# On Almost Perfect Nonlinear Functions Over $\boldsymbol{F}_2^n$

Thierry P. Berger, Anne Canteaut, Pascale Charpin, and Yann Laigle-Chapuy

***Abstract*—We investigate some open problems on almost perfect nonlinear (APN) functions over a finite field of characteristic 2. We provide new characterizations of APN functions and of APN permutations by means of their component functions. We generalize some results of Nyberg (1994) and strengthen a conjecture on the upper bound of nonlinearity of APN functions. We also focus on the case of quadratic functions. We contribute to the current works on APN quadratic functions by proving that a large class of quadratic functions cannot be APN.**

***Index Terms*—Almost bent function, almost perfect nonlinear (APN) function, power function, permutation polynomial.**

## I. Introduction

MOST attacks on symmetric cryptographic algorithms are related to some properties of the Boolean functions describing the system. For iterated block ciphers, the efficiency of the main cryptanalytic techniques (such as linear cryptanalysis, differential cryptanalysis...) can be measured by some quantities related to the confusion part of the round function, usually named S(ubstitution)-box. This paper focuses on the S-boxes which guarantee a high resistance to differential cryptanalysis [4]. This attack successfully applies when two plaintexts with fixed difference lead after the last-but-one round to outputs whose difference takes a certain value with a high probability. Therefore, a necessary security condition is that the output distributions of all derivatives of the involved S-box, $x \mapsto F(x+a)+F(x)$, must be close to the uniform distribution. The relevant parameter for an S-box $F$ with $n$ inputs is then

$$\delta(F) = \max_{a \neq 0, b} \#\left\{x \in \boldsymbol{F}_2^n,\ F(x+a)+F(x)=b\right\}$$

which must be as small as possible. When the number of output bits of the S-box is the same as the number of inputs (this is the case in most ciphers), we have that $\delta(F) \geq 2$, and the functions achieving this bound are called *almost perfect nonlinear* (APN) [27]. Therefore, APN functions are those S-boxes which offer optimal resistance to differential cryptanalysis.

As optimal objects, APN functions are also used in several other areas of telecommunications. Most notably, APN functions correspond to linear codes of length $2^n-1$ and dimension $2n$ which have the best minimal distance 5 [13]. Thus, APN functions are of great interest in coding theory. Despite a number of recent works, many problems remain open. Actually, only a few APN functions are known, and most of them are affinely equivalent to a power function (see, e.g., [6][7]). The first infinite class of quadratic APN functions, which are not equivalent to any power function, was exhibited very recently (see [5] and [19]). In this paper, we investigate some open problems on APN functions and we give partial results.

The next section gives some basic definitions related to APN functions over $\boldsymbol{F}_2^n$. Actually, in the whole paper, we identify the vector space $\boldsymbol{F}_2^n$ with the finite field $\boldsymbol{F}_{2^n}$ of order $2^n$ and such a function $F$ is expressed as a polynomial in $\boldsymbol{F}_{2^n}[x]$. Since $F$ can be represented by the collection of its $n$ Boolean coordinates, we also recall some properties on Boolean functions. In Section III-A, we study the APN functions by means of their Boolean components. We prove that the necessary condition for a function to be APN, introduced in [26], is also sufficient (Theorem 2). Then, we derive a new characterization of APN functions (Corollary 1). We later characterize APN permutations of $\boldsymbol{F}_{2^n}$ (Proposition 2). This last result is motivated by the conjecture that there is no APN permutation of $\boldsymbol{F}_{2^n}$ when $n$ is even. In this context, and using our characterization, we prove that there is no APN permutation whose component functions are plateaued (Corollary 3 and Theorem 3). We also give a new characterization of APN power functions on $\boldsymbol{F}_{2^n}$ when $n$ is even and an upper bound on their nonlinearity (Theorem 4). The last section is devoted to quadratic APN functions. It is well known that the power functions of the form $x^{2^k+1}$ over $\boldsymbol{F}_{2^n}$ with $\gcd(k,n)=1$ are APN. But, the classification of quadratic APN functions which are not equivalent to the previous power functions is still an open problem. Here, we exhibit a whole subclass of quadratic functions which does not contain any APN functions. This result gives us more information about the form of quadratic APN functions (Proposition 7).

## II. Definitions and Basic Properties

In this section, we introduce notation and some basic properties which will be used in the paper. The next definition is general and suitable for Boolean functions. Actually, in this paper, we treat the cases $m=n$ and $m=1$ only.

*Definition 1:* Let $n$ and $m$ be two nonzero integers. Let $F$ be a function from $\boldsymbol{F}_2^n$ into $\boldsymbol{F}_2^m$. For any $a \in \boldsymbol{F}_2^n$, the *derivative of $F$ with respect to $a$* is the function $D_aF$ from $\boldsymbol{F}_2^n$ into $\boldsymbol{F}_2^m$ defined by

$$D_aF(x) = F(x+a)+F(x), \quad \forall x \in \boldsymbol{F}_2^n .$$

If $D_aF$ is constant then $a$ is said to be a *linear structure* of $F$.

Manuscript received May 2, 2005; revised March 20, 2006. The material in this paper was presented in part at the IEEE International Symposium on Information Theory, Adelaide, Australia, September 2005,

T. Berger is with the XLIM, Faculté des Sciences de Limoges, 87060 Limoges Cedex, France (e-mail: Thierry.Berger@unilim.fr).

A. Canteaut, P. Charpin, and Y. Laigle-Chapuy are with INRIA, Domaine de Voluceau, Rocquencourt, BP 105–78153, Le Chesnay Cedex, France (e-mail: Anne.Canteaut@inria.fr; Pascale.Charpin@inria.fr; Yann.Laigle-Chapuy@inria.fr).

Communicated by E. Okamoto, Associate Editor for Complexity and Cryptography.

Digital Object Identifier 10.1109/TIT.2006.880036

The resistance to differential cryptanalysis is related to the following quantities.

*Definition 2:* Let $F$ be a function from $\boldsymbol{F}_2^n$ into $\boldsymbol{F}_2^n$. For any $a$ and $b$ in $\boldsymbol{F}_2^n$, we denote

$$\delta(a,b) = \#\{x \in \boldsymbol{F}_2^n, D_aF(x) = b\}$$

where $\#E$ is the cardinality of any set $E$. Then, we have

$$\delta(F) = \max_{a\neq 0,\ b\in\boldsymbol{F}_2^n} \delta(a,b) \geq 2$$

and the functions for which equality holds are said to be *almost perfect nonlinear* (APN).

The APN property can be equivalently defined as follows.

*Proposition 1:* Let $F$ be any function on $\boldsymbol{F}_2^n$. Then, $F$ is APN if and only if, for any nonzero $a \in \boldsymbol{F}_2^n$, the set $\{D_aF(x), x \in \boldsymbol{F}_2^n\}$ has cardinality $2^{n-1}$.

From now on, we identify the vector space $\boldsymbol{F}_2^n$ with the finite field with $2^n$ elements, $\boldsymbol{F}_{2^n}$. Any function $F$ from $\boldsymbol{F}_2^n$ into $\boldsymbol{F}_2^n$ can then be expressed as a polynomial in $\boldsymbol{F}_{2^n}[x]$. Recall that the *degree* of $F$ is the maximal Hamming weight of its exponents

$$\deg\left(\sum_{i=0}^{2^n-1} \lambda_i x^i\right) = \max\{wt(i)|\lambda_i \neq 0\}$$

where $\lambda_i \in \boldsymbol{F}_{2^n}$ and the weight is calculated on the 2-ary expansion of $i$. We denote by Tr the trace function on $\boldsymbol{F}_{2^n}$, i.e., $\mathrm{Tr}(\beta) = \beta + \beta^2 + \cdots + \beta^{2^{n-1}}$.

The function $F$ can also be represented by $n$ Boolean functions of $n$ variables, its Boolean *coordinates*. Note that the coordinates are sometimes called the components of $F$, but it is more convenient for our purpose to use the following definition, like in [26].

*Definition 3:* Let $F$ be a function from $\boldsymbol{F}_{2^n}$ into $\boldsymbol{F}_{2^n}$. The linear combinations of the coordinates of $F$ are the Boolean functions

$$f_\lambda : x \in \boldsymbol{F}_{2^n} \mapsto \mathrm{Tr}(\lambda F(x)), \quad \lambda \in \boldsymbol{F}_{2^n}$$

where $f_0$ is the null function. The functions $f_\lambda$ are called the *components* of $F$.

We denote by $\mathcal{B}_n$ the set of Boolean functions on $\boldsymbol{F}_{2^n}$. In our context, the linear functions of $\mathcal{B}_n$ are the functions $\varphi_a$, defined by

$$\varphi_a : x \in \boldsymbol{F}_{2^n} \mapsto \mathrm{Tr}(ax), \quad a \in \boldsymbol{F}_{2^n}^*. \tag{1}$$

The following notation will be extensively used in the paper. For any $f \in \mathcal{B}_n$, we denote by $\mathcal{F}(f)$ the following value related to the Fourier (or Walsh) transform of $f$:

$$\mathcal{F}(f) = \sum_{x\in\boldsymbol{F}_{2^n}} (-1)^{f(x)} = 2^n - 2\mathrm{wt}(f) \tag{2}$$

where $\mathrm{wt}(f)$ is the Hamming weight of $f$, i.e., the number of $x \in \boldsymbol{F}_2^n$ such that $f(x) = 1$. The function $f$ is said to be *balanced* if and only if $\mathcal{F}(f) = 0$ or, equivalently, $\mathrm{wt}(f) = 2^{n-1}$.

*Definition 4:* The *Walsh spectrum* of $f \in \mathcal{B}_n$ is the multiset

$$\{\mathcal{F}(f + \varphi_a), a \in \boldsymbol{F}_{2^n}\}.$$

The *nonlinearity* of $f$ is its Hamming distance to the set of all affine functions. It is given by

$$2^{n-1} - \frac{1}{2}\mathcal{L}(f), \quad \text{where} \quad \mathcal{L}(f) = \max_{a\in\boldsymbol{F}_{2^n}} \left|\mathcal{F}(f + \varphi_a)\right|.$$

The lowest possible value for $\mathcal{L}(f)$ is $2^{\frac{n}{2}}$ and this bound is achieved for *bent functions*.

*Definition 5:* [8], [31] Let $f \in \mathcal{B}_n$. The function $f$ is said to be *plateaued* if its Walsh coefficients take at most three values, namely, $0, \pm\mathcal{L}(f)$. Then, $\mathcal{L}(f) = 2^s$ with $s \geq n/2$.

If $s = n/2$ (and $n$ even) then $f$ is said to be *bent* and its Walsh coefficients take two values only, namely, $\pm 2^{\frac{n}{2}}$. Moreover, $f$ is said *plateaued optimal* if $s = (n+1)/2$ for odd $n$ and $s = (n+2)/2$ for even $n$.

These functions belong to a particular class of Boolean functions, which notably includes all quadratic functions and, more generally, *partially bent*[1] functions.

The nonlinearity of a function $F$ from $\boldsymbol{F}_{2^n}$ into $\boldsymbol{F}_{2^n}$ is now defined by means of the nonlinearities of its components.

*Definition 6:* Let $F$ be a function from $\boldsymbol{F}_{2^n}$ into $\boldsymbol{F}_{2^n}$ with components $f_\lambda$, $\lambda \in \boldsymbol{F}_{2^n}^*$. The *nonlinearity* of $F$ is the minimal value of the nonlinearities of the $f_\lambda$. It is equal to

$$\mathcal{N}(F) = 2^{n-1} - \frac{\Lambda(F)}{2}, \quad \text{where } \Lambda(F) = \max_{\lambda\in\boldsymbol{F}_{2^n}^*} \mathcal{L}(f_\lambda).$$

The nonlinearity of $F$ is a measure of its vulnerability to linear attacks. The functions that have maximal nonlinearity are called almost bent (AB) functions. They exist for odd $n$ only.

*Definition 7:* [15] Let $F$ be a function from $\boldsymbol{F}_{2^n}$ into $\boldsymbol{F}_{2^n}$ with components $f_\lambda$, $\lambda \in \boldsymbol{F}_{2^n}$. Then

$$\Lambda(F) \geq 2^{\frac{n+1}{2}}.$$

The functions $F$ which satisfy

$$\Lambda(F) = 2^{\frac{n+1}{2}}$$

are said to be *almost bent* (AB). They exist when $n$ is odd only. Moreover, if $F$ is AB, then for any $a \in \boldsymbol{F}_{2^n}$ and for any nonzero $\lambda$

$$\{\mathcal{F}(f_\lambda + \varphi_a),\ \lambda \in \boldsymbol{F}_{2^n}^*, a \in \boldsymbol{F}_{2^n}\} = \{0, \pm 2^{\frac{n+1}{2}}\} \tag{3}$$

i.e., all $f_\lambda$, $\lambda \neq 0$, are plateaued optimal.

*Remark 1:* Let $F$ be a function from $\boldsymbol{F}_{2^n}$ into $\boldsymbol{F}_{2^n}$. Studying the APN property and the AB property (for odd $n$) is equivalent to studying the weights of an associated code $C_F$ and of its dual $C_F^\perp$ (see an extensive study in [13]).

The Walsh spectrum of a Boolean function and its derivatives are related by the so-called *sum-of-square indicator* introduced

[1]These functions were introduced in [12]; they can be seen as a generalization of quadratic functions.

in [31] and extensively studied in [8], [9], and [32]. The proof of the following theorem can be found in [8] and [32].

*Definition 8:* The *sum-of-square indicator* of $f \in \mathcal{B}_n$ is defined by

$$\nu(f) = \sum_{a \in \boldsymbol{F}_{2^n}} \mathcal{F}^2(D_a f) = 2^{-n} \sum_{a \in \boldsymbol{F}_{2^n}} \mathcal{F}^4(f + \varphi_a).$$

*Theorem 1:* Any $f \in \mathcal{B}_n$ satisfies $\nu(f) \leq 2^n \mathcal{L}^2(f)$. Equality occurs if and only if $f$ is plateaued, that is,

$$\mathcal{L}(f) = 2^s \quad \text{and} \quad \nu(f) = 2^{n+2s}, \qquad \frac{n}{2} \leq s \leq n. \tag{4}$$

## III. On APN Functions

A necessary condition for a function $F$ over $\boldsymbol{F}_{2^n}$ to be APN was provided by Nyberg in [26]. This condition involves the derivatives of the components of $F$. In this section, we prove that this condition is also a sufficient condition and derive another characterization by means of the sum-of-square indicators of the components of $F$. We further discuss some conjectures. We notably apply our characterization to achieve some new results on plateaued functions.

### A. Characterizations of APN Functions

The next theorem is mainly due to Nyberg [26]. We include it only to provide a full characterization of APN functions by means of the derivatives of their component functions.

*Theorem 2:* Let $F$ be a function from $\boldsymbol{F}_{2^n}$ into $\boldsymbol{F}_{2^n}$ and let $f_\lambda$, $\lambda \in \boldsymbol{F}_{2^n}$ denote its components. Then, for any nonzero $a \in \boldsymbol{F}_{2^n}$

$$\sum_{\lambda \in \boldsymbol{F}_{2^n}} \mathcal{F}^2(D_a f_\lambda) \geq 2^{2n+1}. \tag{5}$$

Moreover, $F$ is APN if and only if for all nonzero $a \in \boldsymbol{F}_{2^n}$

$$\sum_{\lambda \in \boldsymbol{F}_{2^n}} \mathcal{F}^2(D_a f_\lambda) = 2^{2n+1}. \tag{6}$$

*Proof:* Set $A = \sum_{\lambda \in \boldsymbol{F}_{2^n}} \mathcal{F}^2(D_a f_\lambda)$. Then $A$ is equal to

$$\sum_{\lambda, x, y \in \boldsymbol{F}_{2^n}} (-1)^{\mathrm{Tr}(\lambda(F(x+a)+F(x)+F(y+a)+F(y)))}.$$

So

$$\begin{aligned} A &= 2^n \# \left\{ (x, y) \in \boldsymbol{F}_{2^n}^2 \mid D_a F(x) = D_a F(y) \right\} \\ &= 2^{2n+1} + 2^n \# \{ (x, y) \mid D_a F(x) = D_a F(y), x \neq y \neq x + a \} \end{aligned}$$

Thus (5) is immediately deduced with equality if and only if $F$ is APN (see Definition 2). □

The previous theorem is more efficient for proving that $F$ is not APN. For instance, if $F$ is such that $D_a f_\lambda$ and $D_a f_{\lambda'}$ are constant, for $\lambda \neq \lambda' \neq 0$ and for some $a$, then the sum in (6) equals at least $2^{2n+2}$; so $F$ is not APN. This argument was widely used for proving more general results [26]. Conversely, the sufficient condition induced by Theorem 2 leads to a better understanding of the properties of APN functions, as indicated in the next example.

*Example 1:* Let $F$ be a polynomial of degree 3 on $\boldsymbol{F}_{2^n}$, where $n$ is even. Thus, any component of $F$ has degree at most 3. Any component $f_\lambda$, $\lambda \neq 0$, has all its derivatives of degree at most 2 ($f_0$ is the null function). This implies that for all $\lambda$ and for all $a$, we have

$$\mathcal{F}(D_a f_\lambda) \equiv 0 \pmod{2^{(n+2)/2}}$$

a congruence which is satisfied by any quadratic nonbent function. Suppose that for any $a$, $|\mathcal{F}(D_a f_\lambda)|$ equals $2^{(n+2)/2}$ for exactly $2^{n-2}$ nonzero values of $\lambda$ and equals 0 for the others. Then, by applying Theorem 2, $F$ is APN, noticing that $\mathcal{F}(D_a f_0) = 2^{2n}$. Is it possible to construct such a function $F$?

It follows from the previous theorem that the APN property is related to the values of the sum-of-square indicators, $\nu(f_\lambda)$, of the components of $F$.

*Corollary 1:* Let $F$ be a function from $\boldsymbol{F}_{2^n}$ into $\boldsymbol{F}_{2^n}$ with components $f_\lambda$, $\lambda \in \boldsymbol{F}_{2^n}^*$. Then

$$\sum_{\lambda \in \boldsymbol{F}_{2^n}^*} \nu(f_\lambda) \geq (2^n - 1) 2^{2n+1}. \tag{7}$$

Moreover, $F$ is APN if and only if

$$\sum_{\lambda \in \boldsymbol{F}_{2^n}^*} \nu(f_\lambda) = (2^n - 1) 2^{2n+1}. \tag{8}$$

Consequently, if $\nu(f_\lambda) = 2^{2n+1}$ for all nonzero $\lambda$, then $F$ is APN.

*Proof:* Set

$$A = \sum_{a \in \boldsymbol{F}_{2^n}^*} \sum_{\lambda \in \boldsymbol{F}_{2^n}} \mathcal{F}^2(D_a f_\lambda).$$

According to (5), we have $A \geq 2^{2n+1}(2^n - 1)$. Since $\mathcal{F}^2(D_0 f_\lambda) = \mathcal{F}^2(D_a f_0) = 2^{2n}$ for any $a$ and for any $\lambda$, then

$$\begin{aligned} A &= \sum_{\lambda \in \boldsymbol{F}_{2^n}^*} \sum_{a \in \boldsymbol{F}_{2^n}} \mathcal{F}^2(D_a f_\lambda) \\ &= \sum_{\lambda \in \boldsymbol{F}_{2^n}^*} \nu(f_\lambda). \end{aligned}$$

Thus, $A = \sum_{\lambda \in \boldsymbol{F}_{2^n}^*} \nu(f_\lambda)$, implying (7). Now, if $F$ is APN then $F$ satisfies (6) and we get $A = 2^{2n+1}(2^n - 1)$. Conversely, assume that $A = 2^{2n+1}(2^n - 1)$. Since for any $a$

$$\sum_{\lambda \in \boldsymbol{F}_{2^n}} \mathcal{F}^2(D_a f_\lambda) \geq 2^{2n+1}$$

these inequalities must be equalities. Then $F$ is APN. The last statement is immediately deduced. □

*Example 2:* When $F$ is the inverse function $x \mapsto x^{2^n - 2}$ over $\boldsymbol{F}_{2^n}$, it is well known that $F$ is APN for odd $n$ and not APN for even $n$. The nonlinearity of $F$ is known, due to the work of Lachaud and Wolfmann [23]. The $\nu(f_\lambda)$ are calculated in [16]. As an illustration of our purpose we recall the following values:

- Let $n$ be odd. Thus,

$$\Lambda(F) = \max\left\{k \equiv 0 \pmod 4 | k < 2^{(n/2)+1}\right\}$$

and, for all $\lambda \neq 0$, $\nu(f_\lambda) = 2^{2n+1}$.
- Let $n$ be even. Thus, $\Lambda(F) = 2^{(n+2)/2}$ and, for all $\lambda \neq 0$, $\nu(f_\lambda) = 2^{2n+1} + 2^{n+3}$.

It appears from Corollary 1 that the APN property only depends on the extended Walsh spectrum of $F$, i.e., on the multiset

$$\mathcal{W}(F) = \{|\mathcal{F}(f_\lambda + \varphi_a)|, \lambda \in \boldsymbol{F}_{2^n}^*,\ a \in \boldsymbol{F}_{2^n}\}.$$

Note that $\mathcal{W}(F)$ consists of all values taken by $|\mathcal{F}(f_\lambda + \varphi_a)|$ and the number of times they occur. In other words, if $F$ is APN, any function $F'$ such that $\mathcal{W}(F') = \mathcal{W}(F)$ is APN too. Indeed, $F$ is APN if and only if the $\nu(f_\lambda)$ satisfy (8). But the values $\nu(f_\lambda)$ are obtained by means of the values of the set $\mathcal{W}(F)$ (see Definition 8).

There are only a few extended Walsh spectra which are known to correspond to APN functions. When $n$ is odd, three APN extended Walsh spectra are known

- $\mathcal{W}(x^3)$ whose elements lie in $\{0, 2^{\frac{n+1}{2}}\}$. It is the Walsh spectrum of all AB function;
- $\mathcal{W}(x^{2^n-2})$ whose elements take all values $k \equiv 0 \bmod 4$ such that $0 \leq k < 2^{\frac{n}{2}+1}$;
- $\mathcal{W}(x^{2^{4g}+2^{3g}+2^{2g}+2^g-1})$ for $n = 5g$ [18], which differs from both previous spectra since it contains a value which is not divisible by $2^{2g+1}$, but all its elements are divisible by 4 (see [11, Propositions 5.3 and 7.13]). For instance, for $n = 15$ (i.e., for $g = 3$), the values in $\mathcal{W}(x^{2^{4g}+2^{3g}+2^{2g}+2^g-1})$ are $0, 2^{2g}, 3\cdot 2^{2g}$, $2^{2g+2}, 5\cdot 2^{2g}, 9\cdot 2^{2g}$.

When $n$ is even, only two APN extended Walsh spectra are known:

- $\mathcal{W}(x^3)$ whose elements lie in $\{0, 2^{\frac{n}{2}}, 2^{\frac{n}{2}+1}\}$;
- $\mathcal{W}(x^{2^{4g}+2^{3g}+2^{2g}+2^g-1})$ for $n = 5g$ [18], which differs from the previous one because it does not have the same divisibility as previously mentioned.

It is worth noticing that two functions $F$ and $G$ with different Walsh spectra may nevertheless be such that their components have the same sum-of-square indicators. For instance, when $n$ is odd, all known APN functions on $\boldsymbol{F}_{2^n}$ are such that their components $f_\lambda$ satisfy $\nu(f_\lambda) = 2^{2n+1}$ for all $\lambda \neq 0$. Conversely, two functions with the same extended Walsh spectrum may be such that the sets $\{\nu(f_\lambda),\ \lambda \in \boldsymbol{F}_{2^n}^*\}$ and $\{\nu(g_\lambda),\ \lambda \in \boldsymbol{F}_{2^n}^*\}$ are different, as we will see in Example 4.

*Open Problem 1:* Find an APN function on $\boldsymbol{F}_{2^n}$, $n$ odd, such that $\nu(f_\lambda) \neq 2^{2n+1}$ for some nonzero $\lambda \in \boldsymbol{F}_{2^n}^*$.

Corollary 1 enables us to characterize APN functions when the corresponding sum-of-square indicators $\nu(f_\lambda)$ take their values in a particular set. Such a situation occurs, for instance, when all the $f_\lambda, \lambda \neq 0$, are plateaued functions, as pointed out in Corollaries 2 and 3. When $n$ is odd, the situation is well known. To be clear, we summarize it in the next corollary and give as proof a short explanation. The even case, which we treat in Corollary 3, is more interesting since we generalize the result of Nyberg, [26, Theorem 10].

*Corollary 2:* Let $n$ be odd and let $F$ be a function from $\boldsymbol{F}_{2^n}$ into $\boldsymbol{F}_{2^n}$ with components $f_\lambda$, $\lambda \in \boldsymbol{F}_{2^n}^*$. Then, the following statements are equivalent:

i) $F$ is APN and all $f_\lambda$, $\lambda \in \boldsymbol{F}_{2^n}^*$ are plateaued;
ii) all $f_\lambda$, $\lambda \in \boldsymbol{F}_{2^n}^*$, are plateaued and satisfy $\nu(f_\lambda) = 2^{2n+1}$;
iii) $F$ is AB.

*Proof:* If $f_\lambda$ is plateaued, then we have $\nu(f_\lambda) = 2^{n+2s}$ with $2s \geq n+1$ (see Theorem 1). If $F$ is APN, then (8) is satisfied with $\nu(f_\lambda) \geq 2^{2n+1}$ for all $\lambda$, implying ii). We deduce from Corollary 1 that ii) implies that $F$ is APN. The equivalence between ii) and iii) is mentioned in Definition 7. □

*Corollary 3:* Let $n$ be even and let $F$ be a function from $\boldsymbol{F}_{2^n}$ into $\boldsymbol{F}_{2^n}$ such that all $f_\lambda, \lambda \in \boldsymbol{F}_{2^n}^*$, are plateaued. Let $B$ be the number of $f_\lambda$ which are bent. Then we have the following.

i) If $B = 0$ then $F$ is not APN.
ii) If $F$ is APN, then $B \geq 2\cdot(2^n-1)/3$ with equality if and only if $\Lambda(F) = 2^{(n+2)/2}$. Conversely, if $B = 2\cdot(2^n-1)/3$ and $\Lambda(F) = 2^{(n+2)/2}$ then $F$ is APN.
iii) If $F$ is APN then it is not a permutation. Moreover, there is no permutation of the form $F + L$ where $L$ is a linear function on $\boldsymbol{F}_{2^n}$.

*Proof:*

i) Assume that there is no $\lambda \neq 0$ such that $f_\lambda$ is bent. Since $n$ is even, we then have $\nu(f_\lambda) \geq 2^{2n+2}$ for all $\lambda$ which contradicts (8). Thus, $F$ is not APN.
ii) Suppose now that $F$ is APN. Thus, (8) holds implying that for some $\lambda$ we must have $\nu(f_\lambda) = 2^{2n}$, i.e. $f_\lambda$ is bent. More precisely

$$\sum_{\lambda \in \boldsymbol{F}_{2^n}^*} \nu(f_\lambda) = (2^n-1)2^{2n+1} = B2^{2n} + N2^{2n+2}$$

and $B + N \geq 2^n - 1$. We must have $B = 2(2^n-1) - 4N$ with $-N \leq B - (2^n-1)$. Hence, $B \leq 4B - 2(2^n-1)$ which leads to $B \geq 2\cdot(2^n-1)/3$ with equality if and only if $N = (2^n-1)/3$. It is equivalent to saying that any nonbent component $f_\lambda$ satisfies $\nu(f_\lambda) = 2^{2n+2}$ and $\mathcal{L}(f_\lambda) = 2^{(n+2)/2}$ (since it is plateaued). It implies that $\Lambda(F) = 2^{(n+2)/2}$. Conversely, assume that $B = 2\cdot(2^n-1)/3$ and $\Lambda(F) = 2^{(n+2)/2}$. Thus, the $(2^n-1)/3$ nonbent components satisfies $\nu(f_\lambda) = 2^{2n+2}$ and (8) holds.
iii) The functions $f_\lambda$ which are bent cannot be balanced. If $F$ is APN then there exists $\lambda$ such that $f_\lambda$ is bent. Thus, $F$ cannot be a permutation. Moreover, for any linear function $L$, the component $(F+L)_\lambda$ is equal to $f_\lambda + \varphi$ for some linear Boolean function $\varphi$. Therefore, it is bent, implying that $F + L$ is not a permutation. □

*Example 3:* There exist APN functions as characterized in the previous corollary. The most famous one is $F : x \mapsto x^3$ where $f_\lambda$ is bent if and only if $\lambda \neq a^3$ for all $a \in \boldsymbol{F}_{2^n}$. Note that $x \mapsto x^3$ is APN for any $n$; it is AB for odd $n$.

*Example 4:* Let us consider an APN function $F$ on $\boldsymbol{F}_{2^n}$ such that all its components $f_\lambda$, $\lambda \in \boldsymbol{F}_{2^n}^*$, are plateaued. When $n$ is odd, Corollary 2 implies that, for any function $G$ which has

the same extended Walsh spectrum as $F$, all components $g_\lambda$, $\lambda \in \boldsymbol{F}_{2^n}^*$, are plateaued optimal. For instance, the function

$$G : x \mapsto x^{2^i+1} + \left(x^{2^i} + x\right) \mathrm{Tr}\left(x^{2^i+1} + x\right),$$

$1 \leq i < \frac{n+1}{2}$, and $\gcd(i,n) = 1$, defined in [6] is *Carlet–Charpin–Zinoviev equivalent* to $x \mapsto x^{2^i+1}$. Therefore, $G$ is AB, implying that, for any $\lambda \neq 0$, we have $\nu(g_\lambda) = 2^{2n+1}$.

When $n$ is even, the situation is completely different. For instance, the APN function defined in [6]

$$G : x \mapsto x^{2^i+1} + (x^{2^i} + x + 1)\mathrm{Tr}(x^{2^i+1})$$

$1 \leq i < \frac{n}{2}$ and $\gcd(i,n) = 1$, has the same Walsh spectrum as $x^3$. But it does not imply that all its components are plateaued. For instance, for $n = 6$ and $i = 1$, $\nu(g_\lambda)$, $\lambda \neq 0$, takes 30 times the value $2^{12}$, 24 times the value $2^{13} + 2^{11}$, and 9 times the value $2^{14}$. Obviously, the $g_\lambda$ for which $\nu(g_\lambda) = 2^{13} + 2^{11}$ are not plateaued.

The preceding example points out that the APN property may lead to different sets $\{\nu(f_\lambda), \lambda \in \boldsymbol{F}_{2^n}^*\}$ whereas only one configuration is known in the odd case. A natural question is to determine whether the configuration that appears in the odd case may also occur when $n$ is even.

*Open Problem 2:* Does there exist an APN function $F$ of $\boldsymbol{F}_{2^n}$, $n$ even, such that $\nu(f_\lambda) = 2^{2n+1}$ for all $\lambda \in \boldsymbol{F}_{2^n}^*$?

### B. APN Permutations

The existence of APN permutations of an even number of variables is a major open problem, especially for the design of block ciphers since practical cryptosystems act on an even number of variables due to implementation constraints. In this subsection, we discuss this open problem.

*Open Problem 3:* Let $F$ be a permutation on $\boldsymbol{F}_{2^n}$, $n$ even. Is it possible for $F$ to be APN?

We will first review what is known about this problem.

*Theorem 3:* Let $F$ be any permutation on $\boldsymbol{F}_{2^n}$, $n = 2t$.
(o) If $n = 4$ then $F$ cannot be APN.
(i) If $F \in \boldsymbol{F}_4[x]$ then $F$ is not APN.
(ii) If $F \in \boldsymbol{F}_{2^t}[x]$ then $F$ is not APN.
(iii) If $F$ is such that all its components $f_\lambda$, $\lambda \in \boldsymbol{F}_{2^n}^*$, are plateaued then $F$ cannot be APN.

*Proof:* (o) was proved using a computer, for instance in [22]. (i) is easy to prove, since if $F \in \boldsymbol{F}_4[x]$ then $F(\boldsymbol{F}_4) = \boldsymbol{F}_4$. Thus, with $\boldsymbol{F}_4 = \{0, 1, \beta, \beta + 1\}$, we obtain

$$F(0) + F(1) + F(\beta) + F(\beta + 1) = 0.$$

(ii) was proved by Hou [22].

The following result was proved by Nyberg in [25]: *Let $n$ be even. If any permutation $F$ is such that all its components $f_\lambda$, $\lambda \in \boldsymbol{F}_{2^n}^*$, are partially bent then $F$ cannot be APN; in particular, there is no quadratic APN permutation of $\boldsymbol{F}_{2^n}$.* Partially bent functions are a kind of plateaued functions which have linear structures and the proof of Nyberg fruitfully used the necessary condition given by Theorem 2. Our Corollary 3 generalizes this result, proving (iii). □

Now, we show that APN permutations are completely characterized by the derivatives of their components. Recall that $F$ is a permutation on $\boldsymbol{F}_{2^n}$ if and only if all its components $f_\lambda$, $\lambda \in \boldsymbol{F}_{2^n}^*$ are balanced. It is well known that this is equivalent to

$$\sum_{a \in \boldsymbol{F}_{2^n}^*} \mathcal{F}(D_a f_\lambda) = -2^n, \quad \forall \lambda \in \boldsymbol{F}_{2^n}^*. \tag{9}$$

We can also use another characterization which leads to the following result.

*Proposition 2:* Let $F$ be a function from $\boldsymbol{F}_{2^n}$ into $\boldsymbol{F}_{2^n}$ with components $f_\lambda$, $\lambda \in \boldsymbol{F}_{2^n}^*$. Then $F$ is a permutation if and only if, for all $a \in \boldsymbol{F}_{2^n}^*$, we have

$$\sum_{\lambda \in \boldsymbol{F}_{2^n}^*} \mathcal{F}(D_a f_\lambda) = -2^n. \tag{10}$$

Consequently $F$ is an APN permutation if and only if, for any $a \in \boldsymbol{F}_{2^n}^*$

$$\sum_{\lambda \in \boldsymbol{F}_{2^n}^*} \mathcal{F}(D_a f_\lambda) = -2^n$$

and

$$\sum_{\lambda \in \boldsymbol{F}_{2^n}^*} \mathcal{F}^2(D_a f_\lambda) = 2^{2n}.$$

*Proof:*

$$\begin{aligned}\sum_{\lambda \in \boldsymbol{F}_{2^n}^*} \mathcal{F}(D_a f_\lambda) &= \sum_{\lambda \in \boldsymbol{F}_{2^n}^*} \sum_{x \in \boldsymbol{F}_{2^n}} (-1)^{\mathrm{Tr}(\lambda(F(x)+F(x+a)))} \\ &= \sum_{x \in \boldsymbol{F}_{2^n}} \sum_{\lambda \in \boldsymbol{F}_{2^n}^*} (-1)^{\mathrm{Tr}(\lambda(F(x)+F(x+a)))}.\end{aligned}$$

The last sum is clearly equal to $-2^n$ if and only if $F(x) + F(x + a) \neq 0$ for all $x$ and for all $a \neq 0$. This means that $F$ is a permutation. □

### C. APN Power Functions

More results on the APN property are known when we focus on the family of power functions, i.e., $F : x \mapsto x^d$ over $\boldsymbol{F}_{2^n}$. For instance, *if there is $h$ which divides $n$ and $d = k(2^h - 1) + 2^r$ for some $k$ and $r$ then $F$ is not APN* [17][13]. Also if $F$ is APN then $\gcd(d, 2^n - 1)$ is known. We present this last result, indicated by Dobbertin, in a more general context.

*Proposition 3:* Let $r$ be a divisor of $n$. Let $F$ be any function on $\boldsymbol{F}_{2^n}$. Assume that $F \in \boldsymbol{F}_{2^r}[x]$. If $F$ satisfies for some $a \in \boldsymbol{F}_{2^r}$

$$F(y) + F(y + a) = \beta, \quad \beta \in \boldsymbol{F}_{2^r}$$

for some $y$ such that $y \notin \boldsymbol{F}_{2^r}$ and $y^{2^r} + y + a \neq 0$, then $F$ is not APN.

Consequently, if $F$ is APN with $F(x) = x^d$, then $\gcd(d, 2^n - 1) = 1$ for odd $n$ and $\gcd(d, 2^n - 1) = 3$ for even $n$.

*Proof:* Since $F$ lies in $\boldsymbol{F}_{2^r}[x]$ then the polynomial $G(x) = F(x) + F(x+a)$ is in $\boldsymbol{F}_{2^r}[x]$ too. Let $y \notin \boldsymbol{F}_{2^r}$ such that the hypotheses are satisfied. Thus,

$$\begin{aligned}(G(y))^{2^r} &= \beta = F(y^{2^r}) + F(y^{2^r} + a)\\ &= F(y) + F(y+a)\end{aligned}$$

where $y^{2^r} \notin \{y, y+a\}$. According to Definition 2, $F$ cannot be APN.

Let $F(x) = x^d$ and set $s = \gcd(d, 2^n - 1)$. Note that such a polynomial $F$ is in $\boldsymbol{F}_2[x]$. Notably, it cannot be an APN permutation for even $n$. Assume that $s > 1$. Choose $y$ in $\boldsymbol{F}_{2^n} \setminus \boldsymbol{F}_2$ such that the order of $y$ equals $s$. Observe that $x \mapsto (x+1)/x$ is a bijection on $\boldsymbol{F}_{2^n} \setminus \{0, 1\}$ and set $y = (z+1)/z$. Then we get

$$\frac{(z+1)^d}{z^d} = 1, \quad \text{i.e.,} \ (z+1)^d + z^d = 0.$$

So, we have $z \notin \boldsymbol{F}_2$ such that $F(z) + F(z+1) = 0$. When $n$ is odd, it is impossible to have $z^2 + z + 1 = 0$. So, if $F$ is APN, the hypothesis $s > 1$ leads to a contradiction (according to the first part of the proposition). We then conclude that $s = 1$ for odd $n$.

Assume now that $n$ is even and $F$ is APN. This is possible only if $z^2 + z + 1 = 0$, that is, $z \in \boldsymbol{F}_4$ (so $y \in \boldsymbol{F}_4$). Then, in this case, $y = (z+1)/z \in \boldsymbol{F}_4$; hence $s = 3$. □

The fact that, for power functions, the APN property has a deeper relationship with the Walsh spectrum of the function is due to the following result.

*Proposition 4:* Let $F$ be any function on $\boldsymbol{F}_{2^n}$ of the form $x \mapsto x^d$. Let $f_\lambda$ denote the components of $F$. Set $s = \gcd(d, 2^n - 1)$ and $2^n - 1 = us$. Let $\alpha$ be a primitive element of $\boldsymbol{F}_{2^n}$. Then $\mathcal{F}(D_a f_\lambda) = \mathcal{F}(D_1 f_{\lambda a^d})$ for all $a, \lambda \in \boldsymbol{F}_{2^n}^*$.

Moreover

$$\nu(f_\lambda) = 2^{2n} + s\sum_{i=0}^{u-1} \mathcal{F}^2(D_1 f_{\lambda\alpha^{id}})$$

and

$$\sum_{\lambda \in \boldsymbol{F}_{2^n}} \mathcal{F}^2(D_a f_\lambda) = \frac{1}{s}\sum_{j=0}^{s-1} \nu(f_{\alpha^j}).$$

*Proof:* We have, for any nonzero $a$

$$\begin{aligned}\mathcal{F}(D_a f_\lambda) &= \sum_{x \in \boldsymbol{F}_{2^n}} (-1)^{\mathrm{Tr}(\lambda(x^d + (x+a)^d))}\\ &= \sum_{x \in \boldsymbol{F}_{2^n}} (-1)^{\mathrm{Tr}(\lambda a^d((\frac{x}{a})^d + (\frac{x}{a}+1)^d))}\\ &= \sum_{y \in \boldsymbol{F}_{2^n}} (-1)^{\mathrm{Tr}(\lambda a^d(y^d + (y+1)^d))}\\ &= \mathcal{F}(D_1 f_{\lambda a^d})\end{aligned}$$

by replacing $y = x/a$. Now,

$$\begin{aligned}\nu(f_\lambda) &= \sum_{a \in \boldsymbol{F}_{2^n}} \mathcal{F}^2(D_a f_\lambda)\\ &= 2^{2n} + \sum_{i=0}^{2^n-2} \mathcal{F}^2(D_1 f_{\lambda\alpha^{id}})\\ &= 2^{2n} + s\sum_{i=0}^{u-1} \mathcal{F}^2(D_1 f_{\lambda\alpha^{id}})\\ &= 2^{2n} + s\sum_{i=0}^{u-1} \mathcal{F}^2(D_1 f_{\lambda\alpha^{is}}) \qquad (11)\end{aligned}$$

since $\alpha^{vud} = 1$ for $1 \le v \le s-1$. Moreover, for any $a \in \boldsymbol{F}_{2^n}^*$, we have

$$\begin{aligned}\sum_{\lambda \in \boldsymbol{F}_{2^n}^*} \mathcal{F}^2(D_a f_\lambda) &= \sum_{\lambda \in \boldsymbol{F}_{2^n}^*} \mathcal{F}^2(D_1 f_{\lambda a^d})\\ &= \sum_{i=0}^{s-1}\sum_{j=0}^{u-1} \mathcal{F}^2(D_1 f_{\alpha^i \alpha^{js}})\end{aligned}$$

where the last equation is obtained by writing $\lambda = \alpha^{i+js}$ and $a^d = \alpha^{ks}$. We then deduce from (11) that

$$\sum_{\lambda \in \boldsymbol{F}_{2^n}^*} \mathcal{F}^2(D_a f_\lambda) = \frac{1}{s}\sum_{j=0}^{s-1} \left(\nu(f_{\alpha^j}) - 2^{2n}\right).$$

The result now comes from the fact that $\mathcal{F}^2(D_a f_\lambda) = 2^{2n}$ for $\lambda = 0$. □

Now, the situation when $n$ is odd is quite clear as pointed out in the following proposition. Note that this proposition includes all APN power functions since any APN power function is a permutation when $n$ is odd.

*Proposition 5:* Let $F$ be any function on $\boldsymbol{F}_{2^n}$ of the form $x \mapsto x^d$. Let $f_\lambda$ denote the components of $F$. Assume that $\gcd(d, 2^n - 1) = 1$. Then the $\nu(f_\lambda)$, $\lambda \in \boldsymbol{F}_{2^n}^*$, are equal and

$$\nu(f_1) = \sum_{\lambda \in \boldsymbol{F}_{2^n}} \mathcal{F}^2(D_1 f_\lambda).$$

Moreover, these statements, which are possible for odd $n$ only, are equivalent:

i) $F$ is an APN permutation;
ii) $\nu(f_\lambda) = 2^{2n+1}$ for some $\lambda$;
iii) $\sum_{\lambda \in \boldsymbol{F}_{2^n}} \mathcal{F}^2(D_1 f_\lambda) = 2^{2n+1}$.

*Proof:* According to the previous proposition, we have for any $\lambda$

$$\begin{aligned}\nu(f_\lambda) &= 2^{2n} + \sum_{i=0}^{2^n-2} \mathcal{F}^2(D_1 f_{\lambda\alpha^{id}})\\ &= \sum_{\mu \in \boldsymbol{F}_{2^n}} \mathcal{F}^2(D_1 f_\mu)\end{aligned}$$

since $s = 1$ and $x \mapsto x^d$ is a permutation on $\boldsymbol{F}_{2^n}$. The second statement is directly deduced from Theorem 2. Recall that $F$ cannot be APN for even $n$ (see Theorem 3 (iii)). □

The fact that $F$ APN, with $F(x) = x^d$ over $\boldsymbol{F}_{2^n}$ ($n$ odd), implies that $\nu(\mathrm{Tr}(x^d)) = 2^{2n+1}$ when $\gcd(d, 2^n - 1) = 1$, was proved by Helleseth [20] in another context (see also [10]).

Here again, the situation is very different when $n$ is even, as pointed out in the following theorem. Recall that $\Lambda(F)$ is defined by Definition 6. Note that it is conjectured that $\Lambda(F)$ cannot be less than $2^{(n+2)/2}$ for even $n$. We prove here that this is true for APN power functions.

*Theorem 4:* Let $n = 2t$ be an even integer and let $F$ be any function on $\boldsymbol{F}_{2^n}$ of the form $x \mapsto x^d$. Let $f_\lambda$ denote the components of $F$. Then, $F$ is APN if and only if

$$\nu(f_1) + 2\nu(f_\alpha) = 3 \cdot 2^{2n+1}$$

where $\alpha$ is a primitive element of $\boldsymbol{F}_{2^n}$.

Moreover, if $F$ is APN, then $\mathcal{F}(f_\lambda)$ equals

$$\begin{cases} (-1)^{t+1}2^{t+1}, & \text{if } \lambda \in \{x^3, x \in \boldsymbol{F}_{2^n}^*\} \\ (-1)^t 2^t, & \text{if } \lambda \notin \{x^3, x \in \boldsymbol{F}_{2^n}^*\} \end{cases}$$

implying that

$$\Lambda(F) \geq 2^{t+1}$$

i.e., the nonlinearity of such $F$ satisfies $\mathcal{N}(F) \leq 2^{n-1} - 2^t$.

*Proof:* Assume that $\gcd(d, 2^n - 1) = 3$. Thus, from Proposition 4, we have for any $a$

$$3 \sum_{\lambda \in \boldsymbol{F}_{2^n}} \mathcal{F}^2(D_a f_\lambda) = \nu(f_1) + 2\nu(f_\alpha)$$

where $\alpha$ is a primitive element of $\boldsymbol{F}_{2^n}$. This comes from the fact that $\nu(f_\alpha) = \nu(f_{\alpha^2})$ because both functions are linearly equivalent.

Recall that if $F : x \mapsto x^d$ is APN, we have $\gcd(d, 2^n - 1) = 3$ (see Proposition 3). Hence, according to Theorem 2, $F$ is APN if and only if

$$\nu(f_1) + 2\nu(f_\alpha) = 3 \cdot 2^{2n+1}.$$

Let $g_\lambda$, $\lambda \in \boldsymbol{F}_{2^n}$, denote the components of $G : x \mapsto x^3$ over $\boldsymbol{F}_{2^n}$. If $F : x \mapsto x^d$ is APN then $d = 3^r k$, $r > 0$, with $\gcd(d, 2^n - 1) = 3$. Thus, we have

$$\begin{aligned} \mathcal{F}(f_\lambda) &= \sum_{x \in \boldsymbol{F}_{2^n}} (-1)^{\mathrm{Tr}(\lambda x^d)} \\ &= \sum_{y \in \boldsymbol{F}_{2^n}} (-1)^{\mathrm{Tr}(\lambda y^{3^r})} \\ &= \sum_{z \in \boldsymbol{F}_{2^n}} (-1)^{\mathrm{Tr}(\lambda z^3)} = \mathcal{F}(g_\lambda). \end{aligned}$$

This is because $x \mapsto x^d$ is 3-to-1 from $\boldsymbol{F}_{2^n}^*$ to the set $\{z^3 | z \in \boldsymbol{F}_{2^n}\}$, since $u^d = v^d$ if and only if $(u/v)^3 = 1$, that is, $u = v\beta$ where $\beta \in \boldsymbol{F}_4^*$.

Now we have $\mathcal{F}(f_\lambda) = \mathcal{F}(g_\lambda)$ with $g_\lambda(x) = \mathrm{Tr}(\lambda x^3)$. The values of $\mathcal{F}(g_\lambda)$ were determined by Carlitz ([14, Theorem 1])

$$\mathcal{F}(g_\lambda) = \begin{cases} (-1)^{t+1}2^{t+1} \\ (-1)^t 2^t \end{cases}$$

according as $\lambda$ is or is not a cube in $\boldsymbol{F}_{2^n}^*$. We deduce that

$$\mathcal{F}(f_1) = -2^{t+1} \quad \text{and} \quad \mathcal{F}(f_\alpha) = 2^t;$$

for even $t$ and

$$\mathcal{F}(f_1) = 2^{t+1} \quad \text{and} \quad \mathcal{F}(f_\alpha) = -2^t$$

for odd $t$. Moreover, we have for any $t$

$$\Lambda(F) \geq |\mathcal{F}(f_1)| = 2^{t+1}.$$ □

*Example 5:* For APN power functions over $\boldsymbol{F}_{2^n}$, $n$ even, two different situations are known.

- For Gold exponents, $d = 2^i + 1$, $\gcd(i, n) = 1$, $1 \leq i < \frac{n}{2}$, we have

  $$\nu(f_1) = 2^{2n+2} \quad \text{and} \quad \nu(f_\alpha) = 2^{2n}.$$

  This corresponds to the situation described in Corollary 3. These functions achieve the highest possible nonlinearity for an APN power function as shown in the previous theorem.
- For Dobbertin's exponent, $d = 2^{4g} + 2^{3g} + 2^{2g} + 2^g - 1$ when $n = 5g$, we have for $n \in \{10, 20\}$

  $$\nu(f_1) = 2^{2n+1} + 2^{n+2g+1}(2^{2g} + 2^g - 1)$$

  and

  $$\nu(f_\alpha) = 2^{2n+1} - 2^{n+2g}(2^{2g} + 2^g - 1).$$

  Here, we have $\Lambda(F) > 2^{\frac{n}{2}+1}$.

### D. Functions With $\delta(F) \geq 4$

We previously focused on APN functions, i.e., the functions for which $\delta(F) = 2$ with

$$\delta(F) = \max_{a \neq 0, b \in \boldsymbol{F}_2^n} \#\{x \in \boldsymbol{F}_2^n, D_a F(x) = b\}.$$

Now, we point out that some results on the sum-of-square indicators of the components of $F$ can be derived from Nyberg's result [26], when $\delta(F) \geq 4$.

*Proposition 6:* Let $F$ be a function from $\boldsymbol{F}_{2^n}$ into $\boldsymbol{F}_{2^n}$ with components $f_\lambda$, $\lambda \in \boldsymbol{F}_{2^n}^*$. Then, there exists $a \in \boldsymbol{F}_{2^n}^*$ such that

$$\sum_{\lambda \in \boldsymbol{F}_{2^n}} \mathcal{F}^2(D_a f_\lambda) \geq 2^{2n+1} + 2^n \delta(F)(\delta(F) - 2).$$

*Proof:* We use the same notation as in Definition 2. Let $a \in \boldsymbol{F}_{2^n}^*$ be such that there exists $b \in \boldsymbol{F}_{2^n}$ with $\delta(a, b) = \delta(F)$. Let

$A_i$ denote the number of $b \in \boldsymbol{F}_{2^n}$ such that $\delta(a,b) = i$. Recall the following formula due to Nyberg [26]: for any $a \in \boldsymbol{F}_{2^n}^*$

$$\sum_{\lambda \in \boldsymbol{F}_{2^n}} \mathcal{F}^2(D_a f_\lambda) = 2^n \sum_{b \in \boldsymbol{F}_{2^n}} \delta^2(a,b).$$

We deduce the following:

$$2^{-n} \sum_{\lambda \in \boldsymbol{F}_{2^n}} \mathcal{F}^2(D_a f_\lambda) = \delta(F)^2 A_{\delta(F)} + \sum_{i=2}^{\delta(F)-2} i^2 A_i \geq \delta(F)^2 A_{\delta(F)} + 2 \sum_{i=2}^{\delta(F)-2} i A_i \quad (12)$$

with equality if and only if $\delta(a,b) \in \{\delta(F), 2, 0\}$ for all $b \in \boldsymbol{F}_{2^n}$. Moreover, we have

$$\sum_{i=2}^{\delta(F)-2} i A_i = 2^n - \delta(F) A_{\delta(F)}. \quad (13)$$

Thus,

$$\sum_{\lambda \in \boldsymbol{F}_{2^n}} \mathcal{F}^2(D_a f_\lambda) \geq 2^{2n+1} + 2^n \delta(F)(\delta(F) - 2)$$

with equality if and only if $A_{\delta(F)} = 1$ and $A_i = 0$ for all $4 \leq i \leq \delta(F) - 2$. □

*Corollary 4:* Let $F$ be a power permutation on $\boldsymbol{F}_{2^n}$, $n$ even, i.e.,

$$F(x) = x^d, \qquad \text{with } \gcd(d, 2^n - 1) = 1.$$

Let $f_\lambda$ denote the components of $f$. Then, all $\nu(f_\lambda)$, $\lambda \in \boldsymbol{F}_{2^n}^*$, are equal and satisfy

$$\nu(f_\lambda) \geq 2^{2n+1} + 2^{n+3}.$$

Moreover, if equality holds, then $\delta(F) = 4$.

*Proof:* When $F$ is a power permutation, we have from Proposition 5 that, for all $\lambda \in \boldsymbol{F}_{2^n}^*$

$$\nu(f_\lambda) = \sum_{\mu \in \boldsymbol{F}_{2^n}} \mathcal{F}^2(D_1 f_\mu).$$

Moreover, we know from Proposition 4 that, for any $a \in \boldsymbol{F}_{2^n}^*$

$$\sum_{\mu \in \boldsymbol{F}_{2^n}} \mathcal{F}^2(D_1 f_\mu) = \sum_{\mu \in \boldsymbol{F}_{2^n}} \mathcal{F}^2(D_a f_\mu).$$

From the previous proposition, we deduce that, for all $\lambda \in \boldsymbol{F}_{2^n}^*$

$$\nu(f_\lambda) \geq 2^{2n+1} + 2^n \delta(F)(\delta(F) - 2).$$

When $n$ is even, $F$ cannot be APN, i.e., $\delta(F) \geq 4$. Thus, it implies that

$$\nu(f_\lambda) \geq 2^{2n+1} + 2^{n+3}, \qquad \text{for all } \lambda \in \boldsymbol{F}_{2^n}^*. \quad (14)$$

Conversely, any power permutation which satisfies (14) with equality is such that $\delta(F) = 4$. Indeed, we clearly have that $\delta(F) \geq 4$ from Corollary 1. Moreover, for $\delta(F) \geq 6$, we would have

$$\nu(f_\lambda) \geq 2^{2n+1} + 3 \cdot 2^{n+3}, \qquad \text{for all } \lambda \in \boldsymbol{F}_{2^n}^*. \quad \square$$

*Example 6:* When $n$ is even, the inverse function $F : x \mapsto x^{2^n-2}$ over $\boldsymbol{F}_{2^n}$, which is used in the AES S-boxes, satisfies

$$\nu(f_\lambda) = 2^{2n+1} + 2^{n+3}, \qquad \text{for all } \lambda \in \boldsymbol{F}_{2^n}^*$$

(see Example 2). Then, the sum-of-square indicators of its components achieve the lowest possible value for a power permutation of $\boldsymbol{F}_{2^n}$ when $n$ is even.

Since it is still unknown whether APN permutations of $\boldsymbol{F}_{2^n}$ exist when $n$ is even, the use of permutations $F$ with $\delta(F) = 4$ is suitable in cryptographic applications. When $F$ is not a power function, the values

$$\sum_{\lambda \in \boldsymbol{F}_{2^n}} \mathcal{F}^2(D_a f_\lambda)$$

may differ when $a$ varies. We know from (12) and (13) that any function $F$ with $\delta(F) = 4$ satisfies

$$\sum_{\lambda \in \boldsymbol{F}_{2^n}} \mathcal{F}^2(D_a f_\lambda) = 2^{2n+1} + 2^{n+3} A_4(a)$$

where $A_4(a)$ is the number of $b \in \boldsymbol{F}_{2^n}$ such that $\delta(a,b) = 4$. Therefore, we have

$$\sum_{\lambda \in \boldsymbol{F}_{2^n}^*} \nu(f_\lambda) = (2^n - 1)2^{2n+1} + A 2^{n+3} \quad (15)$$

where $A = \sum_{a \in \boldsymbol{F}_{2^n}^*} A_4(a)$. Note that, if the sum-of-square indicators are such that (15) is satisfied for $A \in \{1, 2\}$, then $\delta(F) = 4$. Indeed, $\delta(F) = 2$ implies that

$$\sum_{\lambda \in \boldsymbol{F}_{2^n}^*} \nu(f_\lambda) = (2^n - 1)2^{2n+1}$$

from Corollary 1. Moreover, if $\delta(F) \geq 6$, we deduce from Proposition 6 and Theorem 2 that

$$\sum_{\lambda \in \boldsymbol{F}_{2^n}^*} \nu(f_\lambda) = \sum_{a \in \boldsymbol{F}_{2^n}^*} \sum_{\lambda \in \boldsymbol{F}_{2^n}} \mathcal{F}^2(D_a f_\lambda) \geq (2^n - 1)2^{2n+1} + 3 \cdot 2^{n+3}.$$

The case $A = 2^n - 1$ in (15) is achieved by the inverse function which is such that $A_4(a) = 1$ for any nonzero $a$. However, we can wonder whether some functions $F$ with $\delta(F) = 4$ achieve a lower value for $A$. Thus, the following open problem arises.

*Open Problem 4:* Find a permutation $F$ on $\boldsymbol{F}_{2^n}$, $n$ even, with components $f_\lambda$, $\lambda \in \boldsymbol{F}_{2^n}^*$, such that $\delta(F) = 4$ and

$$\sum_{\lambda \in \boldsymbol{F}_{2^n}^*} \nu(f_\lambda) = (2^n - 1)2^{2n+1} + A 2^{n+3}$$

for some integer $A < 2^n - 1$.

## IV. Quadratic APN Functions

An infinite class of quadratic APN functions, which are not equivalent to any power function, was characterized very recently (see [5] and [19]). This disproves a conjecture on APN

functions of degree 2, saying that such functions are equivalent to the power functions $x \mapsto x^{2^k+1}$ over $\boldsymbol{F}_{2^n}$ with $\gcd(k,n)=1$ and $1 \leq k \leq n/2$. Here, we contribute to the classification of APN quadratic functions. We prove that there are no APN quadratic functions on $\boldsymbol{F}_{2^n}$ of the form

$$F(x) = \sum_{i=1}^{n-1} c_i x^{2^i+1}, \quad c_i \in \boldsymbol{F}_{2^n} \tag{16}$$

except the previously mentioned power functions. We will use the Hermite's criterion. A proof of the next theorem can be found in ([24, Theorem 7.4]).

*Theorem 5:* [Hermite's criterion] Let $\boldsymbol{F}_q$ be any finite field of characteristic $p$. Then a polynomial $P \in \boldsymbol{F}_q[x]$ is a permutation polynomial of $\boldsymbol{F}_q$ if and only if both of the following conditions hold:

i) $P$ has exactly one root in $\boldsymbol{F}_q$;
ii) for each integer $t$ with $1 \leq t < q-1$ such that $t \not\equiv 0 \pmod p$, the degree of $P(x)^t \pmod{x^q - x}$ is less than or equal to $q-2$.

In order to specify our purpose, we first discuss some open problems.

### A. Some Open Problems

Let $F$ be a quadratic function on $\boldsymbol{F}_{2^n}$. Then, for any $a$, the function $D_aF$ is affine or constant. Thus, it is obviously deduced from Proposition 1:

*Corollary 5:* Any quadratic function $F$ on $\boldsymbol{F}_{2^n}$ is APN if and only if for all nonzero $a$, the set $\{D_aF(x), x \in \boldsymbol{F}_2^n\}$ is a flat of codimension 1.

Recall that when $n$ is odd then any quadratic function $F$ is APN if and only if it is AB, that is, all coordinate functions of $F$ are plateaued optimal. Note that we proved this property for nonquadratic functions by Corollary 2.

More generally, Bending *et al.* introduced *crooked* functions in [1], [30]. Such a function $F$ is defined on $\boldsymbol{F}_{2^n}$ with $n$ odd and is such that for all nonzero $a$, the set $\{D_aF(x), x \in \boldsymbol{F}_2^n\}$ is an affine hyperplane. Note that Nyberg and Knudsen, in an earlier paper, have already described the quadratic functions (for odd $n$) which satisfy this last property [28]. Crooked functions are AB and the only known *crooked* functions are quadratic.

*Open Problem:* Construct crooked functions which are not quadratic.

Another problem is about the characterization of APN quadratic functions which are not affinely equivalent to a power function. Note that in [6], [7], Budaghyan, Carlet, and Pott exhibited the first known APN functions which are not affinely equivalent to a power function, but these are of degree greater than 2. The first class of APN quadratic functions, not equivalent to a power function, was recently shown in [5] and [19]. It is composed of binomials of $\boldsymbol{F}_{2^n}[x]$ with $n = 3k$ and $\gcd(3,k) = 1$. So, the existence of a similar class for $n \neq 3k$ remains an open problem.

Clearly, the classification of APN quadratic functions is not yet achieved. In the next section, we prove that the class of quadratic functions defined by (16) is APN only when it is an APN power function. Notably, our next Theorem 6 has the following consequence.

*Proposition 7:* Let $F$ be any quadratic function which is not a power function. Then if $F$ is APN its expression contains at least one term of the form $cx^{2^i+2^j}$, $c \in \boldsymbol{F}_{2^n}^*$, where $i > 0$ and $j > 0$.

### B. On A Class of Quadratic Functions

Note that (16) is not the general expression of quadratic functions on $\boldsymbol{F}_{2^n}$ since it does not include any term of the form $x^{2^i+2^j}$, with $i, j > 0$. On the other hand, note that if $F$ is APN then $F+L$ is APN too, where $L$ is any affine polynomial. We first prove a useful lemma in order to characterize the APN property for the class of quadratic functions defined by (16).

*Lemma 1:* Let $H$ be a polynomial on $\boldsymbol{F}_{2^n}$ such that $H(0) = 0$ and satisfying

$$\forall a, \forall b, a \neq b \neq 0, \quad H(a) \neq H(b)$$

and $H(e) = 0$ for a unique $e \neq 0$. Then the degree of $H$ is exactly $2^n - 1$.

*Proof:* Since $H(0) = H(e) = 0$, then $H$ is not a permutation. The image of $H$, i.e., the set $I = \{H(x) | x \in \boldsymbol{F}_{2^n}\}$, contains exactly $2^n - 1$ elements, including 0, which appears twice. Thus, there is only one nonzero element, say $\beta \in \boldsymbol{F}_{2^n}^*$, which is not in $I$. Let us define the polynomial $P$ on $\boldsymbol{F}_{2^n}$ by

$$P(x) = \begin{cases} H(x), & \text{for } x \neq e \\ \beta, & \text{for } x = e. \end{cases}$$

Then the image of $P$ has cardinality $2^n$, meaning that $P$ is a permutation. Now we are going to express the polynomial $W = H+P$. Note that, from the definition of $P$, $W(x) = 0$ unless $x = e$ and $W(e) = P(e) = \beta$. We claim that the unique representation of $W$ modulo $x^{2^n} + x$ is

$$W(x) = \beta\left((x+e)^{2^n-1} + 1\right).$$

This is simply because the right-hand polynomial above has degree $2^n - 1$ and is equal to $W$ for each $x$. Thus, we proved that

$$P(x) = H(x) + \beta\left((x+e)^{2^n-1} + 1\right).$$

Since $P$ is a permutation, its degree is at most $2^n - 2$ (from Theorem 5). This implies that $H$ must have the term $\beta x^{2^n-1}$; its degree is $2^n - 1$. □

*Proposition 8:* Let $F$ be defined by (16). Then, $F$ is APN if and only if the polynomial $Q : x \mapsto F(x)/x^2$, i.e.,

$$Q(x) = \sum_{i=1}^{n-1} c_i x^{2^i-1} \tag{17}$$

is a permutation polynomial on $\boldsymbol{F}_{2^n}$.

*Proof:* For any $a \in \boldsymbol{F}_{2^n}^*$, we have

$$D_aF(x) = \sum_{i=1}^{n-1} c_i \left(x^{2^i}a + xa^{2^i}\right) + F(a).$$

Then, the set $\{D_aF(x), x \in \boldsymbol{F}_2^n\}$ has cardinality $2^{n-1}$ if and only if the affine polynomial $D_aF$ has a kernel of dimension 1, i.e.,

$$\sum_{i=1}^{n-1} c_i \left(x^{2^i}a + xa^{2^i}\right) \neq 0, \qquad \text{for all } x \notin \{0, a\}$$

or, equivalently, $Q(x) \neq Q(a)$ for all $x \notin \{0, a\}$ (by dividing by $xa$ the polynomial above). Therefore, $F$ is APN if and only if for any two distinct $a$ and $b$ in $\boldsymbol{F}_{2^n}^*$, $Q(a) \neq Q(b)$. Moreover, if there exists $a \neq 0$ such that $Q(a) = Q(0) = 0$, this element $a$ is unique. In this case, we know from Lemma 1 that $Q$ has degree $2^n - 1$, which is impossible. Therefore, the previous condition is equivalent to the fact that $Q$ is a permutation polynomial.

Now, using Hermite's criterion, the permutation polynomials of the form (17) are completely characterized. The first part of the next theorem was actually proved by Payne [29] in another context, the general problem of *the complete determination of all ovoids in the projective plane* $\mathrm{PG}(2, 2^s)$. For a detailed proof, in our context, see [2] and [3].

*Theorem 6:* A polynomial of $\boldsymbol{F}_{2^n}[x]$ of the form

$$Q(x) = \sum_{i=1}^{n-1} c_i x^{2^i-1}, \qquad c_i \in \boldsymbol{F}_{2^n} \tag{18}$$

cannot be a permutation polynomial unless $Q(x) = cx^{2^k-1}$ with $\gcd(k, n) = 1$ and $c \in \boldsymbol{F}_{2^n}^*$.

Consequently, a quadratic function $F$ over $\boldsymbol{F}_{2^n}$ of the form (16) is APN if and only if $F(x) = cx^{2^k+1}$ with $\gcd(k, n) = 1$ and $c \in \boldsymbol{F}_{2^n}^*$.

*Proof:* It was proved by Payne [29] that any polynomial of the form (18), with at least two terms, cannot be a permutation (see also [21, Lemma 8.40]). When $Q(x) = cx^{2^k-1}$ then $Q$ is a permutation if and only if $\gcd(k, n) = 1$. The proof is completed by applying Proposition 8 to the functions defined by (16). □

## V. Conclusion

During this work, our main purpose was to tackle several open problems on APN functions. Our main results deal with nonlinearity, APN permutations, and quadratic APN functions. Despite these results, we point out that a number of interesting problems remain open and that these are difficult problems. Among those open issues, one of the most important ones from a cryptographic point of view is the existence of APN permutations depending on an even number of variables. We want to mention also (in the even case) that our result on the nonlinearity of APN power functions is conjectured to be true for any power function, for a long time. In the last part of this paper, we emphasize that the theoretical study of quadratic functions remains of great interest.

## Acknowledgment

The authors would like to thank the anonymous reviewers who, by numerous comments and suggestions, have contributed to improve the manuscript.

## References

[1] T. Bending and D. F. Der Flass, "Crooked functions, bent functions, and distance regular graphs," *Electron. J. Combin.*, vol. 5, no. 1, 1998, R34.

[2] T. P. Berger, A. Canteaut, P. Charpin, and Y. Laigle-Chapuy, "On almost perfect nonlinear functions," in *Proc. IEEE Int. Symp. Information Theory*, Adelaide, Australia, Sep. 2005.

[3] ——, Almost perfect nonlinear functions Res. Rep. INRIA, RR-5774, 2005 [Online]. Available: http://www.inria.fr/rrrt/

[4] E. Biham and A. Shamir, "Differential cryptanalysis of des-like cryptosystems," *J. Cryptol.*, vol. 4, no. 1, pp. 3–72, 1991.

[5] L. Budaghyan, C. Carlet, P. Felke, and G. Leander, An Infinite Class of Quadratic APN Functions Which are not Equivalent to Power Mappings Cryptology ePrint Archive Rep. 2005/359, 2005 [Online]. Available: http://eprint.iacr.org/

[6] L. Budaghyan, C. Carlet, and A. Pott, "New constructions of almost bent and almost perfect nonlinear polynomials," in *Proc. Workshop on Coding and Cryptography—WCC 2005*, Bergen, Norway, Mar. 2005, pp. 306–315.

[7] ——, "New classes of almost bent and almost perfect nonlinear polynomials," *IEEE Trans. Inf. Theory*, vol. 52, no. 3, pp. 1141–1152, Mar. 2006.

[8] A. Canteaut, C. Carlet, P. Charpin, and C. Fontaine, "Propagation characteristics and correlation-immunity of highly nonlinear boolean functions," in *Advances in Cryptology—Eurocrypt 2000 Volume 1807 of Lecture Notes in Computer Science*. Berlin, Germany: Springer-Verlag, 2000, pp. 507–522.

[9] ——, "On cryptographic properties of the cosets of $R(1, m)$," *IEEE Trans. Inf. Theory*, vol. 47, no. 4, pp. 1494–1513, May 2001.

[10] A. Canteaut, P. Charpin, and H. Dobbertin, "Binary $m$-sequences with three-valued crosscorrelation: A proof of welch conjecture," *IEEE Trans. Inf. Theory*, vol. 46, no. 1, pp. 4–8, Jan. 2000.

[11] ——, "Weight divisibility of cyclic codes, highly nonlinear functions on GF(2 m) and crosscorrelation of maximum-length sequences," *SIAM J. Discr. Math.*, vol. 13, no. 1, pp. 105–138, 2000.

[12] C. Carlet, "Partially-bent functions," *Des., Codes, Cryptogr.*, no. 3, pp. 135–145, 1993.

[13] C. Carlet, P. Charpin, and V. Zinoviev, "Codes, bent functions and permutations suitable for DES-like cryptosystems," *Des., Codes, Cryptogr.*, vol. 15, no. 2, pp. 125–156, 1998.

[14] L. Carlitz, "Explicit evaluation of certain exponential sums," *Math. Scand.*, vol. 44, pp. 5–16, 1979.

[15] F. Chabaud and S. Vaudenay, "Links between differential and linear cryptanalysis," in *Advances in Cryptology—EUROCRYPT'94 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1995, vol. 950, pp. 356–365.

[16] P. Charpin, T. Helleseth, and V. Zinoviev, "Propagation characteristics of $x \mapsto x^{-1}$ and Kloosterman sums," *Finite Fields Appl.*, to be published.

[17] P. Charpin, A. Tietäväinen, and V. Zinoviev, "On binary cyclic codes with minimum distance $d = 3$," *Probl. Inf. Transm.*, vol. 33, no. 4, pp. 287–296, 1997.

[18] H. Dobbertin, "Almost perfect nonlinear power functions on $\mathrm{GF}(2^n)$: A new class for $n$ divisible by 5," in *Proc. Finite Fields and Applications Fq5*. Berlin, Germany: Springer-Verlag, 2000, pp. 113–121.

[19] Y. Edel, G. Kyureghyan, and A. Pott, "A new APN function which is not equivalent to a power mapping," *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 744–747, Feb. 2006.

[20] T. Helleseth, "Some results about the cross-correlation function between two maximal linear sequences," *Discr. Math.*, vol. 16, pp. 209–232, 1976.

[21] J. W. P. Hirschfeld, *Projective Geometries Over Finite Fields*, 2nd ed. London, U.K.: Clarendon, 1998, Oxford Mathematical Monographs.

[22] X.-D. Hou, "Affinity of permutations of $\boldsymbol{F}_2^n$," *Discr. Appl. Math.*, vol. 154, pp. 313–325, 2006.

[23] G. Lachaud and J. Wolfmann, "The weights of the Orthogonals of the extended quadratic binary Goppa codes," *IEEE Trans. Inf. Theory*, vol. 36, no. 3, pp. 686–692, May 1990.

[24] R. Lidl and H. Niederreiter, *Finite Fields*. Cambridge, U.K.: Cambridge Univ. Press, 1983.

[25] K. Nyberg, "Differentially uniform mappings for cryptography," in *Advances in Cryptology—EUROCRYPT'93, Volume 765 of Lecture Notes in Computer Science*. Berlin, Germany: Springer-Verlag, 1993, pp. 55–64.

[26] ——, "S-boxes and round functions with controllable linearity and differential uniformity," in *Fast Software Encryption—FSE'94 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1995, vol. 1008, pp. 111–130.

[27] K. Nyberg and L. R. Knudsen, "Provable security against differential cryptanalysis," in *Advances in Cryptology—CRYPTO'92 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1993, vol. 740, pp. 566–574.

[28] K. Nyberg and L. R. Knudsen, "Provable security against a differential attack," *J. Cryptol.*, vol. 8, no. 1, 1995.

[29] S. E. Payne, "A complete determination of translation ovoids in finite Desarguian planes," *Lincei—Rend. Sc. Fis. Mat. E Nat.*, vol. LI, Nov. 1971.

[30] E. R. V. Dam and D. F. D. Flass, Codes, Graphs, and Schemes from Nonlinear Functions, Tilburg Univ., Tilburg, The Netherlands, Tech. Rep., Res. Memo., FEW 790, May 2000.

[31] X.-M. Zhang and Y. Zheng, "GAC—The criterion for global avalanche characterics of cryptographic functions," *J. Universal Comp. Sci.*, vol. 1, no. 5, pp. 320–337, 1995.

[32] Y. Zheng and X.-M. Zhang, "Plateaued functions," in *Information and Communication Security, ICICS'99 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1999, vol. 1726, pp. 284–300.