+y_1=x_2+y_2=x_3+y_3}}(-1)^{v_1\cdot(F(x_1)+F(y_1)+F(x_3)+F(y_3))+v_2\cdot(F(x_2)+F(y_2)+F(x_3)+F(y_3))}=$$

$$2^{2n}\sum_{x,y,z,t\in\mathbb{F}_2^n}(-1)^{v_1\cdot(F(x)+F(y)+F(z)+F(x+y+z))+v_2\cdot(F(y)+F(z)+F(t)+F(y+z+t))}, \tag{6}$$

(by replacing x_1 by x, x_2 by t, x_3 by y, y_3 by z and y_1,y_2 by their values by means of the other elements). Hence, including back the cases $v_2=0$ and $v_2=v_1$, (5) is equivalent to:

$$\sum_{x,y,z,t,v_2\in\mathbb{F}_2^n}(-1)^{v_1\cdot(F(x)+F(y)+F(z)+F(x+y+z))+v_2\cdot(F(y)+F(z)+F(t)+F(y+z+t))}=$$

$$2^{3n}(2^n-2)+2^n\sum_{x,y,z\in\mathbb{F}_2^n}(-1)^{v_1\cdot(F(x)+F(y)+F(z)+F(x+y+z))}$$
$$+\sum_{x,y,z,t\in\mathbb{F}_2^n}(-1)^{v_1\cdot(F(x)+F(x+y+z)+F(t)+F(y+z+t))}=$$
$$2^{3n}(2^n-2)+2^{n+1}\sum_{x,y,z\in\mathbb{F}_2^n}(-1)^{v_1\cdot(F(x)+F(y)+F(z)+F(x+y+z))}.$$

Since F is APN, we have $F(y)+F(z)+F(t)+F(y+z+t)=0$ if and only if $y=z$ or $y=t$ or $z=t$, and then we have:

$$\sum_{x,y,z,t,v_2\in\mathbb{F}_2^n}(-1)^{v_1\cdot(F(x)+F(y)+F(z)+F(x+y+z))+v_2\cdot(F(y)+F(z)+F(t)+F(y+z+t))}=$$
$$2^n\sum_{\substack{x,y,z,t\in\mathbb{F}_2^n\\ y=z \text{ or } y=t \text{ or } z=t}}(-1)^{v_1\cdot(F(x)+F(y)+F(z)+F(x+y+z))}=$$
$$2^{4n}+2^{n+1}\sum_{x,y,z\in\mathbb{F}_2^n}(-1)^{v_1\cdot(F(x)+F(y)+F(z)+F(x+y+z))}-2^{3n+1}=$$
$$2^{3n}(2^n-2)+2^{n+1}\sum_{x,y,z\in\mathbb{F}_2^n}(-1)^{v_1\cdot(F(x)+F(y)+F(z)+F(x+y+z))},$$

which proves (5). □

It is difficult to say if the situation is similar with differentially 4-uniform $(n,n-1)$-functions. It is clearly the case when the function has the form $F=L\circ G$ where L is an affine surjective $(n,n-1)$-function and G is an APN (n,n)-function (since, denoting by L^* the adjoint operator of the linear part of L, we have that L^* is injective and that, for every $v\neq 0$ and every a, $W_F^2(a,v)$ then equals $W_G^2(a,L^*(v))$, see e.g. [7]) but we leave open the general case.

4.2 Componentwise Walsh uniform functions

After the observation of Proposition 4.1, a natural question is to know whether all APN (n,n)-functions are such that fixing both v_1 and v_2 gives the same mean, and in the case the reply is no, to see if there exist APN functions having such property. The same questions can be also asked about differentially 4-uniform $(n,n-1)$-functions.

Definition 4.2 *An (n,m)-function F is called* componentwise Walsh uniform *(CWU) if, for every pair (v_1,v_2) of nonzero and distinct elements of $\mathbb{F}_2^m$, we have*

$$\sum_{u_1,u_2\in\mathbb{F}_2^n}W_F^2(u_1,v_1)W_F^2(u_2,v_2)W_F^2(u_1+u_2,v_1+v_2)=2^{5n}. \tag{7}$$

The notion of CWU is clearly EA-invariant (the proof is similar to that of Proposition 3.6).

Remark 4.3 *If F is plateaued, then it is CWU if and only if the proportion of those ordered pairs in $\{(u_1,u_2)\in(\mathbb{F}_2^n)^2;\ W_F(u_1,v_1)\neq 0$ and $W_F(u_2,v_2)\neq 0\}$ such that $W_F(u_1+u_2,v_1+v_2)\neq 0$ is the same as the proportion of those elements u_3 in $\mathbb{F}_2^n$ such that $W_F(u_3,v_1+v_2)\neq 0$. Indeed, if this property is satisfied then denoting again by λ_v the amplitude of the component function $v\cdot F$, Parseval's relation implies that this proportion necessarily equals $\frac{2^{2n}}{\lambda^2_{v+v'}}$ divided by the number 2^n of all u_3, that is, $\frac{2^n}{\lambda^2_{v+v'}}$ and we have then*

$$\sum_{u_1,u_2\in\mathbb{F}_2^n} W_F^2(u_1,v_1)W_F^2(u_2,v_2)W_F^2(u_1+u_2,v_1+v_2)=$$

$$\left(\sum_{u_1\in\mathbb{F}_2^n} W_F^2(u_1,v_1)\right)\left(\sum_{u_2\in\mathbb{F}_2^n} W_F^2(u_2,v_2)\right)\frac{2^n}{\lambda^2_{v+v'}}\lambda^2_{v+v'}=2^{5n}.$$

The converse is similar.
Note that the property above is satisfied automatically if v_1+v_2 is such that the component function $(v_1+v_2)\cdot F$ is bent, since the proportion is 1 in both cases; it is then also satisfied automatically if v_1 (or v_2) is such that the component function $v_1\cdot F$ (or $v_2\cdot F$) is bent. Hence, it is enough to check the property when none of the component functions $v_1\cdot F$, $v_2\cdot F$ and $(v_1+v_2)\cdot F$ is bent.

We continue with similar easy observations. Firstly, componentwise Walsh uniformity can be characterized by a property of the sums of values taken by the function over 2-dimensional affine spaces:

Proposition 4.4 *Let F be any (n,m)-function. Then F is CWU if and only if, for every pair (v_1,v_2) of nonzero and distinct elements of $\mathbb{F}_2^m$, we have:*

$$\sum_{x,y,z,t\in\mathbb{F}_2^n}(-1)^{v_1\cdot(F(x)+F(y)+F(z)+F(x+y+z))+v_2\cdot(F(y)+F(z)+F(t)+F(y+z+t))}=2^{3n};\quad(8)$$

equivalently:

$$\sum_{a,x,y,t\in\mathbb{F}_2^n}(-1)^{v_1\cdot(D_aF(x)+D_aF(y))+v_2\cdot(D_aF(y)+D_aF(t))}=2^{3n}.$$

Indeed, we have already seen that

$$\sum_{u_1,u_2\in\mathbb{F}_2^n} W_F^2(u_1,v_1)W_F^2(u_2,v_2)W_F^2(u_1+u_2,v_1+v_2)=$$

$$2^{2n}\sum_{\substack{(x_1,y_1,x_2,y_2,x_3,y_3)\in(\mathbb{F}_2^n)^6\\ x_1+y_1=x_2+y_2=x_3+y_3}}(-1)^{v_1\cdot(F(x_1)+F(y_1)+F(x_3)+F(y_3))+v_2\cdot(F(x_2)+F(y_2)+F(x_3)+F(y_3))}.$$

Of course, according to Theorem 1.1 and to Theorem 1.2, we have:

Proposition 4.5 *Let $m \in \{n-1, n\}$ and let F be a CWU (n,m)-function. Then if $m = n$, F is APN and if $m = n-1$, F is differentially 4-uniform.*

Determining precisely what are those APN (n,n)-functions which are CWU is an interesting and probably very difficult question in general, that we leave open. We are able to give a partial result:

Proposition 4.6 *Every APN function whose component functions are all partially-bent (that is, such that, for every nonzero $a, v \in \mathbb{F}_2^n$, the function $v \cdot D_aF(x)$ is either constant or balanced, see [4]) is CWU. In particular, every quadratic APN function is CWU.*

Proof. According to Proposition 4.4, F is CWU if and only if, for every distinct nonzero v_1, v_2:

$$\sum_{\substack{a\in\mathbb{F}_2^n;\, v_1\cdot D_aF=cst \\ \text{and } v_2\cdot D_aF=cst}} \sum_{x,y,t\in\mathbb{F}_2^n} (-1)^{v_1\cdot(D_aF(x)+D_aF(y))+v_2\cdot(D_aF(y)+D_aF(t))} = 2^{3n}.$$

Since F is APN, for every $a \neq 0$, the set $\{D_aF(x),\, x \in \mathbb{F}_2^n\}$ has 2^{n-1} elements. Functions $x \to v_1 \cdot D_aF(x)$ and $t \to v_2 \cdot D_aF(t)$ are then both constant (that is, functions $x \to v_1 \cdot (D_aF(x) + D_aF(0))$ and $t \to v_2 \cdot (D_aF(t) + D_aF(0))$ are both null) if and only if $a = 0$. Indeed, the set $\{D_aF(x) + D_aF(0),\, x \in \mathbb{F}_2^n\}$ having 2^{n-1} elements, it cannot belong to the $(n-2)$-dimensional vector space orthogonal to both v_1 and v_2. This completes the proof. □

Remark 4.7 *A set plays an important role for power APN functions $F(x) = x^d$ defined over the finite field $\mathbb{F}_{2^n}$: $\Delta_F = \{F(x) + F(x+1) + 1; x \in \mathbb{F}_{2^n}\}$ (see [13] and the following sections). The component functions of F are all partially-bent if and only if, for every $v \in \mathbb{F}_{2^n}$, denoting by 1_{Δ_F} the indicator of Δ_F, the Boolean function $tr_1^n(v1_{\Delta_F})$ is either constant or balanced. This happens of course when F is quadratic. In fact, F is then crooked (see [6]). We do not know an example where F is not quadratic.*

In Table 2 below, we report a computer investigation studying the CWUness of those (n,n)-functions which belong to the known infinite classes of non-quadratic power APN functions, for n between 3 and 11. We include among these classes, for n odd, the compositional inverses of Gold, Kasami, Welch, Niho and Dobbertin functions since the notion of CWU is not CCZ-invariant; this can be checked in the table by the fact that some permutations are CWU while their inverses are not. We indicate when all functions in a class are quadratic for a given n by writing "**Quad**". When all components are partially-bent but are not quadratic, we write "**PB**" (but we did not find any such case for the values of n visited); as we have seen, all **Quad** and **PB** functions are CWU. For those CWU functions whose components are not all partially-bent, we indicate "**CWU**" (for Kasami functions, we indicate the values

of i for which there are non-partially-bent components; we restrict ourselves to $2 \leq i < \frac{n}{2}$ since i and $n-i$ give linearly equivalent functions). For those functions which are not CWU, we write explicitly "**Not**CWU". We write "Na" when the functions do not exist in the considered class for the considered value of n, or are not APN.

$n=$	3	4	5	6	7	8	9	10	11
Kasami: $x^{4^i-2^i+1}$ $i \in \mathbb{Z}/n\mathbb{Z}$ $(i,n)=1,\ i<n/2$	**Quad**	**Quad**	**CWU** $i=2$	**Quad**	**CWU** $i=2,3$	**CWU** $i=3$	**CWU** $i=2,4$	**CWU** $i=3$	**CWU** $i=2,3,4,5$
Inverse function: x^{2^n-2}	**Quad**	Na	**CWU**	Na	**Not**CWU	Na	**Not**CWU	Na	**Not**CWU
Welch: $x^{2^{\frac{n-1}{2}}+3}$, n odd	**Quad**	Na	**CWU**	Na	**CWU**	Na	**Not**CWU	Na	**Not**CWU
Niho: $x^{2^{\frac{n-1}{2}}+2^{\frac{n-1}{4}}-1}$ if $4\|n-1$, $x^{2^{\frac{n-1}{2}}+2^{\frac{3n-1}{4}}-1}$ if $4\|n-3$	**Quad**	Na	**Quad**	Na	**Not**CWU	Na	**Not**CWU	Na	**Not**CWU
Dobbertin: $x^{2^{\frac{4n}{5}}+2^{\frac{3n}{5}}+2^{\frac{2n}{5}}+2^{\frac{n}{5}}-1}$ $5 \mid n$	Na	Na	**CWU**	Na	Na	Na	Na	**Not**CWU	Na
Gold composi-tional inverse	**Quad**	Na	**CWU**	Na	**CWU** $i=2,3$ **Not**CWU $i=1$	Na	**CWU** $i=4$ **Not**CWU $i=1,2$	Na	**CWU** $i=5$ **Not**CWU $i=1,2,3,4$
Kasami composi-tional inverse	**Quad**	Na	**Quad** $i=2$ **CWU** $i=1$	Na	**CWU** $i=2$ **Not**CWU $i=1,3$	Na	**Not**CWU	Na	**Not**CWU
Welch composi-tional inverse	**Quad**	Na	**Quad**	Na	**CWU**	Na	**Not**CWU	Na	**Not**CWU
Niho composi-tional inverse	**Quad**	Na	**CWU**	Na	**CWU**	Na	**Not**CWU	Na	**Not**CWU
Dobbertin composi-tional inverse	Na	Na	**CWU**	Na	Na	Na	Na	Na	Na

Table 2. Componentwise Walsh uniformity of known non-quadratic infinite classes of APN power functions

An important observation in this table is of course that all Kasami APN functions are CWU for $n \leq 11$, whatever is the parity of n and whatever is the value of i co-

prime with n, as well as the compositional inverse of Gold function $x^{2^{\frac{n-1}{2}}+1}$ (n odd). We shall prove that these properties are true for the infinite classes.

Remark 4.8 *Let us see why AB (n,n)-functions can be not CWU. We know (see e.g. [5]) that for every AB function F, every c and every z in $\mathbb{F}_2^n$, the equation $F(x)+F(y)+F(z)+F(x+y+z)=c$ has 2^n-2 solutions if $c\neq 0$ and $3\cdot 2^n-2$ if $c=0$. But in $\sum_{x,y,z,t\in\mathbb{F}_2^n}(-1)^{v_1\cdot(F(x)+F(y)+F(z)+F(x+y+z))+v_2\cdot(F(y)+F(z)+F(t)+F(y+z+t))}$ (see Proposition 4.4), both y and z are common to $F(x)+F(y)+F(z)+F(x+y+z)$ and $F(y)+F(z)+F(t)+F(y+z+t)$. This is why the strong property of AB functions does not suffice.*

Remark 4.9 *Since most of the known AB functions are not CWU and all AB functions are CAPN, and since Kasami functions in even dimension are CWU and not CAPN, the notions of CAPNness and CWU are independent, in the sense that no one is implied by the other.*

4.3 The case of APN power permutations

Let F be any power APN function $F(x)=x^d$ on $\mathbb{F}_{2^n}$. We denote by Δ_F the set $\{F(x)+F(x+1)+1,\ x\in\mathbb{F}_{2^n}\}$, which has size 2^{n-1}. It is well-known that, for every $u,v\in\mathbb{F}_{2^n}$, we have:

$$\begin{aligned}
W_F^2(u,v) &= \sum_{x,y\in\mathbb{F}_{2^n}} (-1)^{tr_1^n(v(F(x)+F(y))+u(x+y))}\\
&= \sum_{x,a\in\mathbb{F}_{2^n}} (-1)^{tr_1^n(vD_aF(x)+ua)}\\
&= \sum_{x,a\in\mathbb{F}_{2^n}} (-1)^{tr_1^n(vD_aF(ax)+ua)}\\
&= \sum_{x,a\in\mathbb{F}_{2^n}} (-1)^{tr_1^n(vF(a)D_1F(x)+ua)}\\
&= 2\sum_{a\in\mathbb{F}_{2^n},z\in 1+\Delta_F} (-1)^{tr_1^n(vF(a)z+ua)} \qquad (9)\\
&= 2\sum_{z\in 1+\Delta_F} W_F(u,vz), \qquad (10)
\end{aligned}$$

where $1+\Delta_F=\{1+z;\ z\in\Delta_F\}$. We changed x into ax for $a\neq 0$ in the third equality and used that $D_0F(x)=D_0F(0)$.

Remark 4.10 *Thanks to (9), we have:*

$$\begin{aligned} W_F^2(u,v) &= 2 \sum_{a\in\mathbb{F}_{2^n}, z\in\Delta_F} (-1)^{tr_1^n(vF(a)(z+1)+ua)} \\ &= 2 \sum_{a\in\mathbb{F}_{2^n}} (-1)^{tr_1^n(vF(a)+ua)} \widehat{1_{\Delta_F}}(vF(a)) \\ &= 2 \sum_{a\in\mathbb{F}_{2^n}} (-1)^{tr_1^n(va+uF^{-1}(a))} \widehat{1_{\Delta_F}}(va) \end{aligned}$$

(this last equality being valid only if F is bijective).
We also have:

$$\begin{aligned} \widehat{1_{\Delta_F}}(v) &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{tr_1^n(v(F(x)+F(x+1)))} \\ &= 2^{-n} \sum_{x,u\in\mathbb{F}_{2^n}} (-1)^{tr_1^n(v(F(x)+F(y))+u(x+y+1))} \\ &= 2^{-n} \sum_{u\in\mathbb{F}_{2^n}} W_F^2(u,v)(-1)^{tr_1^n(u)}. \end{aligned}$$

According to (9), we have:

$$\sum_{u_1,u_2\in\mathbb{F}_{2^n}} W_F^2(u_1,v_1)W_F^2(u_2,v_2)W_F^2(u_1+u_2,v_1+v_2) =$$

$$2^3 \sum_{u_1,u_2\in\mathbb{F}_{2^n}} \sum_{a,b,c\in\mathbb{F}_{2^n}, x,y,z\in 1+\Delta_F} (-1)^{tr_1^n(v_1F(a)x+v_2F(b)y+(v_1+v_2)F(c)z+u_1(a+c)+u_2(b+c))} =$$

$$2^{2n+3} \sum_{a\in\mathbb{F}_{2^n}, (x,y,z)\in(1+\Delta_F)^3} (-1)^{tr_1^n(v_1F(a)x+v_2F(a)y+(v_1+v_2)F(a)z)} =$$

$$2^{2n+3} \sum_{a\in\mathbb{F}_{2^n}, (x,y,z)\in\Delta_F^3} (-1)^{tr_1^n(v_1F(a)x+v_2F(a)y+(v_1+v_2)F(a)z)}.$$

If n is odd, then $gcd(d, 2^n-1) = 1$ for every APN function $F(x) = d$ and F is then a permutation (as proved by Dobbertin and reported in [5]), and $F(a)$ ranges over $\mathbb{F}_{2^n}$. We have then:

$$\sum_{u_1,u_2\in\mathbb{F}_{2^n}} W_F^2(u_1,v_1)W_F^2(u_2,v_2)W_F^2(u_1+u_2,v_1+v_2) =$$

$$2^{3n+3}|\{(x,y,z)\in\Delta_F^3;\ v_1x+v_2y+(v_1+v_2)z=0\}|.$$

Hence:

Proposition 4.11 *Let F be any power APN permutation. Then, F is CWU if and only if, for every $v_1, v_2 \in \mathbb{F}_{2^n}^*, v_1 \neq v_2$:*

$$|\{(x,y,z)\in\Delta_F^3;\ v_1x+v_2y+(v_1+v_2)z=0\}| = 2^{2n-3}. \tag{11}$$

Equivalently, the set Δ_F^3 intersects in 2^{2n-3} points any 2-dimensional $\mathbb{F}_{2^n}$-vector subspace of $\mathbb{F}_{2^n}^3$ passing through $(1,1,1)$ and different from the planes of equations $x=y$, $x=z$ and $y=z$.

The condition of Proposition 4.11 seems similar to the condition expressing that the complement[1] of Δ_F in $\mathbb{F}_{2^n}$ is a cyclic difference set with Singer parameters (see [13]), which writes:

$$\text{for all distinct nonzero } v_1, v_2 \text{ in } \mathbb{F}_{2^n}, |\{(x,y) \in \Delta_F^2;\ v_1x + v_2y = 0\}| = 2^{n-2};$$

that is, the set ${\Delta_F}^2$ intersects in 2^{n-2} points any 1-dimensional $\mathbb{F}_{2^n}$-subspace of $\mathbb{F}_{2^n}^2$ different from the axes and from the line of equation $x=y$. But the condition of Proposition 4.11 seems more complex since it involves addition as well as multiplication, while equality $v_1x + v_2y = 0$, that is, $v_1x = v_2y$, involves in fact only multiplication.

By analogy with the term of cyclic difference set with Singer parameters and that of additive difference set (which means that for all nonzero $v \in \mathbb{F}_{2^n}$, $|\{(x,y) \in \Delta^2;\ x+y=v\}|$ equals a constant) and for easing the presentation of the rest of this paper, we name the property in Proposition 4.11 as follows:

Definition 4.12 *Let Δ be any subset of $\mathbb{F}_{2^n}$. We say that Δ is a* cyclic-additive difference set with Singer-like parameters *if, for all distinct nonzero $v_1, v_2 \in \mathbb{F}_{2^n}$, we have $|\{(x,y,z) \in \Delta^3;\ v_1x + v_2y + (v_1+v_2)z = 0\}| = 2^{2n-3}$.*

Note that if we take the convention that $\frac{a}{b}$ takes indifferently any value if $a=b=0$ and (as usual in finite fields) equals 0 if $a=0, b\neq 0$ or $a\neq 0, b=0$, we have, for distinct nonzero v_1, v_2 that $|\{(x,y,z) \in \Delta^3;\ v_1x + v_2y + (v_1+v_2)z = 0\}| = |\{(x,y,z) \in \Delta^3;\ \frac{v_2}{v_1} = \frac{x+z}{y+z}\}|$. The notion of cyclic-additive difference set with Singer-like parameters is then not only invariant under multiplication of the elements of Δ by a nonzero constant (like cyclic difference sets) but also invariant under addition of a constant to any element of Δ, contrary to the cyclic difference set property (see [13]).

Remark 4.13 *More generally, we can define the notion of k-th order cyclic-additive difference set, satisfying that, for all nonzero $v_1, \ldots, v_k \in \mathbb{F}_{2^n}$ whose sum is nonzero, $|\{(x_1, \ldots, x_k) \in \Delta^k;\ \frac{v_1x_1+\cdots+v_kx_k}{v_1+\cdots+v_k} \in \Delta\}|$ equals $2^{k(n-1)-1}$. For $k=1$ it just tells that Δ has size 2^{n-1}.*

Important Remark 4.14 *The simplest example of a cyclic difference set with Singer parameters is the so-called* Singer set *$S_d = \{x \in \mathbb{F}_{2^n}; tr_1^n(x^d) = 1\}$, where d is co-prime with 2^n-1. Indeed, we have for every $\lambda \notin \mathbb{F}_2$ that $|\{(x,y) \in S_d^2;\ \lambda x + y = 0\}| = \sum_{x\in\mathbb{F}_{2^n}} tr_1^n(x^d) tr_1^n(\lambda^d x^d) = \frac{1}{4}\sum_{x\in\mathbb{F}_{2^n}} (1-(-1)^{tr_1^n(x^d)})(1-(-1)^{tr_1^n(\lambda^d x^d)}) = 2^{n-2} + \frac{1}{4}\sum_{x\in\mathbb{F}_{2^n}} (-1)^{tr_1^n(x^d+\lambda^d x^d)} = 2^{n-2} + \frac{1}{4}\sum_{x\in\mathbb{F}_{2^n}} (-1)^{tr_1^n((1+\lambda^d)x^d)} = 2^{n-2}$.*

[1] We take the complement so that it is a subset of the multiplicative group $\mathbb{F}_{2^n}^*$.

Let us see if such set is a cyclic-additive difference set with Singer-like parameters. We have:

$$|\{(x,y,z)\in S_d^3;\ v_1x+v_2y+(v_1+v_2)z=0\}|=$$

$$\sum_{x,y\in\mathbb{F}_{2^n}} tr_1^n(x^d)tr_1^n(y^d)tr_1^n\left(\left(\frac{v_1x+v_2y}{v_1+v_2}\right)^d\right)=$$

$$\frac{1}{8}\sum_{x,y\in\mathbb{F}_{2^n}}(1-(-1)^{tr_1^n(x^d)})(1-(-1)^{tr_1^n(y^d)})\left(1-(-1)^{tr_1^n\left(\left(\frac{v_1x+v_2y}{v_1+v_2}\right)^d\right)}\right)=$$

$$2^{2n-3}-\frac{1}{8}\sum_{x,y\in\mathbb{F}_{2^n}}(-1)^{tr_1^n\left(x^d+y^d+\left(\frac{v_1x+v_2y}{v_1+v_2}\right)^d\right)}=$$

$$2^{2n-3}-\frac{1}{8}\left(\sum_{\substack{x,z\in\mathbb{F}_{2^n}\\ x\neq 0}}(-1)^{tr_1^n\left(x^d\left(1+z^d+\left(\frac{v_1+v_2z}{v_1+v_2}\right)^d\right)\right)}+\sum_{y\in\mathbb{F}_{2^n}}(-1)^{tr_1^n\left(y^d+\left(\frac{v_2y}{v_1+v_2}\right)^d\right)}\right)=$$

$$2^{2n-3}-2^{n-3}|\{z\in\mathbb{F}_{2^n};1+z^d+\left(\frac{v_1+v_2z}{v_1+v_2}\right)^d=0\}|+2^{n-3},$$

and S_d is then a cyclic-additive difference set with Singer-like parameters if and only if, for every distinct nonzero v_1,v_2, the equation $z^d+\left(\frac{v_1+v_2z}{v_1+v_2}\right)^d=1$ has a unique solution in $\mathbb{F}_{2^n}$.

There exist such d. For instance, $d=1$ satisfies this property, whatever is n. Another example valid whatever is n is $d=2^n-2$. Indeed, the equation $z^{2^n-2}+\left(\frac{v_1+v_2z}{v_1+v_2}\right)^{2^n-2}=1$ does not have solution $z=0$ nor $z=\frac{v_1}{v_2}$ and is then equivalent to "$z\notin\{0,\frac{v_1}{v_2}\}$ and $\frac{1}{z}+\frac{v_1+v_2}{v_1+v_2z}=1$", and this latter equation has unique solution $z=\left(\frac{v_1}{v_2}\right)^{2^{n-1}}\notin\{0,\frac{v_1}{v_2}\}$. A third example is when n is odd and d is a Gold APN exponent, that is, $d=2^i+1$ where $(i,n)=1$. This could be checked by considering again the equation $z^d+\left(\frac{v_1+v_2z}{v_1+v_2}\right)^d=1$, but it can be seen in a simpler way as follows: we have $\sum_{x,y\in\mathbb{F}_{2^n}}(-1)^{tr_1^n\left(x^d+y^d+\left(\frac{v_1x+v_2y}{v_1+v_2}\right)^d\right)}=2^{-n}\sum_{\substack{u,x,y,\\ z\in\mathbb{F}_{2^n}}}(-1)^{tr_1^n\left(x^d+y^d+z^d+u\left(\frac{v_1x+v_2y}{v_1+v_2}+z\right)\right)}=2^{-n}\sum_{u\in\mathbb{F}_{2^n}}W_F\left(\frac{v_1}{v_1+v_2}u,1\right)W_F\left(\frac{v_2}{v_1+v_2}u,1\right)W_F(u,1)$, and we know (see e.g. [13, Appendix]) that for n odd, denoting $F(x)=x^d$, $W_F(u,1)$ is null when $tr_1^n(u)=0$ and we have that, for every u, one at least among $tr_1^n\left(\frac{v_1}{v_1+v_2}u\right)$, $tr_1^n\left(\frac{v_2}{v_1+v_2}u\right)$ and $tr_1^n(u)$ is null since the sum of these three bits is null.

But there are also examples of integers d co-prime with 2^n-1 which do not have the property. Indeed, for every d such that D_d is a cyclic-additive difference set with Singer-like parameters, if we denote $\frac{v_2}{v_1+v_2}$ by λ, the mapping which maps every $\lambda\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2$ to the unique $z\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2$ such that $z^d+(\lambda z+\lambda+1)^d=1$ is injective because "$z^d+(\lambda z+\lambda+1)^d=1$ and $z^d+(\lambda' z+\lambda'+1)^d=1$" implies

$(\lambda z+\lambda+1)^d = (\lambda' z+\lambda'+1)^d$ *and therefore* $\lambda = \lambda'$ *since* $z \neq 1$. *Hence this mapping is bijective and its compositional inverse maps* z *to* $\lambda = \frac{(z^d+1)^{\frac{1}{d}}+1}{z+1}$. *There exist integers* d *co-prime with* 2^n-1 *such that the function* $z \mapsto \frac{(z^d+1)^{\frac{1}{d}}+1}{z+1}$ *is not a permutation of* $\mathbb{F}_{2^n} \setminus \mathbb{F}_2$.
This illustrates the difference between the cyclic and cyclic-additive difference set properties.
We leave open the question of the determination of all power permutations $F(x) = x^d$ *such that the corresponding Singer set is a cyclic-additive difference set with Singer-like parameters.*

We continue with our investigation of CWUness for APN power permutations. Denoting by 1_{Δ_F} the indicator of Δ_F and by $\widehat{1_{\Delta_F}}$ its Fourier transform, we have:

$$|\{(x,y,z) \in \Delta_F^3;\ v_1x + v_2y + (v_1+v_2)z = 0\}| =$$
$$\sum_{(x,y)\in\mathbb{F}_{2^n}^2} 1_{\Delta_F}(x)1_{\Delta_F}(y)1_{\Delta_F}\left(\frac{v_1x+v_2y}{v_1+v_2}\right) =$$
$$2^{-3n} \sum_{x,y,u,u',u''\in\mathbb{F}_{2^n}} \widehat{1_{\Delta_F}}(u)\widehat{1_{\Delta_F}}(u')\widehat{1_{\Delta_F}}(u'')(-1)^{tr_1^n\left(ux+u'y+u''\frac{v_1x+v_2y}{v_1+v_2}\right)} =$$
$$2^{-n} \sum_{a\in\mathbb{F}_{2^n}} \widehat{1_{\Delta_F}}(v_1a)\widehat{1_{\Delta_F}}(v_2a)\widehat{1_{\Delta_F}}((v_1+v_2)a) =$$
$$2^{-n} \sum_{a\in\mathbb{F}_{2^n}} \left(2^{n-1}\delta_0(a) - \frac{1}{2}W_{1_{\Delta_F}}(v_1a)\right)\left(2^{n-1}\delta_0(a) - \frac{1}{2}W_{1_{\Delta_F}}(v_2a)\right)$$
$$\left(2^{n-1}\delta_0(a) - \frac{1}{2}W_{1_{\Delta_F}}((v_1+v_2)a)\right) =$$
$$2^{-n}\left(2^{3n-3} - \frac{1}{8}\sum_{a\in\mathbb{F}_{2^n}} W_{1_{\Delta_F}}(v_1a)W_{1_{\Delta_F}}(v_2a)W_{1_{\Delta_F}}((v_1+v_2)a)\right),$$

since $W_{1_{\Delta_F}}(0) = 0$ because $|\Delta_F| = 2^{n-1}$, and the condition of Proposition 4.11 is equivalent to

$$\sum_{a\in\mathbb{F}_{2^n}} \widehat{1_{\Delta_F}}(v_1a)\widehat{1_{\Delta_F}}(v_2a)\widehat{1_{\Delta_F}}((v_1+v_2)a) = 2^{3n-3}, \tag{12}$$

or equivalently:

$$\sum_{a\in\mathbb{F}_{2^n}} W_{1_{\Delta_F}}(v_1a)W_{1_{\Delta_F}}(v_2a)W_{1_{\Delta_F}}((v_1+v_2)a) = 0, \tag{13}$$

for every distinct nonzero v_1, v_2. Note that Δ_F can be replaced by ${\Delta_F}^c$, or $1+\Delta_F = \{D_1F(x); x \in \mathbb{F}_{2^n}\}$, or ${\Delta_F}^c + 1$ (since, for every Boolean function f, we have, denoting $g(x) = f(x+1)$, that $W_g(a) = (-1)^{tr_1^n(a)}W_f(a)$).

Remark 4.15 *Let us characterize by the Walsh transform the fact that the set Δ_F associated with some power permutation F is a cyclc difference set with Singer parameters, i.e. for all distinct nonzero v_1, v_2 in $\mathbb{F}_{2^n}$, $|\{(x,y) \in \Delta_F^2;\ v_1x+v_2y=0\}| = 2^{n-2}$. This condition is equivalent to $\sum_{(x,y)\in\Delta_F^2} \sum_{b\in\mathbb{F}_{2^n}} (-1)^{tr_1^n(b(v_1x+v_2y))} = 2^{2n-2}$, that is, $\sum_{x,y,a\in\mathbb{F}_{2^n}} (-1)^{tr_1^n(F(a)(v_1(F(x)+F(x+1)+1)+v_2(F(y)+F(y+1)+1))} = 2^{2n}$, that is, $\sum_{x,y,a\in\mathbb{F}_{2^n}} (-1)^{tr_1^n(v_1(F(x)+F(x+a)+F(a))+v_2(F(y)+F(y+a)+F(a))} = 2^{2n}$, which is equivalent to:*

$$\sum_{\substack{x,y,a\\ b,u\in\mathbb{F}_{2^n}}} (-1)^{tr_1^n(v_1(F(x)+F(x')+F(x''))+v_2(F(y)+F(y')+F(y'')+u(x''+y'')+u'(x+x'+x'')+u''(y+y'+y''))}$$

$$= 2^{5n},$$

that is, $\sum_{u,u',u''\in\mathbb{F}_{2^n}} W_F^2(u',v_1)W_F(u+u',v_1)W_F^2(u'',v_2)W_F(u+u'',v_2) = 2^{5n}$.

4.4 A general result on plateaued power APN functions

In this subsection and the next one, we give general results which will allow us to prove the CWUness of the two infinite classes of functions suggested by Table 2. In the case of APN power permutations, we have seen above that this is equivalent to the cyclic-additive difference set property of $\Delta_F = \{F(x)+F(x+1)+1; x \in \mathbb{F}_{2^n}\}$. It is in general very difficult to prove directly, given some nonquadratic APN function F, that Δ_F is a cyclic-additive difference set with Singer-like parameters. We shall be able to give such direct proof for the compositional inverse of the Gold (n,n)-function $x^{2^{\frac{n-1}{2}}+1}$, n odd, but we could not find one for the Kasami functions. We let such proof as an open problem. Fortunately, there exists a very useful general result on plateaued functions which will lead to a rather simple proof:

Theorem 4.16 *[6] Let F be an (n,m)-function. Then:*

- *F is plateaued if and only if, for every $v \in \mathbb{F}_2^m$, the size of the set*

$$\{(a,b) \in (\mathbb{F}_2^n)^2;\ D_aD_bF(x) = v\} \tag{14}$$

  does not depend on $x \in \mathbb{F}_2^n$ (in other words, the value distribution of $D_aD_bF(x)$ when (a,b) ranges over $(\mathbb{F}_2^n)^2$ is independent of $x \in \mathbb{F}_2^n$).
- *F is plateaued with single amplitude if and only if the size of the set in (14) does not depend on $x \in \mathbb{F}_2^n$, nor on $v \in \mathbb{F}_2^m$ when $v \neq 0$.*

Note that the value distribution of $D_aD_bF(x)$ when $(a,b) \in (\mathbb{F}_2^n)^2$ equals the value distribution of $D_aF(b) + D_aF(x)$.

We deduce the next theorem which will allow us to address the case of Kasami functions for n odd:

Theorem 4.17 *Let $F(x) = x^d$ be any plateaued APN power function over $\mathbb{F}_{2^n}$. Let $\Delta_F = \{F(x) + F(x+1) + 1; x \in \mathbb{F}_{2^n}\}$. Then Δ_F is a cyclic-additive difference set with Singer-like parameters if and only if its complement is a cyclic difference set with Singer parameters.*

Proof. Since F is APN, every value x in Δ_F is matched twice by $F(b)+F(b+1)+1 = D_1F(b)+1$ and saying that Δ_F is a cyclic-additive difference set with Singer-like parameters is then equivalent (by replacing x by $D_1F(b)+1$, y by $D_1F(b')+1$ and z by $D_1F(c)+1$) to saying that, for every distinct nonzero v_1, v_2, we have $|\{(b,b',c) \in \mathbb{F}_{2^n}^3; v_1(D_1F(b)+D_1F(c))+v_2(D_1F(b')+D_1F(c))=0\}| = 2^{2n}$. Multiplying this equality by $F(a)$, where $a \neq 0$, and dividing b, b' and c by a, transforms this condition into the equivalent condition $|\{(a,b,b',c) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^3; v_1(D_aF(b)+D_aF(c))+v_2(D_aF(b')+D_aF(c))=0\}| = 2^{2n}(2^n-1)$. Since F is plateaued, we can apply Theorem 4.16 and we have that, when a and b (resp. b') range over $\mathbb{F}_{2^n}$, with $a \neq 0$, the distribution, c being fixed, of the values of $D_aF(b)+D_aF(c)$ (resp. $D_aF(b')+D_aF(c)$) does not depend on the choice of c. Hence, the condition that Δ_F is a cyclic-additive difference set with Singer-like parameters (which corresponds to c ranging in $\mathbb{F}_{2^n}$) is equivalent to the condition with c fixed to 0: $|\{(a,b,b') \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^2; v_1(D_aF(b)+D_aF(0))+v_2(D_aF(b')+D_aF(0))=0\}| = 2^n(2^n-1)$, that is,$|\{(b,b') \in \mathbb{F}_{2^n}^2; v_1(D_1F(b)+D_1F(0))+v_2(D_1F(b')+D_1F(0))=0\}| = 2^n$, that is, Δ_F^c is a cyclic difference set with Singer parameters. □

Theorem 4.17 together with Proposition 4.11 and with the main result of [13] will solve in the same time, for n odd (so that F is a permutation), the question of the CWUness of Kasami APN functions and the cyclic-additive property of the related set Δ_F. We shall also need the following lemma, for handling the case of the inverse of Gold function:

Lemma 4.18 *Let F be any power permutation. Then $b \in 1+\Delta_F$ if and only if $1 \in \{F^{-1}(b)(F^{-1}(y)+F^{-1}(y+1)); y \in \mathbb{F}_{2^n}\}$. In particular, in the case where F^{-1} is a Gold permutation (n odd), $1+\Delta_F$ has equation $tr_1^n\left(\frac{1}{F^{-1}(x)}\right)=1$.*

Proof. For every $b, x \in \mathbb{F}_{2^n}$, we have $b = F(x)+F(x+a)$ if and only if $a = F^{-1}(b+F(x))+F^{-1}(F(x))$. We deduce that we have $b \in \{F(x)+F(x+a); x \in \mathbb{F}_{2^n}\}$ if and only if $a \in \{F^{-1}(y)+F^{-1}(y+b); y \in \mathbb{F}_{2^n}\}$. Hence, $b \in 1+\Delta_F$ if and only if $1 \in \{F^{-1}(b+y)+F^{-1}(y); y \in \mathbb{F}_{2^n}\}$. Since F is a power permutation, F^{-1} is also a power function, and this writes then $1 \in \{F^{-1}(b)(F^{-1}(y)+F^{-1}(y+1)); y \in \mathbb{F}_{2^n}\}$. In the case where F^{-1} is a Gold permutation (n odd), this writes $1 \in F^{-1}(b)\{z \in \mathbb{F}_{2^n}; tr_1^n(z)=1\}$ and then $1+\Delta_F$ has equation $tr_1^n\left(\frac{1}{F^{-1}(x)}\right)=1$. □

Remark 4.19 *When F is the inverse of a Gold permutation, $1+\Delta_F$ is then a Singer set and is then a cyclic difference set in $\mathbb{F}_{2^n}^*$ with Singer parameters; we have $|\{(x,y) \in (1+\Delta_F)^2;\ v_1x = v_2y\}| = 2^{n-2}$ for every distinct nonzero v_1, v_2 in $\mathbb{F}_{2^n}$. Note however that this does not allow to apply Theorem 4.17 since, in general, Δ_F^c is not a cyclic difference set (we know this thanks to Table 2). We shall see that for $F^{-1}(x) = x^{2^{\frac{n-1}{2}}+1}$, Δ_F^c is a cyclic difference set.*

4.5 A stronger result on those plateaued functions whose components are unbalanced, usable with plateaued power APN functions when n is even

If n is even then, as proved by Dobbertin (and also reported in [5]), we have $gcd(d, 2^n - 1) = 3$ and we cannot then use Proposition 4.11. We have:

$$\sum_{u_1,u_2\in\mathbb{F}_{2^n}} W_F^2(u_1, v_1)W_F^2(u_2, v_2)W_F^2(u_1 + u_2, v_1 + v_2) =$$

$$2^{2n+3} \sum_{a\in\mathbb{F}_{2^n},(x,y,z)\in\Delta_F^3} (-1)^{tr_1^n(a^3(v_1x+v_2y+(v_1+v_2)z))},$$

and we know from [10] that:
- if $w = 0$, then $\sum_{a\in\mathbb{F}_{2^n}}(-1)^{tr_1^n(a^3w)} = 2^n$,
- if w is a nonzero cube, then $\sum_{a\in\mathbb{F}_{2^n}}(-1)^{tr_1^n(a^3w)} = (-2)^{\frac{n}{2}+1}$,
- if w is not a cube, then $\sum_{a\in\mathbb{F}_{2^n}}(-1)^{tr_1^n(a^3w)} = (-2)^{\frac{n}{2}}$.

To be able to handle the case n even, we would then need to have information not only on the size of the set $\{(x, y, z) \in \Delta_F^3;\ v_1x+v_2y+(v_1+v_2)z = 0\}$ as in the case of n odd, but also on the sets $\{(x, y, z) \in \Delta_F^3;\ v_1x+v_2y+(v_1+v_2)z$ *is a nonzero cube*$\}$ and $\{(x, y, z) \in \Delta_F^3;\ v_1x + v_2y + (v_1 + v_2)z$ *is not a cube*$\}$. In fact, there is a much simpler way to address the case n even: we know that in this case, all the component functions $tr_1^n(vF)$ of F are unbalanced. Indeed, since we have $tr_1^n(vF)(0) = 0$ and since, for every $x \in \mathbb{F}_{2^n}^*$, function $tr_1^n(vF)$ is constant on the multiplicative coset $x\mathbb{F}_4^*$, the Hamming weight of $tr_1^n(vF)$ is divisible by 3 and therefore different from 2^{n-1}.

Theorem 4.20 *[6] Let F be any (n, m)-function. Then F is plateaued with component functions all unbalanced if and only if, for every $v, x \in \mathbb{F}_2^n$, we have:*

$$\left|\{(a, b) \in (\mathbb{F}_2^n)^2\,;\ D_aD_bF(x) = v\}\right| =$$

$$\left|\{(a, b) \in (\mathbb{F}_2^n)^2\,;\ F(a) + F(b) = v\}\right|.$$

Here again we have

$$\left|\{(a, b) \in (\mathbb{F}_2^n)^2\,;\ D_aD_bF(x) = v\}\right| = \left|\{(a, b) \in (\mathbb{F}_2^n)^2\,;\ D_aF(b) + D_aF(x) = v\}\right|.$$

Hence, the CWUness of any plateaued APN power function over $\mathbb{F}_{2^n}$, n even, depends only on the distribution of its values, and since all APN functions over $\mathbb{F}_{2^n}$, n even, have the same value distribution and the quadratic APN function $F(x) = x^3$ is CWU, we have:

Theorem 4.21 *All plateaued APN power functions over $\mathbb{F}_{2^n}$, n even, are CWU.*

4.6 Proofs of the CWUness of the two remaining CWU classes

The case of APN Kasami functions for n even has been solved in the previous subsection: they are CWU thanks to Theorem 4.21 and to their plateauedness [13, 20], and their associated set Δ_F is a cyclic-additive difference set with Singer-like parameters thanks to Theorem 4.17, to the main result of [13] in the even case, and to the plateauedness of Kasami APN functions. We still have to prove the CWUness of the compositional inverse of the Gold (n,n)-function $x^{2^{\frac{n-1}{2}}+1}$, n odd, and of Kasami (n,n)-functions $F(x)=x^{2^{2i}-2^i+1}$, with $(i,n)=1$, for n odd as well.

The case of compositional inverse of Gold (n,n)-function $x^{2^{\frac{n-1}{2}}+1}$, n odd
Note that this function being AB, it is plateaued and according to Proposition 4.11 and Theorem 4.17, it is equivalent to check its CWUness, the fact that the related set Δ_F is a cyclic-additive difference set with Singer-like parameters and the fact that its complement is a cyclic difference set with Singer parameters. Note that we have $(2^{\frac{n-1}{2}}+1)(2^{\frac{n+1}{2}}-2)=2^n-2=-1 \pmod{2^n-1}$ and therefore $\frac{1}{2^{\frac{n-1}{2}}+1}=2-2^{\frac{n+1}{2}} \pmod{2^n-1}$ and $F(x)+F(x+1)+1=\left(x^{1-2^{\frac{n-1}{2}}}+(x+1)^{1-2^{\frac{n-1}{2}}}+1\right)^2=\left(\frac{x+x^{2^{\frac{n+1}{2}}}}{(x^2+x)^{2^{\frac{n-1}{2}}}}\right)^2$ and therefore $\Delta_F=\left\{\frac{x^2+x^{2^{\frac{n+1}{2}}}}{x^2+x};x\in\mathbb{F}_{2^n}\right\}$, and $F(x)+F(x+1)=\left(\frac{x+x^{2^{\frac{n-1}{2}}}}{(x^2+x)^{2^{\frac{n-1}{2}}}}\right)^2$ and therefore $1+\Delta_F=\left\{\frac{x+x^{2^{\frac{n+1}{2}}}}{x^2+x};x\in\mathbb{F}_{2^n}\right\}$. We leave open the question of finding a relation between Δ_F and $1+\Delta_F$ which would allow to deduce directly that Δ_F is a cyclic difference set from the fact that $1+\Delta_F$ is one.

Theorem 4.22 *For every odd n, the compositional inverse F of Gold (n,n)-function $x^{2^{\frac{n-1}{2}}+1}$ is CWU and the associated set $\Delta_F=\{F(x)+F(x+1)+1;x\in\mathbb{F}_{2^n}\}$ is a cyclic-additive difference set with Singer-like parameters.*

Proof. According to Lemma 4.18, we have:

$$1+\Delta_F=\left\{x\in\mathbb{F}_{2^n}^*,\ tr_1^n\left(\frac{1}{x^{2^{\frac{n-1}{2}}+1}}\right)=1\right\}.$$

With the convention $\frac{1}{0}=0$, we have, changing x into x^{-1}:
$W_{1_{\Delta_F+1}}(u) = \sum_{x\in\mathbb{F}_{2^n}}(-1)^{tr_1^n\left(\frac{1}{x^{2^{\frac{n-1}{2}}+1}}+ux\right)} = \sum_{x\in\mathbb{F}_{2^n}}(-1)^{tr_1^n\left(x^{2^{\frac{n-1}{2}}+1}+ux^{-1}\right)} = \sum_{x\in\mathbb{F}_{2^n}}(-1)^{tr_1^n\left(x^{2^{\frac{n-1}{2}}+1}+ux^{\left(2^{\frac{n-1}{2}}+1\right)\left(2^{\frac{n+1}{2}}-2\right)}\right)} = \sum_{x\in\mathbb{F}_{2^n}}(-1)^{tr_1^n\left(x+ux^{2^{\frac{n+1}{2}}-2}\right)}$. Condition (13) applied with $1+\Delta_F$ in the place of Δ_F (recall that the notion of cyclic-additive difference set with Singer-like parameters is invariant under translation,

contrary to that of cyclic difference set with Singer parameters) becomes then:

$$\sum_{a,x,y,z\in\mathbb{F}_{2^n}} (-1)^{tr_1^n(x+y+z+v_1ax^{2^{\frac{n+1}{2}}-2}+v_2ay^{2^{\frac{n+1}{2}}-2}+(v_1+v_2)az^{2^{\frac{n+1}{2}}-2})} = 0,$$

or equivalently, by dividing, when $a \neq 0$, x, y, z by $a^{\frac{1}{2^{\frac{n+1}{2}}-2}}$ and, subsequently a into $\frac{1}{a^{2^{\frac{n+1}{2}}-2}}$:

$$\sum_{a,x,y,z\in\mathbb{F}_{2^n}} (-1)^{tr_1^n(a(x+y+z)+v_1x^{2^{\frac{n+1}{2}}-2}+v_2y^{2^{\frac{n+1}{2}}-2}+(v_1+v_2)z^{2^{\frac{n+1}{2}}-2})} = 0,$$

that is

$$\sum_{\substack{x,y,z\in\mathbb{F}_{2^n}\\ x+y+z=0}} (-1)^{tr_1^n(v_1x^{2^{\frac{n+1}{2}}-2}+v_2y^{2^{\frac{n+1}{2}}-2}+(v_1+v_2)z^{2^{\frac{n+1}{2}}-2})} = 0,$$

or equivalently by replacing v_1 by v_1^2 and v_2 by v_2^2, and denoting $d = 2^{\frac{n-1}{2}} - 1$:

$$\sum_{\substack{x,y,z\in\mathbb{F}_{2^n}\\ x+y+z=0}} (-1)^{tr_1^n(v_1x^d+v_2y^d+(v_1+v_2)z^d)} = 0.$$

We have for $x \neq y$ that $x + y + z = 0$ implies $v_1x^d + v_2y^d + (v_1 + v_2)z^d = v_1x^d + v_2y^d + (v_1 + v_2)\frac{x^{d+1}+y^{d+1}}{x+y} = \frac{v_1y^{d+1}+v_2x^{d+1}+v_1x^dy+v_2xy^d}{x+y} = (v_1y + v_2x)\frac{x^d+y^d}{x+y}$. Hence, the condition to be checked is

$$\sum_{\substack{x,y\in\mathbb{F}_{2^n}\\ x\neq y}} (-1)^{tr_1^n\left((v_1y+v_2x)\frac{x^d+y^d}{x+y}\right)} + \sum_{x\in\mathbb{F}_{2^n}} (-1)^{tr_1^n\left((v_1+v_2)x^d\right)} = 0.$$

In other words, since $\sum_{x\in\mathbb{F}_{2^n}} (-1)^{tr_1^n\left((v_1+v_2)x^d\right)} = 0$ for $v_1 \neq v_2$ because d is co-prime with $2^n - 1$, we need to prove that the function:

$$\varphi : (v_1, v_2) \mapsto (1 - \delta_0(v_1))(1 - \delta_0(v_2))(1 - \delta_0(v_1 + v_2)) \sum_{\substack{x,y\in\mathbb{F}_{2^n}\\ x\neq y}} (-1)^{tr_1^n\left((v_1y+v_2x)\frac{x^d+y^d}{x+y}\right)}$$

is identically null. When $v_1 = v_2 \neq 0$, we have $\sum_{\substack{x,y\in\mathbb{F}_{2^n}\\ x\neq y}} (-1)^{tr_1^n\left((v_1y+v_2x)\frac{x^d+y^d}{x+y}\right)} = \sum_{\substack{x,y\in\mathbb{F}_{2^n}\\ x\neq y}} (-1)^{tr_1^n\left(v_1(x^d+y^d)\right)} = \sum_{x,y\in\mathbb{F}_{2^n}} (-1)^{tr_1^n\left(v_1(x^d+y^d)\right)} - 2^n = -2^n$; the condition that φ be identically null is then equivalent to the fact that the function: $(v_1, v_2) \mapsto$

$$(1-\delta_0(v_1)-\delta_0(v_2)+\delta_0(v_1, v_2)) \sum_{\substack{x,y\in\mathbb{F}_{2^n}\\ x\neq y}} (-1)^{tr_1^n\left((v_1y+v_2x)\frac{x^d+y^d}{x+y}\right)} + (\delta_0(v_1+v_2)-\delta_0(v_1, v_2))\, 2^n$$

is identically null. Equivalently, the Fourier transform (that we shall denote by ϕ) of this latter function:

$$\begin{aligned}\phi : (w_1, w_2) \mapsto & \sum_{\substack{x,y,v_1,v_2 \in \mathbb{F}_{2^n} \\ x \neq y}} (-1)^{tr_1^n\left((v_1 y + v_2 x)\frac{x^d+y^d}{x+y} + v_1 w_1 + v_2 w_2\right)} \\ & - \sum_{\substack{x,y,v_2 \in \mathbb{F}_{2^n} \\ x \neq y}} (-1)^{tr_1^n\left(v_2 x \frac{x^d+y^d}{x+y} + v_2 w_2\right)} - \sum_{\substack{x,y,v_1 \in \mathbb{F}_{2^n} \\ x \neq y}} (-1)^{tr_1^n\left(v_1 y \frac{x^d+y^d}{x+y} + v_1 w_1\right)} \\ & + 2^{2n} - 2^n + \left(2^n \delta_0(w_1 + w_2) - 1\right) 2^n\end{aligned}$$

is identically null. We have $\sum_{\substack{x,y,v_1,v_2 \in \mathbb{F}_{2^n} \\ x \neq y}} (-1)^{tr_1^n\left((v_1 y + v_2 x)\frac{x^d+y^d}{x+y} + v_1 w_1 + v_2 w_2\right)} = 2^{2n} \left|\left\{(x,y) \in \mathbb{F}_{2^n}^2; x \neq y \text{ and } y\frac{x^d+y^d}{x+y} = w_1 \text{ and } x\frac{x^d+y^d}{x+y} = w_2\right\}\right|$. The system of equations $\begin{cases} y\frac{x^d+y^d}{x+y} = w_1 \\ x\frac{x^d+y^d}{x+y} = w_2 \end{cases}$ under the condition $x \neq y$ has no solution if $w_1 = w_2$, and has solutions:

- $x = (w_2)^{\frac{1}{d}}, y = 0$ if $w_1 = 0, w_2 \neq 0$,
- $x = 0, y = (w_1)^{\frac{1}{d}}$ if $w_1 \neq 0, w_2 = 0$,
- x, y such that $\begin{cases} xw_1 = yw_2 \\ x^d(1 + \frac{w_1^d}{w_2^d}) = w_1 + w_2 \end{cases}$, that is, $x = w_2\left(\frac{w_1+w_2}{w_1^d+w_2^d}\right)^{\frac{1}{d}}, y = w_1\left(\frac{w_1+w_2}{w_1^d+w_2^d}\right)^{\frac{1}{d}}$ if $w_1 \neq w_2, w_1 \neq 0, w_2 \neq 0$.

Hence, we have: $\sum_{\substack{x,y,v_1,v_2 \in \mathbb{F}_{2^n} \\ x \neq y}} (-1)^{tr_1^n\left((v_1 y + v_2 x)\frac{x^d+y^d}{x+y} + v_1 w_1 + v_2 w_2\right)} = 2^{2n}(1 - \delta_0(w_1 + w_2))$. We also have, for every nonzero v_2, that $\sum_{\substack{x,y \in \mathbb{F}_{2^n} \\ x \neq y}} (-1)^{tr_1^n\left(v_2 x \frac{x^d+y^d}{x+y} + v_2 w_2\right)} = \sum_{\substack{x,y \in \mathbb{F}_{2^n} \\ x \neq y}} (-1)^{tr_1^n\left(v_2 y^d + v_2 \frac{x^{d+1}+y^{d+1}}{x+y} + v_2 w_2\right)} = \sum_{\substack{x,y,z \in \mathbb{F}_{2^n} \\ x \neq y, x+y+z=0}} (-1)^{tr_1^n\left(v_2 y^d + v_2 z^d + v_2 w_2\right)} = \sum_{y,z \in \mathbb{F}_{2^n}} (-1)^{tr_1^n\left(v_2 y^d + v_2 z^d + v_2 w_2\right)} - \sum_{y \in \mathbb{F}_{2^n}} (-1)^{tr_1^n\left(v_2 y^d + v_2 w_2\right)} = 0$.

Similarly, for every nonzero v_1, $\sum_{\substack{x,y,v_1 \in \mathbb{F}_{2^n} \\ x \neq y}} (-1)^{tr_1^n\left(v_1 y \frac{x^d+y^d}{x+y} + v_1 w_1\right)} = 0$.

We deduce that $\sum_{\substack{x,y,v_2 \in \mathbb{F}_{2^n} \\ x \neq y}} (-1)^{tr_1^n\left(v_2 x \frac{x^d+y^d}{x+y} + v_2 w_2\right)} = \sum_{\substack{x,y,v_1 \in \mathbb{F}_{2^n} \\ x \neq y}} (-1)^{tr_1^n\left(v_1 y \frac{x^d+y^d}{x+y} + v_1 w_1\right)} = 2^{2n} - 2^n$. Hence, $\phi(w_1, w_2) = 2^{2n}(1 - \delta_0(w_1 + w_2)) - 2 \cdot (2^{2n} - 2^n) + 2^{2n} - 2^n + (2^n \delta_0(w_1 + w_2) - 1)\, 2^n$ is identically null, which proves the result. □

Remark 4.23 *Since we know that the compositional inverse F of Gold (n,n)-function $x^{2^{\frac{n-1}{2}}+1}$ is AB, another approach for proving Theorem 4.22 is by determining the support of $W_F(u,v)$ and directly calculating, for v_1 and v_2 distinct and*

nonzero: $\sum_{u_1,u_2\in\mathbb{F}_{2^n}} W_F^2(u_1,v_1)W_F^2(u_2,v_2)W_F^2(u_1+u_2,v_1+v_2)$. *We have* $W_F(u,v) = \sum_{x\in\mathbb{F}_{2^n}}(-1)^{tr_1^n(vx+ux^{2^i+1})}$, *where* $i=\frac{n-1}{2}$. *It is well-known and easily checked that the kernel of the associated symplectic form* $(x,y)\mapsto tr_1^n(vx+ux^{2^i+1})+tr_1^n(vy+uy^{2^i+1})+tr_1^n(v(x+y)+u(x+y)^{2^i+1})$ *(the so-called radical) has equation* $ux^{2^i}+(ux)^{2^{n-i}}=0$, *that is,* $u^{2^i}x^{2^{2i}}+ux=0$, *which, for* $u\neq 0$, *has unique nonzero solution* $x=u^{-\frac{1}{2^i+1}}$, *since* i *is co-prime with* n. *The support of* $W_F(u,v)$ *has then equation* $tr_1^n\left(vu^{-\frac{1}{2^{\frac{n-1}{2}}+1}}\right)=1$, *that is,* $tr_1^n\left(vu^{2^{\frac{n+1}{2}}-2}\right)=1$. *But this finally leads to verifying that the set* $\{(u_1,u_2)\in\mathbb{F}_{2^n}; tr_1^n\left(v_1u_1^{2^{\frac{n+1}{2}}-2}\right)=tr_1^n\left(v_2u_2^{2^{\frac{n+1}{2}}-2}\right)=tr_1^n\left((v_1+v_2)(u_1+u_2)^{2^{\frac{n+1}{2}}-2}\right)=1\}$ *has size* 2^{n-3} *and then to the same kind of calculations as in the proof above.*

The case of Kasami (n,n)-functions $F(x)=x^{2^{2i}-2^i+1}$, with $(i,n)=1$
Recall that the CWUness of these functions in the case n even has been proved in Subsection 4.5 and, since we know from Dillon and Dobbertin in [13, Theorem A] that the complement of $\Delta_F=\{F(x)+F(x+1)+1;\ x\in\mathbb{F}_{2^n}\}$ is a cyclic difference set with Singer parameters whatever is the parity of n, Theorem 4.17 proves the cyclic-additive difference set property in the case n even (since F is plateaued). Since we know that for n odd F is AB and therefore also plateaued, we deduce from Theorem 4.17 that Δ_F is a cyclic-additive difference set with Singer-like parameters. This proves, thanks to Proposition 4.11, that all Kasami APN functions over $\mathbb{F}_{2^n}$, n odd, are CWU. We have then proved:

Theorem 4.24 *All Kasami APN functions are CWU and their associated sets* Δ_F *are cyclic-additive difference sets with Singer-like parameters.*

Remark 4.25 *Theorem 4.20 allows proving directly that the complement of* Δ_F *is a cyclic difference set with Singer parameters when* F *is any plateaued APN power function and* n *is even, since it shows that its cyclic difference set property depends only on the value distribution of* F *and is then the same for all plateaued APN power functions, and we know that, for the particular APN function* $F(x)=x^3$, *the complement of* Δ_F *is a Singer set (it equals* $\{x\in\mathbb{F}_{2^n}; tr_1^n(x)=1\}$*). Recall that Dillon-Dobbertin's proof of the cyclic difference set property of all Kasami APN functions needed very subtile arguments and was also quite long. It is nice to see that, for* n *even, the properties of plateaued functions can simplify the question (but of course, we still need the proof of plateauedness, which was not that simple either). It would be nice to have similar situation for* n *odd. We leave this for future work.*

4.7 The case of (n,m)-functions with $m<n$

Let us see now that componentwise Walsh uniform (n,m)-functions also exist for $m<n$.

Proposition 4.26 *If F is a CWU (n,m)-function and L is a surjective affine (m,k)-function, then $L \circ F$ is CWU.*

This is straightforward according to the observations in [7]. Note that the same result stands if we replace "componentwise Walsh uniform" by "plateaued". Determining precisely what are those differentially 4-uniform $(n, n-1)$-functions which are CWU is an interesting question, that we leave also open.

Note that the existence of differentially 6-uniform $(n, n-2)$-functions for $n \geq 6$ is an open question (a few differentially 6-uniform $(5,3)$-functions are known, as mentioned in [8]).

Conclusion

We introduced the property of componentwise APNness (CAPNness) of (n,n)-functions, implying APNness, and showed that all AB functions and all APN power permutations have this property. We proved that CAPN functions do not exist for n even. We introduced the property of componentwise Walsh uniformity (CWU), implying APNness in the case of (n,n)-functions and differential 4-uniformity in the case of $(n, n-1)$-functions, which is satisfied by all quadratic APN (n,n)-functions and more generally by all those APN (n,n)-functions whose component functions are all partially-bent. We proved the CWUness of two infinite classes of (n,n)-functions whose component functions are not all partially-bent: those of the compositional inverse of one of the Gold AB permutations and of all Kasami APN functions. We showed that the other main classes of APN functions are not CWU.
We leave open the following questions:

1. determine all CAPN functions,
2. exhibit CAPN functions which would not be AB functions nor APN power permutations,
3. exhibit APN functions in odd dimension which are not CAPN,
4. determine whether the CAPNness of permutations is equivalent to the CAPNness of their compositional inverses, and more generally, whether CAPNness is CCZ-invariant,
5. determine whether $(n, n-1)$-functions are differentially 4-uniform if and only if, for every $v_1 \neq 0$: $\sum_{\substack{u_1,u_2 \in \mathbb{F}_{2^n}, v_2 \in \mathbb{F}_2^{n-1} \\ v_2 \neq 0, v_2 \neq v_1}} W_F^2(u_1,v_1) W_F^2(u_2,v_2) W_F^2(u_1+u_2, v_1+v_2) = 2^{5n}(2^{n-1}-2)$,
6. determine all CWU functions,
7. determine all power permutations $F(x) = x^d$ such that the corresponding Singer set is a cyclic-additive difference set with Singer-like parameters,
8. find a direct proof (without using Theorems 4.17 and 4.21) of the CWUness of Kasami functions,
9. find a simpler proof of the cyclic difference set property of $\Delta_F = \{F(x) + F(x+1) + 1;\ x \in \mathbb{F}_{2^n}\}$ when F is a Kasami function with n odd, similar to the one obtained in this paper for n even,

10. find a relation between Δ_F and $1+\Delta_F$ when F is the compositional inverse of Gold (n,n)-function $x^{2^{\frac{n-1}{2}}+1}$, n odd, which would allow to deduce directly that Δ_F is a cyclic difference set from the fact that $1+\Delta_F$ is one,
11. find any other short proof (possibly using Theorems 4.17 and 4.21) of the CWUness of the compositional inverse of Gold (n,n)-function $x^{2^{\frac{n-1}{2}}+1}$, n odd,
12. determine precisely what are those differentially 4-uniform $(n,n-1)$-functions which are CWU,
13. prove or disprove the existence of differentially 6-uniform $(n,n-2)$-functions for $n \geq 6$, possibly by suing the results of the present paper.

Acknowledgements. We are much indebted to Stjepan Picek for his great help in building Table 2 and in making computations which helped us in delicate proofs. We are grateful to Sihem Mesnager for her useful observations all along this work, and we thank Xi Chen for finding minor errors in a first version. We wish to thank many other researchers for their informations on the problems visited and tracks followed by the author while he was searching a proof of the CWUness of Kasami functions: Antonia Bluher, Thomas Cusick, Cunsheng Ding, Faruk Gologlu, Tor Helleseth, William Kantor, Philippe Langevin, Gregor Leander, Gary McGuire, Gary Mullen, Daniel Panario and Alexander Pott.

References

1. L. Budaghyan, "Construction and Analysis of Cryptographic Functions", Springer Verlag, 2015.
2. 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.
3. C. Carlet. *Codes de Reed-Muller, codes de Kerdock et de Preparata*. PhD thesis. Publication of LITP, Institut Blaise Pascal, Université Paris 6, 90.59, 1990.
4. C. Carlet. Boolean Functions for Cryptography and Error Correcting Codes. Chapter of the monography *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, Y. Crama and P. Hammer eds, Cambridge University Press, pp. 257-397 (2010). Preliminary version available at www.math.univ-paris13.fr/~carlet/english.html
5. C. Carlet. Vectorial Boolean Functions for Cryptography. Chapter of the monography *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, Y. Crama and P. Hammer eds, Cambridge University Press, pp. 398-469 (2010). Preliminary version available at www.math.univ-paris13.fr/~carlet/english.html
6. C. Carlet. Boolean and vectorial plateaued functions, and APN functions. *IEEE Transactions on Information Theory* Vol. 61 no. 11, pp. 6272-6289, 2015.
7. C. Carlet. Characterizations of the differential uniformity of vectorial functions by the Walsh transform, IACR ePrint Archive 2017.
8. C. Carlet and Y. Al Salami. A New Construction of Differentially 4-uniform $(n,n-1)$-Functions. *Advances in Mathematics of Communications*, Vol. 9, no. 4, pp. 541 - 565, 2015.
9. 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).
10. L. Carlitz, Explicit evaluation of certain exponential sums, In *Math. Scand.,* **44** (1979), 5–16.
11. F. Chabaud and S. Vaudenay. Links between Differential and Linear Cryptanalysis. *Proceedings of EUROCRYPT'94, Lecture Notes in Computer Science* 950, pp. 356-365, 1995.

12. J. F. Dillon, Geometry, codes and difference sets: exceptional connections, Codes and Designs (Columbus, OH, 2000), 73 85, Ohio State Univ. Math. Res. Inst. Publ., 10, de Gruyter, Berlin, 2002.
13. J. F. Dillon and H. Dobbertin. New cyclic difference sets with Singer parameters. *Finite Fields and Applications* 10, pp. 342-389, 2004.
14. H. Dobbertin. Another proof of Kasami's Theorem. *Designs, Codes and Cryptography* 17, pp. 177-180, 1999.
15. S. Mesnager: Characterizations of Plateaued and Bent Functions in Characteristic p. Proceedings of SETA 2014, pp. 72-82, 2014.
16. G. Mullen and D. Panario. *Handbook of finite fields*. CRC Press Book, 2013.
17. K. Nyberg. Perfect non-linear S-boxes. *Proceedings of EUROCRYPT' 91, Lecture Notes in Computer Science* 547, pp. 378-386, 1992.
18. K. Nyberg. Differentially uniform mappings for cryptography. *Proceedings of EUROCRYPT' 93, Lecture Notes in Computer Science* 765, pp. 55-64, 1994.
19. E. R. van Dam and D. Fon-Der-Flaass. Codes, graphs, and schemes from nonlinear functions. *Eur. J. Comb.* 24(1), pp. 85-98, 2003.
20. S. Yoshihara. Plateauedness of Kasami APN functions. Preprint, 2016.