Vectorial Boolean Functions for Cryptography

Claude Carlet*

June 1, 2008

To appear as a chapter of the volume "Boolean Methods and Models", published by Cambridge University Press, Eds Yves Crama and Peter Hammer

*University of Paris 8; also with INRIA, Projet CODES (address: BP 105 - 78153, Le Chesnay Cedex, FRANCE); e-mail: claude.carlet@inria.fr.

Contents

1 Introduction

This chapter, which deals with multi-output Boolean functions viewed from a cryptographic viewpoint, follows the previous one (dedicated to Boolean functions). It focuses on functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ (where $\mathbb{F}_2$ is the finite field with two elements, denoted by $\mathcal{B}$ in some chapters of the present volume), but many results can also be stated for mappings between Abelian groups (see [37], for instance). *We refer to the chapter "Boolean Functions for Cryptography and Error Correcting Codes" for all the definitions and properties concerning Boolean functions and error correcting codes, that will be needed in the present chapter.* As in the chapter "Boolean Functions for Cryptography and Error Correcting Codes", additions of bits performed not modulo 2 will be denoted by $+$, and additions calculated modulo 2 will be denoted by $\oplus$. All the multiple sums calculated in characteristic 0 will be denoted by $\sum_i$ and all the sums calculated modulo 2 will be denoted by $\bigoplus_i$. For simplicity and because there will be no ambiguity, we shall denote by $+$ the addition of vectors of $\mathbb{F}_2^n$ or of elements of the finite field $\mathbb{F}_{2^n}$.

Let n and m be two positive integers. The mappings from the vectorspace $\mathbb{F}_2^n$, of all binary vectors of length n, to the vectorspace $\mathbb{F}_2^m$, are called (n,m)-*functions*. Such function F being given, the Boolean functions $f_1, \ldots, f_m$ defined, at every $x \in \mathbb{F}_2^n$, by $F(x) = (f_1(x), \ldots, f_m(x))$, are called the *coordinate functions* of F. When the numbers m and n are not specified, (n,m)-functions are called *multi-output Boolean functions*, *vectorial Boolean functions* or *S-boxes*[1].

They play a central role in iterative *block ciphers*. The round functions of these ciphers consist of vectorial Boolean functions combined in different ways involving the key, and the whole ciphers are finally formed by iterating certain numbers of rounds. See the chapter "Boolean Functions for Cryptography and Error Correcting Codes" for figures displaying the places of the S-boxes in the two main block ciphers: DES and AES.
The main attacks on block ciphers are the following. The *differential attack*, introduced by Biham and Shamir [7], uses the existence of ordered pairs (α, β) of binary strings such that, a plaintext block m being randomly chosen, the bitwise difference between the ciphertexts c and c' corresponding to m and $m \oplus \alpha$ is more likely equal to β than if c and c' were randomly chosen; let us call a differential such an ordered pair (α, β). The related

[1] "S" for "Substitution". The term of S-box is most often used to designate more precisely those vectorial Boolean functions whose role is to provide confusion (see Subsection 4.1 of the chapter "Boolean Functions for Cryptography and Error Correcting Codes" for the meaning of this term).

criterion on the S-boxes used in the round functions of the cipher is that the output to their derivatives (see definition at Proposition 2) be as uniformly distributed as possible (except for the derivatives at 0, obviously). There are several ways to mount the attack of differential cryptanalysis. The most common one is to use differentials for the *reduced cipher*, that is, the input to the last round (*i*.e. the cipher obtained from the original one by removing its last round); this allows to distinguish the reduced cipher from a random permutation and the existence of such *distinguisher* allows to recover the key used in the last round (either by an exhaustive search if this key is shorter than the master key, or by using specificities of the cipher). The *linear attack*, introduced by Matsui [91], and based on an idea from [105], uses as distinguishers triples (α, β, γ) of binary strings such that, a plaintext block m and a key k being randomly chosen, and $\alpha \cdot m$ denoting the usual inner product, the bit $\alpha \cdot m \oplus \beta \cdot c \oplus \gamma \cdot k$ has (significantly enough) a probability different from $1/2$ of being null. The related criterion on the S-boxes used in the round functions of the cipher is that the linear combinations, with coefficients not all null, of the coordinate functions of each S-box (the so-called *component functions*) have nonlinearities (see definition in the chapter "Boolean Functions for Cryptography and Error Correcting Codes", at Subsection 4.1) as high as possible. The *higher order differential attack* [87] exploits the fact that the algebraic degree of the S-box is low and the *interpolation attack* [76] is efficient when the degree of the univariate polynomial representation of the S-box over $\mathbb{F}_{2^n}$ – see the next page – has low degree. *Algebraic attacks* also exist on block ciphers (see *e.g.* [48]), exploiting the existence of multivariate equations involving the input to the S-box and its output (an example of such equation is $xy = 1$ in the case of the AES), but their efficiency has to be more precisely studied.

In the *pseudo-random generators* of *stream ciphers*, (n, m)-functions can be used to combine the outputs to n linear feedback shift registers (LFSR), or to filter the content of a single one, generating then m bits at each clock cycle instead of only one, which increases the speed of the cipher (but risks decreasing its robustness). The attacks, described in the chapter "Boolean Functions for Cryptography and Error Correcting Codes", are obviously also efficient on these kinds of ciphers.

1.1 Representation of vectorial functions

• The notion of *algebraic normal form* of Boolean functions can easily be extended to (n, m)-functions. Such a function F is uniquely represented as

a polynomial on n variables with coefficients in $\mathbb{F}_2^m$:

$$F(x) = \sum_{I \in \mathcal{P}(N)} a_I \left(\prod_{i \in I} x_i \right) = \sum_{I \in \mathcal{P}(N)} a_I \, x^I, \tag{1}$$

where $\mathcal{P}(N)$ denotes the power set of $N = \{1, \ldots, n\}$, and a_I belongs to $\mathbb{F}_2^m$. This polynomial is called again the algebraic normal form (ANF) of F. Its existence and uniqueness, can be deduced from those of the ANF of the coordinate functions of F. According to the relations recalled at Subsection 2.1 of the chapter "Boolean Functions for Cryptography and Error Correcting Codes", a_I equals $\sum_{x \in \mathbb{F}_2^n / \; supp(x) \subseteq I} F(x)$ (this sum being calculated in $\mathbb{F}_2^n$). Conversely, we have $F(x) = \sum_{I \subseteq supp(x)} a_I$.
The *algebraic degree* of the function is by definition the degree of its ANF: $d^\circ F = \max\{|I| / \, a_I \neq (0, \ldots, 0); I \in \mathcal{P}(N)\}$. It therefore equals the maximum algebraic degree of the coordinate functions of F. It is a *right and left affine invariant* (that is, its value does not change when we compose F, on the right or on the left, by an affine automorphism). Another notion of degree is also relevant to cryptography: the minimum algebraic degree of all the nonzero linear combinations of the coordinate functions of F, often called the *minimum degree*.
• A second representation of (n, m)-functions exists when $m = n$: we endow $\mathbb{F}_2^n$ with the structure of the field $\mathbb{F}_{2^n}$, as explained in the chapter "Boolean Functions for Cryptography and Error Correcting Codes" (see "The trace representation", at Subsection 2.1); any (n, n)-function F then admits a unique representation as a univariate polynomial over $\mathbb{F}_{2^n}$, of degree at most $2^n - 1$:

$$F(x) \;=\; \sum_{j=0}^{2^n - 1} \delta_j x^j \;, \quad \delta_j \in \mathbb{F}_{2^n} \;. \tag{2}$$

Indeed, the (linear) mapping which maps any such polynomial to the corresponding (n, n)-function is clearly linear and has kernel $\{0\}$ (since a nonzero univariate equation of degree at most $2^n - 1$ over a field can not have more than $2^n - 1$ solutions). The dimensions of the vectorspaces of, respectively, all such polynomials, and all (n, n)-functions, being equal to each other, this mapping is bijective.
The way to obtain the ANF from this *univariate polynomial* representation is the following: let us change x into $\sum_{i=1}^n x_i \alpha_i$, where $(\alpha_1, \ldots, \alpha_n)$ is a basis of the $\mathbb{F}_2$-vectorspace $\mathbb{F}_{2^n}$, and write the binary expansion of j: $\sum_{s=0}^{n-1} j_s 2^s$,

$j_s \in \{0,1\}$. We have:

$$\begin{aligned} F(x) &= \sum_{j=0}^{2^n-1} \delta_j \left(\sum_{i=1}^{n} x_i \alpha_i \right)^j \\ &= \sum_{j=0}^{2^n-1} \delta_j \left(\sum_{i=1}^{n} x_i \alpha_i \right)^{\sum_{s=0}^{n-1} j_s 2^s} \\ &= \sum_{j=0}^{2^n-1} \delta_j \prod_{s=0}^{n-1} \left(\sum_{i=1}^{n} x_i \alpha_i^{2^s} \right)^{j_s}. \end{aligned}$$

Expanding these last products, simplifying and decomposing again over the basis $(\alpha_1, \ldots, \alpha_n)$ will give the ANF of F.
It is then possible to read the algebraic degree of F directly on the univariate polynomial representation: let us denote by $w_2(j)$ the number of nonzero coefficients j_s in the binary expansion $\sum_{s=o}^{n-1} j_s 2^s$ of j, *i.*e. $w_2(j) = \sum_{s=0}^{n-1} j_s$. The number $w_2(j)$ is called the *2-weight* of j. Then, function F has algebraic degree $\max_{j=0,\ldots,2^n-1/\,\delta_j \neq 0} w_2(j)$. Indeed, according to the above equalities, its algebraic degree is clearly upper bounded by this number, and it can not be strictly smaller, because the number of those (n,n)-functions of algebraic degrees at most d equals the number of those univariate polynomials $\sum_{j=0}^{2^n-1} \delta_j x^j$, $\delta_j \in \mathbb{F}_{2^n}$, such that $\max_{j=0,\ldots,2^n-1/\,\delta_j \neq 0} w_2(j) \leq d$.
In particular, F is linear (resp. affine) if and only if $F(x)$ is a *linearized polynomial* over $\mathbb{F}_{2^n}$: $\sum_{j=0}^{n-1} \delta_j x^{2^j}$, $\delta_j \in \mathbb{F}_{2^n}$ (resp. a linearized polynomial plus a constant).
- If m is a divisor of n, then any (n,m)-function F can be viewed as a function from $\mathbb{F}_{2^n}$ to itself, since $\mathbb{F}_{2^m}$ is a sub-field of $\mathbb{F}_{2^n}$. Hence, the function admits a univariate polynomial representation. More precisely, it can be represented in the form $tr_{n/m}(\sum_{j=0}^{2^n-1} \delta_j x^j)$, where $tr_{n/m}$ is the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$. Indeed, there exists a function G from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ such that F equals $tr_{n/m} \circ G$ (for instance, $G(x) = \lambda F(x)$, where $tr_{n/m}(\lambda) = 1$).
• We shall call *Walsh transform* of F the function which maps any $(u,v) \in \mathbb{F}_2^n \times \mathbb{F}_2^{m*}$ to $\sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot F(x) \oplus u \cdot x}$ (that is, the value at u of the discrete Fourier transform of the *sign function* $(-1)^{v \cdot F}$, or in other terms the Walsh transform of the Boolean function $v \cdot F$). K. Nyberg derives from it in [97] a polynomial representation, that she calls the *multidimensional Walsh transform*: she defines the polynomial

$$\mathcal{W}(F)(x_1, \cdots, x_m) = \sum_{x \in \mathbb{F}_2^n} \prod_{j=1}^{m} x_j^{f_i(x)} \in \mathbb{Z}[x_1, \cdots, x_m]/(x_1^2 - 1, \cdots, x_m^2 - 1),$$

where $f_1, \cdots, f_m$ are the coordinate functions of F and the multidimensional Walsh transform maps every linear (n,m)-function L to the polynomial $\mathcal{W}(F+L)(x_1, \cdots, x_m)$. This is a representation with uniqueness of F, since, for every L, the knowledge of $\mathcal{W}(F+L)$ is equivalent to that of the evaluation of $\mathcal{W}(F+L)$ at $(\chi_1, \cdots, \chi_m)$ for every choice of χ_j, $j = 1, \cdots, m$, in the set $\{-1, 1\}$ of the roots of the polynomial $x_j^2 - 1$. For such a choice, let us define the vector $v \in \mathbb{F}_2^m$ by $v_j = 1$ if $\chi_j = -1$ and $v_j = 0$ otherwise. Then this evaluation equals $\sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot F(x) \oplus u \cdot x}$, where $u = \sum_{j=1}^m v_j L_j \in \mathbb{F}_2^n$, where L_j is the vector such that the j-th coordinate of $L(x)$ equals $L_j \cdot x$. It is then a simple matter to see that knowing the multidimensional Walsh transform of F is equivalent to knowing its Walsh transform. Obviously and for the same reasons, the multidimensional Walsh transform satisfies a Paeseval's relation.

1.2 Balanced functions

An (n,m)-function F is called *balanced* if it takes every value of $\mathbb{F}_2^m$ the same number 2^{n-m} of times. Let us denote, for every $b \in \mathbb{F}_2^m$, by φ_b the indicator function of the pre-image $F^{-1}(b) = \{x \in \mathbb{F}_2^n / F(x) = b\}$, defined by $\varphi_b(x) = 1$ if $F(x) = b$ and $\varphi_b(x) = 0$ otherwise, then, F is balanced if every such function φ_b has Hamming weight 2^{n-m}.
Obviously, the balanced (n,n)-functions are the permutations on $\mathbb{F}_2^n$.
The S-boxes, used in block or stream ciphers, are preferably balanced.

Proposition 1 *[89] An (n,m)-function is balanced if and only if every nonzero linear combination of its coordinate functions is balanced, or equivalently, if and only if the Boolean function $v \cdot F$ is balanced for every $v \in \mathbb{F}_2^m$, $v \neq 0$.*

Proof. The function φ_b being defined as above, the relation:

$$\sum_{v \in \mathbb{F}_2^m} (-1)^{v \cdot (F(x)+b)} = \begin{cases} 2^m \text{ if } F(x) = b \\ 0 \text{ otherwise} \end{cases} = 2^m \, \varphi_b(x), \tag{3}$$

is valid for every $x \in \mathbb{F}_2^n$, every $b \in \mathbb{F}_2^m$ and every (n,m)-function F, since the function $v \mapsto v \cdot (F(x) + b)$ is linear. Thus:

$$\sum_{x \in \mathbb{F}_2^n ; v \in \mathbb{F}_2^m} (-1)^{v \cdot (F(x)+b)} = 2^m \, |F^{-1}(b)| = 2^m \; w_H(\varphi_b). \tag{4}$$

Hence, the discrete Fourier transform of the function $v \mapsto \sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot F(x)}$ equals the function $b \mapsto 2^m \; |F^{-1}(b)|$, and F is balanced if and only if the

function $v \mapsto \sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot F(x)}$ is null on $\mathbb{F}_2^{m*}$. $\diamond$

The notion of covering sequence of a balanced Boolean function has been generalized to vectorial functions and the properties of this generalization have been studied in [42].

The notion of algebraic immunity of S-boxes has been studied in [1].

2 Nonlinearities of S-boxes

2.1 Nonlinearity of S-boxes in block ciphers; bent, almost bent and almost perfect nonlinear functions

A generalization to (n, m)-functions of the notion of nonlinearity of Boolean functions has been introduced by Nyberg [93] and studied by Chabaud and Vaudenay [44]:

Definition 1 *The* nonlinearity $\mathcal{NL}(F)$ *of an* (n, m)*-function* F *is the minimum nonlinearity of all the component functions* $x \in \mathbb{F}_2^n \mapsto v \cdot F(x)$, $v \in \mathbb{F}_2^m$, $v \neq 0$.

In other words, $\mathcal{NL}(F)$ equals the minimum Hamming distance between all the component functions of F and all affine functions on n variables. This generalization is closely related to the linear attack (see introduction).
The nonlinearity of S-boxes is clearly a right and left affine invariant and the nonlinearity of an S-box F does not change if we add to F an affine function. Moreover, if A is a surjective linear (or affine) function from $\mathbb{F}_2^p$ (where p is some positive integer) into $\mathbb{F}_2^n$, then it is easily shown that $\mathcal{NL}(F \circ A) = 2^{p-n}\mathcal{NL}(F)$.
According to the equality relating the nonlinearity of a Boolean function to the maximum magnitude of its Walsh transform, we have:

$$\mathcal{NL}(F) = 2^{n-1} - \frac{1}{2} \max_{v \in \mathbb{F}_2^{m*};\ u \in \mathbb{F}_2^n} \left| \sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot F(x) \oplus u \cdot x} \right|. \tag{5}$$

Note that "$\max_{v \in \mathbb{F}_2^{m*};\ u \in \mathbb{F}_2^n}$" can be replaced by "$\max_{(u,v) \in \mathbb{F}_2^n \times \mathbb{F}_2^m; (u,v) \neq (0,0)}$". Hence, if $n = m$ and if F is a permutation, then F and its inverse F^{-1} have the same nonlinearity (change the variable x into $F^{-1}(x)$).

We shall call *Walsh spectrum* of F the multi-set of all the values $\sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot F(x) \oplus u \cdot x}$ of the Walsh transform of F, where $u \in \mathbb{F}_2^n, v \in \mathbb{F}_2^{m*}$, *extended Walsh spectrum* of F the multi-set of their absolute values, and *Walsh support* of F the

set of those (u, v) such that $\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x} \neq 0$.

Remark. We have

$$\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x} = \sum_{b\in\mathbb{F}_2^m}\widehat{\varphi_b}(u)(-1)^{v\cdot b} \tag{6}$$

where $\widehat{\varphi_b}$ is the discrete Fourier transform of the Boolean function φ_b.
Also, if we denote by G_F the graph $\{(x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2^m / y = F(x)\}$ of F, and by 1_{G_F} its indicator, then we have $\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x} = \widehat{1_{G_F}}(u, v)$. Note that, if we write the values of the function $\widehat{1_{G_F}}$ in a $2^m \times 2^n$ matrix (in which the term located at the line indexed by $v \in \mathbb{F}_2^m$ and at the column indexed by $u \in \mathbb{F}_2^n$ equals $\widehat{1_{G_F}}(u, v)$), then, the matrix corresponding to the composition $F \circ H$ of F with an (r, n)-function H, equals the product (in the same order) of the matrices associated to F and H, divided by 2^n. Indeed, for every $w \in \mathbb{F}_2^r$ and every $v \in \mathbb{F}_2^m$, we have

$$\begin{aligned}
\sum_{u\in\mathbb{F}_2^n}\widehat{1_{G_F}}(u, v)\widehat{1_{G_H}}(w, u) &= \sum_{u\in\mathbb{F}_2^n; x\in\mathbb{F}_2^r; y\in\mathbb{F}_2^n}(-1)^{v\cdot F(y)\oplus u\cdot y\oplus u\cdot H(x)\oplus w\cdot x} \\
&= 2^n \sum_{x\in\mathbb{F}_2^r; y\in\mathbb{F}_2^n \,/\, y=H(x)}(-1)^{v\cdot F(y)\oplus w\cdot x} \\
&= 2^n\widehat{1_{G_{F\circ H}}}(w, v),
\end{aligned}$$

since $\sum_{u\in\mathbb{F}_2^n}(-1)^{u\cdot y\oplus u\cdot H(x)}$ equals 2^n if $y = H(x)$, and is null otherwise. $\diamond$

Relation with linear codes As observed in [36, 107], there is a relationship between the maximum possible nonlinearity of (n, m)-functions and the possible parameters of the supercodes of the Reed-Muller code of order 1. Let C be a linear $[2^n, K, D]$ binary code including the Reed-Muller code $RM(1, n)$ as a subcode. Let $(b_1, \ldots, b_K)$ be a basis of C completing a basis $(b_1, \ldots, b_{n+1})$ of $RM(1, n)$. The n-variable Boolean functions corresponding to the vectors $b_{n+2}, \ldots, b_K$ are the coordinate functions of an $(n, K - n - 1)$-function whose nonlinearity is D. Conversely, if $D > 0$ is the nonlinearity of some (n, m)-function, then the linear code equal to the union of the cosets $v \cdot F + RM(1, n)$, where v ranges over F_2^m, has parameters $[2^n, n + m + 1, D]$. Existence and non-existence[2] results on highly nonlinear vectorial functions are deduced in [107] and upper bounds on the nonlinearity of (n, m)-functions are derived in [38].

[2]Using the linear programming bound due to Delsarte.

2.1.1 The upper bounds on $\mathcal{NL}(F)$ and the functions achieving them

Covering radius bound: the covering radius bound $\mathcal{NL}(f) \leq 2^{n-1} - 2^{n/2-1}$, valid for every n-variable Boolean function, is *a fortiori* valid for every (n,m)-function:

$$\mathcal{NL}(F) \leq 2^{n-1} - 2^{n/2-1}. \tag{7}$$

Definition 2 *An (n,m) function is called* bent *if it achieves the covering radius bound* (7) *with equality.*

Clearly, an (n,m)-function is bent if and only if all of the component functions $v \cdot F$, $v \neq 0$ of F are bent (*i.e.* achieve the same bound). Hence, the algebraic degree of any bent (n,m)-function is at most $n/2$. Note also that, since any n-variable Boolean function f is bent if and only if all of its derivatives $D_a f(x) = f(x) \oplus f(x+a)$, $a \neq 0$, are balanced, an (n,m)-function F is bent if and only if, for every $v \in \mathbb{F}_2^m$, $v \neq 0$, and every $a \in \mathbb{F}_2^n$, $a \neq 0$, the function $v \cdot (F(x) + F(x+a))$ is balanced. According to Proposition 1, this is equivalent to saying that, for every $a \in \mathbb{F}_2^n$, $a \neq 0$, the function $F(x) + F(x+a)$ is balanced.

Proposition 2 *An (n,m)-function is bent if and only if all of its* derivatives *$D_a F(x) = F(x) + F(x+a)$, $a \in \mathbb{F}_2^{n*}$, are balanced.*

For this reason, bent functions are also called *perfect nonlinear*[3]; they contribute then to an optimum resistance to the differential attack (see introduction) of those cryptosystems in which they are involved (but they are not balanced). They can be used to design *authentication schemes* (or codes); see [45].
Thanks to the observations made at Subsection 1.1 (where we saw that the evaluation of the multidimensional Walsh transform corresponds in fact to the evaluation of the Walsh transform), it is a simple matter to characterize the bent functions as those functions whose squared expression of the multidimensional Walsh transform at L is the same for every L.

Existence of bent (n,m)-functions: since bent n-variable Boolean functions exist only if n is even, bent (n,m)-functions exist only under this same condition. But, as shown by Nyberg in [92], this is not sufficient for the existence of bent (n,m)-functions. Indeed, we have seen in Relation (4)

[3]We shall see that perfect nonlinear (n,n)-functions do not exist; but they do exist in other characteristics than 2 (see *e.g.* [37]); they are then often called *planar*.

that, for any element $b \in \mathbb{F}_2^m$, the size of $F^{-1}(b)$ (that is, the Hamming weight of φ_b) is equal to $2^{-m}\sum_{x\in\mathbb{F}_2^n;v\in\mathbb{F}_2^m}(-1)^{v\cdot(F(x)+b)}$. Denoting, for every $v \in \mathbb{F}_2^{n*}$, by $\widetilde{v\cdot F}$ the dual of the Boolean function $x \mapsto v \cdot F(x)$, we have $\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)} = 2^{n/2}(-1)^{\widetilde{v\cdot F}(0)}$. The size of $F^{-1}(b)$ equals then $2^{n-m} + 2^{n/2-m}\sum_{v\in\mathbb{F}_2^{n*}}(-1)^{\widetilde{v\cdot F}(0)\oplus v\cdot b}$. Since the sum $\sum_{v\in\mathbb{F}_2^{n*}}(-1)^{\widetilde{v\cdot F}(0)\oplus v\cdot b}$ has an odd value ($\mathbb{F}_2^{n*}$ having an odd size), we deduce that, if $m \leq n$ then $2^{n/2-m}$ must be an integer. And it is also easily shown that $m > n$ is impossible. Hence:

Proposition 3 *Bent (n, m)-functions exist only if n is even and $m \leq n/2$.*

It is a simple matter to show that, for every ordered pair (n, m) satisfying this condition, bent functions do exist. The two main classes of bent Boolean functions described in the chapter "Boolean Functions for Cryptography and Error Correcting Codes" (see Subsection 6.4.1) lead to two classes of bent (n, m)-functions (this was first observed by Nyberg in [92]). We endow $\mathbb{F}_2^{n/2}$ with the structure of the field $\mathbb{F}_{2^{n/2}}$. We identify $\mathbb{F}_2^n$ with $\mathbb{F}_{2^{n/2}} \times \mathbb{F}_{2^{n/2}}$.

- Let us define $F(x, y) = L(x\,\pi(y)) + H(y)$, where the product $x\,\pi(y)$ is calculated in $\mathbb{F}_{2^{n/2}}$, where L is any linear or affine mapping from $\mathbb{F}_{2^{n/2}}$ onto $\mathbb{F}_2^m$, π is any permutation of $\mathbb{F}_{2^{n/2}}$ and H is any $(n/2, m)$-function. This gives a so-called *Maiorana-McFarland's bent* (n, m)-function. More generally, we obtain bent functions by taking for F any (n, m)-function such that, for every $v \in \mathbb{F}_2^{m*}$, the Boolean function $v \cdot F$ belongs, up to linear equivalence, to Maiorana-McFarland's class of bent functions. The function $L(x\,\pi(y)) + H(y)$ has this property, since the function $v \cdot L(z)$ is a nonzero linear function, and then equals $tr(\lambda z)$ for some $\lambda \neq 0$, where tr is the (absolute) trace function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$.
Modifications of these Maiorana-McFarland's bent functions have been proposed in [95], using the classes $\mathcal{C}$ and $\mathcal{D}$ of bent Boolean functions recalled in the chapter "Boolean Functions for Cryptography and Error Correcting Codes".
- Defining $F(x, y) = G(\frac{x}{y})$ (with $\frac{x}{y} = 0$ if $y = 0$), where G is a balanced $(n/2, m)$-function, gives also a bent (n, m)-function: for every $v \neq 0$, the function $v\cdot F$ belongs to the class $\mathcal{PS}_{ap}$ of Dillon's functions (seen in the chapter "Boolean Functions for Cryptography and Error Correcting Codes"), according to Proposition 1.
Note that, given any bent (n, m)-function F, any chopped (n, m')-function (with $m' < m$) obtained by deleting some coordinates of F (or more gener-

ally by composing it on the left with any surjective affine mapping) is still bent. But there exist other secondary constructions (that is, constructions of new bent functions from known ones). In [34] is given the following secondary construction of bent Boolean functions: let $r \leq s$ be two positive integers with the same parity and let $n = r + s$; let ϕ be a mapping from $\mathbb{F}_2^s$ to $\mathbb{F}_2^r$ and g a Boolean function on $\mathbb{F}_2^s$; let us assume that, for every $a \in \mathbb{F}_2^r$, the set $\phi^{-1}(a)$ is an $(n-2r)$-dimensional affine subspace of $\mathbb{F}_2^s$ and that, if $r < s$, the restriction of g to $\phi^{-1}(a)$ (viewed as a Boolean function on $\mathbb{F}_2^{n-2r}$ via an affine isomorphism between $\phi^{-1}(a)$ and this vectorspace) is bent; then the function $f_{\phi,g}(x,y) = x \cdot \phi(y) \oplus g(y)$, $x \in \mathbb{F}_2^r$, $y \in \mathbb{F}_2^s$, where "$\cdot$" is an inner product in $\mathbb{F}_2^r$, is bent on $\mathbb{F}_2^n$. This gives:

Proposition 4 *Let r and s be two positive integers with the same parity and let $r \leq \frac{s}{3}$. Let ψ be any mapping from $\mathbb{F}_2^s$ to $\mathbb{F}_{2^r}$ such that, for every $a \in \mathbb{F}_{2^r}$, the set $\psi^{-1}(a)$ is an $(s-r)$-dimensional affine subspace of $\mathbb{F}_2^s$. Let H be any (s,r)-function whose restriction to $\psi^{-1}(a)$ (viewed as an $(s-r,r)$-function via an affine isomorphism between $\psi^{-1}(a)$ and $\mathbb{F}_2^{s-r}$) is bent for every $a \in \mathbb{F}_{2^r}$. Then the function $F_{\psi,H}(x,y) = x\,\psi(y) + H(y)$, $x \in F_{2^r}, y \in F_2^s$, is a bent function from $\mathbb{F}_2^{r+s}$ to F_{2^r}.*

Indeed, for every $v \in F_{2^r}^*$, the function $tr(v\,F_{\psi,H}(x,y))$ (where tr is the trace function from $\mathbb{F}_{2^r}$ to $\mathbb{F}_2$) is bent, according to the result of [34] with $\phi(y) = v\,\psi(y)$ and $g(y) = tr(v\,H(y))$. The condition $r \leq \frac{s}{3}$, more restrictive than $r \leq s$, is meant so that $r \leq \frac{s-r}{2}$, which is necessary for allowing the restrictions of H to be bent. The condition on ψ being easily satisfied[4], it is then a simple matter to choose H. Hence, this construction is quite effective (but only for designing more bent (n,m)-functions when $m \leq n/4$).

In [33] is also given a very general secondary construction of bent Boolean functions which can be adapted to vectorial functions as follows:

Proposition 5 *Let r and s be two positive even integers and m a positive integer such that $m \leq r/2$. Let H be a function from $\mathbb{F}_2^n = \mathbb{F}_2^r \times \mathbb{F}_2^s$ to $\mathbb{F}_2^m$. Assume that, for every $y \in \mathbb{F}_2^s$, the function $H_y : x \in \mathbb{F}_2^r \to H(x,y)$ is a bent (r,m)-function. For every nonzero $v \in \mathbb{F}_2^m$ and every $a \in \mathbb{F}_2^r$ and $y \in \mathbb{F}_2^s$, let us denote by $f_{a,v}(y)$ the value at a of the dual of the Boolean function $v \cdot H_y$, that is, the binary value such that $\sum_{x \in \mathbb{F}_2^r} (-1)^{v \cdot H(x,y) \oplus a \cdot x} = 2^{r/2}(-1)^{f_{a,v}(y)}$. Then H is bent if and only if, for every nonzero $v \in \mathbb{F}_2^m$ and every $a \in \mathbb{F}_2^r$, the Boolean function $f_{a,v}$ is bent.*

[4]Note that it does not make ψ necessarily affine.

Indeed, by definition of $f_{a,v}$, we have, for every nonzero $v \in \mathbb{F}_2^m$ and every $a \in \mathbb{F}_2^r$ and $b \in \mathbb{F}_2^s$:

$$\sum_{\substack{x\in\mathbb{F}_2^r\\ y\in\mathbb{F}_2^s}} (-1)^{v\cdot H(x,y)\oplus a\cdot x\oplus b\cdot y} = 2^{r/2} \sum_{y\in\mathbb{F}_2^s} (-1)^{f_{a,v}(y)\oplus b\cdot y}.$$

An obvious example of application of Proposition 5 is the so-called direct sum of bent functions: $H(x,y) = F(x) + G(y)$, where F is a bent (r,m)-function and G a bent (s,m)-function.
Another example is by choosing every H_y in the Maiorana-McFarland's class: $H_y(x,x') = x\,\pi_y(x') + G_y(x')$, $x, x' \in \mathbb{F}_{2^{r/2}}$, where π_y is bijective for every $y \in \mathbb{F}_2^s$. For every $v \in \mathbb{F}^*_{2^{r/2}}$ and every $a, a' \in \mathbb{F}_{2^{r/2}}$, we have then $f_{(a,a'),v}(y) = tr\left(a'\,\pi_y^{-1}\left(\frac{a}{v}\right) + v\,G_y\left(\pi_y^{-1}\left(\frac{a}{v}\right)\right)\right)$, where tr is the trace function from $\mathbb{F}_{2^{r/2}}$ to $\mathbb{F}_2$. Then H is bent if and only if, for every $v \in \mathbb{F}^*_{2^{r/2}}$ and every $a, a' \in \mathbb{F}_{2^{r/2}}$, the function $y \to tr\left(a'\,\pi_y^{-1}(a) + v\,G_y(\pi_y^{-1}(a))\right)$ is bent on $\mathbb{F}_2^s$. A simple possibility for achieving this is to choose $s = r/2$ and π_y^{-1} and G_y such that, for every a, the mapping $y \to \pi_y^{-1}(a)$ is an affine automorphism of $\mathbb{F}_{2^{r/2}}$ (*e.g.* $\pi_y^{-1}(a) = \pi_y(a) = a + y$) and, for every a, the function $y \to G_y(a)$ is bent.

Sidelnikov-Chabaud-Vaudenay bound: Since bent (n,m)-functions do not exist if $m > n/2$, there is a chance that upper bounds better than the covering radius bound exist in this case. Such a bound has been re-discovered by Chabaud and Vaudenay in [44]. We say "re-discovered" because a bound on sequences due to Sidelnikov [102] is equivalent to the bound obtained by Chabaud and Vaudenay for power functions and its proof is in fact valid for all functions. Note that other bounds have been obtained in [38] and improve, when m is sufficiently greater than n (which makes them less interesting, cryptographically), upon the covering radius bound and the Sidelnikov-Chabaud-Vaudenay bound (examples are given). A more precise insight on the Sidelnikov-Chabaud-Vaudenay bound is also given in this same paper.

Theorem 1 *Let n and m be any positive integers; $m \geq n-1$. Let F be any (n,m)-function. Then:*

$$\mathcal{NL}(F) \leq 2^{n-1} - \frac{1}{2}\sqrt{3\times 2^n - 2 - 2\frac{(2^n-1)(2^{n-1}-1)}{2^m-1}}.$$

Proof. Recall that $\mathcal{NL}(F) = 2^{n-1} - \frac{1}{2}\ \max_{v\in\mathbb{F}_2^{m*};\ u\in\mathbb{F}_2^n} \left|\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x}\right|$. We have:

$$\max_{\substack{v\in\mathbb{F}_2^{m*}\\ u\in\mathbb{F}_2^n}} \left(\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x}\right)^2 \geq \frac{\sum_{\substack{v\in\mathbb{F}_2^{m*}\\ u\in\mathbb{F}_2^n}} \left(\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x}\right)^4}{\sum_{\substack{v\in\mathbb{F}_2^{m*}\\ u\in\mathbb{F}_2^n}} \left(\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x}\right)^2}. \quad (8)$$

Parseval's relation states that, for every $v \in \mathbb{F}_2^m$:

$$\sum_{u\in\mathbb{F}_2^n} \left(\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x}\right)^2 = 2^{2n}.$$

Using the fact that any character sum $\sum_{x\in E}(-1)^{\ell(x)}$ associated to a linear function ℓ over any $\mathbb{F}_2$-vectorspace E is nonzero if and only if ℓ is null on E, we can state that:

$$\sum_{v\in\mathbb{F}_2^m,\ u\in\mathbb{F}_2^n} \left(\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x}\right)^4$$

$$= \sum_{x,y,z,t\in\mathbb{F}_2^n} \left[\sum_{v\in\mathbb{F}_2^m}(-1)^{v\cdot(F(x)+F(y)+F(z)+F(t))}\right]\left[\sum_{u\in\mathbb{F}_2^n}(-1)^{u\cdot(x+y+z+t)}\right]$$

$$= 2^{n+m}\left|\left\{(x,y,z,t)\in\mathbb{F}_2^{4n}/\ \begin{cases} x+y+z+t & =0\\ F(x)+F(y)+F(z)+F(t) & =0\end{cases}\right\}\right|$$

$$= 2^{n+m}|\{(x,y,z)\in\mathbb{F}_2^{3n}/\ F(x)+F(y)+F(z)+F(x+y+z)=0\}| \quad (9)$$

$$\geq 2^{n+m}|\{(x,y,z)\in\mathbb{F}_2^{3n}/\ x=y \text{ or } x=z \text{ or } y=z\}|. \quad (10)$$

We have $|\{(x,y,z)/\ x=y \text{ or } x=z \text{ or } y=z\}| = 3\cdot|\{(x,x,y)/\ x,y\in\mathbb{F}_2^n\}| - 2\cdot|\{(x,x,x)/\ x\in\mathbb{F}_2^n\}| = 3\cdot 2^{2n} - 2\cdot 2^n$. Hence:

$$\max_{v\in\mathbb{F}_2^{m*};\ u\in\mathbb{F}_2^n} \left(\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x}\right)^2 \geq$$

$$\frac{2^{n+m}(3\cdot 2^{2n} - 2\cdot 2^n) - 2^{4n}}{(2^m-1)\,2^{2n}} = 3\times 2^n - 2 - 2\frac{(2^n-1)(2^{n-1}-1)}{2^m-1}$$

and this gives the desired bound. ◇

It is a simple matter to show that this *Sidelnikov-Chabaud-Vaudenay bound* improves upon the covering radius bound (7) only for $m \geq n$ (and the question of improving upon the covering radius bound for $n/2 < m < n$, when n is even and for $m < n$, when n is odd, is open). It is also clear that, when $m \geq n$, it can be achieved only if $n = m$ with n odd.

2.1.2 Almost perfect nonlinear and almost bent functions

Definition 3 *The (n, n)-functions F which achieve the bound of Theorem 1 with equality – that is, such that $\mathcal{NL}(F) = 2^{n-1} - 2^{\frac{n-1}{2}}$ – are called* almost bent *(AB).*

Remark. The term of *almost* bent is a little misleading. It gives the feeling that these functions are not quite optimal while they are; according to Nyberg's result (Proposition 3), (n, n)-bent functions do not exist.

According to Inequality (8), the AB functions are those (n, n)-functions such that, for every $u, v \in \mathbb{F}_2^n$, $v \neq 0$, the sum $\sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot F(x) \oplus u \cdot x}$ (that is, the Walsh transform of the function $v \cdot F$) equals 0 or $\pm 2^{\frac{n+1}{2}}$ (indeed, the maximum of a sequence of non-negative integers equals the ratio of the sum of their squares over the sum of their values if and only if these integers have at most one nonzero value). Note that this condition does not depend on the choice of the inner product.
There exists a bound on the algebraic degree of AB functions, similar to the bound for bent functions:

Proposition 6 *[36] Let F be any (n, n)-function. If F is AB, then the algebraic degree of F is less than or equal to $(n + 1)/2$.*

This is a direct consequence of the fact that the Walsh transform of any function $v \cdot F$ is divisible by $2^{\frac{n+1}{2}}$, and of Proposition 9 of the chapter "Boolean Functions for Cryptography and Error Correcting Codes" (bounding the algebraic degree of a Boolean function, given the divisibility of its Walsh transform values). Note that the divisibility plays also a role with respect to the algebraic degree of the composition of two vectorial functions. In [32] has been proved that, if the Walsh transform values of a vectorial function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ are divisible by 2^ℓ then, for every vectorial function $F' : \mathbb{F}_2^n \to \mathbb{F}_2^n$, the algebraic degree of $F' \circ F$ is at most equal to the algebraic degree of F' plus $n - \ell$. This means that using AB power functions as S-boxes in block ciphers may not be a good idea. Suboptimal functions (as the inverse function, see below) may be better, as usual in cryptography

(since optimal functions have much structure, which can be used in attacks).

Inequality (10) is an equality if and only if the relation $F(x)+F(y)+F(z)+F(x+y+z)=0$ can be achieved only when $x=y$ or $x=z$ or $y=z$. There are two equivalent ways of characterizing this property:
- the restriction of F to any 2-dimensional flat (*i.e.* affine subspace) of $\mathbb{F}_2^n$ is non-affine (indeed, the set $\{x,y,z,x+y+z\}$ is a flat and it is 2-dimensional if and only if $x\neq y$ and $x\neq z$ and $y\neq z$; saying that $F(x)+F(y)+F(z)+F(x+y+z)=0$ is equivalent to saying that the restriction of F to this flat is affine);
- the equation $F(x)+F(x+a)=F(y)+F(y+a)$ can be achieved only for $a=0$ or $x=y$ or $x=y+a$ (denote $x+z$ by a).
Hence, Inequality (10) implies that all AB functions are such that, for every $a\in\mathbb{F}_2^{n*}$ and every $b\in\mathbb{F}_2^n$, the equation $F(x)+F(x+a)=b$ has at most 2 solutions (that is, 0 or 2 solutions, since if it has one solution x, then it has $x+a$ for second solution).

Definition 4 *An (n,n)-function F is called* almost perfect nonlinear *(APN) if, for every $a\in\mathbb{F}_2^{n*}$ and every $b\in\mathbb{F}_2^n$, the equation $F(x)+F(x+a)=b$ has 0 or 2 solutions; that is, equivalently, if the restriction of F to any 2-dimensional flat (*i.e. *affine subspace) of $\mathbb{F}_2^n$ is non-affine.*

Remark. Here again, the term of *almost* perfect nonlinear is a little misleading, giving the feeling that these functions are not quite optimal while they are.

The notion of plateaued function will play a role in the sequel.

Definition 5 *An (n,m)-function is called* plateaued *if, for every nonzero $v\in\mathbb{F}_2^m$, the function $v\cdot F$ is plateaued, that is, there exists a positive integer λ_v (called the amplitude of $v\cdot F$) such that the values of its Walsh transform: $\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x}$, $u\in\mathbb{F}_2^n$, all belong to the set $\{0,\pm\lambda_v\}$.*

Then, because of Parseval's relation, 2^{2n} equals λ_v^2 times the size of the set $\{u\in\mathbb{F}_2^n\ /\ \sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x}\neq 0\}$, and λ_v equals then a power of 2 whose exponent is greater than or equal to $n/2$ (since this size is at most 2^n). The extreme case $\lambda_v=2^{n/2}$ corresponds to the case where $v\cdot F$ is bent. Every *quadratic* function (that is, every function of algebraic degree 2) is plateaued, see the chapter "Boolean Functions for Cryptography and Error Correcting Codes".

Proposition 7 *Every AB function is APN. More precisely, any vectorial function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is AB if and only if F is APN and the functions $v \cdot F$, $v \neq 0$, are plateaued with the same amplitude.*

This comes directly from Relations (8) and (10). *We shall see below, thanks to Proposition 12, that the condition "with the same amplitude" is in fact not necessary in this proposition (for n odd).* According to Definition 4, F is APN if, for every distinct nonzero vectors a and a', its second derivative $D_a D_{a'} F(x) = F(x)+F(x+a)+F(x+a')+F(x+a+a')$ takes only non-zero values.
Note that, according to Relations (9) and (10), and to the two lines following them, F is APN if and only if

$$\sum_{v \in \mathbb{F}_2^n, u \in \mathbb{F}_2^n} \left(\sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot F(x) \oplus u \cdot x} \right)^4 = 3 \cdot 2^{4n} - 2 \cdot 2^{3n} \tag{11}$$

or equivalently (using Parseval's relation):

$$\sum_{\substack{v \in \mathbb{F}_2^n * \\ u \in \mathbb{F}_2^n}} \left(\sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot F(x) \oplus u \cdot x} \right)^2 \left(\left(\sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot F(x) \oplus u \cdot x} \right)^2 - 2^{n+1} \right) = 0. \tag{12}$$

APN property is a particular case of a notion introduced by Nyberg [92, 93]: an (n, m)-function F is called *differentially δ-uniform* if, for every nonzero $a \in \mathbb{F}_2^n$ and every $b \in \mathbb{F}_2^m$, the equation $F(x) + F(x + a) = b$ has at most δ solutions. The number δ is then lower bounded by 2^{n-m} and equals 2^{n-m} if and only if F is perfect nonlinear.
The smaller δ is, the better is the contribution of F to a resistance to differential cryptanalysis. When $m = n$, the smallest possible value of δ is 2, since we already saw that if x is a solution of equation $F(x) + F(x + a) = b$ then $x + a$ is also a solution. Hence, APN functions contribute to a maximum resistance to differential cryptanalysis when $m = n$ and AB functions contribute to a maximum resistance to both linear and differential cryptanalyses.

Note that if F is a quadratic (n, n)-function, the equation $F(x) + F(x + a) = b$ is a linear equation. It admits then at most 2 solutions for every nonzero a and every b if and only if the related homogeneous equation $F(x) + F(x + a) + F(0) + F(a) = 0$ admits at most 2 solutions for every nonzero a. Hence, F is APN if and only if the associated bilinear symmetric

$(2n,n)$-function $\varphi_F(x,y) = F(0)+F(x)+F(y)+F(x+y)$ never vanishes when x and y are $\mathbb{F}_2$-linearly independent vectors of $\mathbb{F}_2^n$. For functions of higher degrees, the fact that $\varphi_F(x,y)$ (which is no longer bilinear) never vanishes when x and y are linearly independent is only a necessary condition for APNness.

A subclass of APN functions (and a superclass of APN quadratic permutations), called crooked functions, has been considered in [3] and further studied in [20, 84]. All known crooked functions are quadratic. Every power crooked function is a Gold function (see definition below).

Other characterizations of AB and APN functions

• The properties of APNness and ABness can be translated in terms of Boolean functions, as observed in [36]:

Proposition 8 *Let F be any (n,n)-function. For every $a,b \in \mathbb{F}_2^n$, let $\gamma_F(a,b)$ equal 1 if the equation $F(x)+F(x+a)=b$ admits solutions, with $a \neq 0$. Otherwise, let $\gamma_F(a,b)$ be null. Then, F is APN if and only if γ_F has weight $2^{2n-1}-2^{n-1}$, and is AB if and only if γ_F is bent. Its dual is then the indicator of the Walsh support of F, deprived of $(0,0)$.*

Proof.
1) If F is APN, then for every $a \neq 0$, the mapping $x \mapsto F(x)+F(x+a)$ is two-to-one (that is, the size of the pre-image of any vector equals 0 or 2). Hence, γ_F has weight $2^{2n-1}-2^{n-1}$. The converse is also straightforward.
2) We assume now that F is APN. For every $u,v \in \mathbb{F}_2^n$, replacing $(-1)^{\gamma_F(a,b)}$ by $1-2\gamma_F(a,b)$ in the character sum $\sum_{a,b\in\mathbb{F}_2^n}(-1)^{\gamma_F(a,b)\oplus u\cdot a\oplus v\cdot b}$ leads to $\sum_{a,b\in\mathbb{F}_2^n}(-1)^{u\cdot a\oplus v\cdot b} - 2\sum_{a,b\in\mathbb{F}_2^n}\gamma_F(a,b)(-1)^{u\cdot a\oplus v\cdot b}$. Denoting by δ_0 the Dirac symbol ($\delta_0(u,v)=1$ if $u=v=0$ and 0 otherwise), we deduce that the Walsh transform of γ_F equals $2^{2n}\ \delta_0(u,v) - \sum_{x\in\mathbb{F}_2^n, a\in\mathbb{F}_2^{n*}}(-1)^{u\cdot a\oplus v\cdot(F(x)+F(x+a))} = 2^{2n}\ \delta_0(u,v) - \left(\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x}\right)^2 + 2^n$. Hence, F is AB if and only if the value of this Walsh transform equals $\pm 2^n$ at every $(u,v)\in\mathbb{F}_2^n\times\mathbb{F}_2^n$, *i.e.* if γ_F is bent. Moreover, if γ_F is bent, then for every $(u,v)\neq 0$, we have $\widetilde{\gamma_F}(u,v)=0$, that is, $\sum_{a,b\in\mathbb{F}_2^n}(-1)^{\gamma_F(a,b)\oplus u\cdot a\oplus v\cdot b} = 2^n$ if and only if $\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x} = 0$. Hence, the dual of γ_F is the indicator of the Walsh support of F, deprived of $(0,0)$. ◇

• Obviously, an (n,n)-function F is APN if and only if, for every $(a,b) \neq (0,0)$, the system $\left\{ \begin{array}{rcl} x+y & = & a \\ F(x)+F(y) & = & b \end{array} \right.$ admits 0 or 2 solutions. As shown in [50], it is AB if and only if the system $\left\{ \begin{array}{rcl} x+y+z & = & a \\ F(x)+F(y)+F(z) & = & b \end{array} \right.$ admits $3 \cdot 2^n - 2$ solutions if $b = F(a)$ and $2^n - 2$ solutions otherwise. This can easily be proved by using the facts that F is AB if and only if, for every $v \in \mathbb{F}_2^{n*}$ and every $u \in \mathbb{F}_2^n$, we have $\left(\sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot F(x) \oplus u \cdot x}\right)^3 = 2^{n+1} \sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot F(x) \oplus u \cdot x}$, and that two pseudo-Boolean functions (that is, two functions from $\mathbb{F}_2^n$ to $\mathbb{Z}$) are equal to each other if and only if their discrete Fourier transforms are equal to each other: the value at (a,b) of the Fourier transform of the function equal to $\left(\sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot F(x) \oplus u \cdot x}\right)^3$ if $v \neq 0$, and to 0 otherwise equals

$$\sum_{\substack{u \in \mathbb{F}_2^n \\ v \in \mathbb{F}_2^n}} \left(\sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot F(x) \oplus u \cdot x} \right)^3 (-1)^{a \cdot u \oplus b \cdot v} - 2^{3n} =$$

$$2^{2n} \left| \left\{ (x,y,z) \in \mathbb{F}_2^{3n} \,/\, \left\{ \begin{array}{l} x+y+z = a \\ F(x)+F(y)+F(z) = b \end{array} \right. \right\} \right| - 2^{3n},$$

and the value of the Fourier transform of the function which is equal to $2^{n+1} \sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot F(x) \oplus u \cdot x}$ if $v \neq 0$, and to 0 otherwise equals

$$2^{3n+1} \left| \left\{ x \in \mathbb{F}_2^n \,/\, \left\{ \begin{array}{l} x = a \\ F(x) = b \end{array} \right. \right\} \right| - 2^{2n+1}.$$

This proves the result. Note that $3 \cdot 2^n - 2$ is the number of triples (x,x,a), (x,a,x) and (a,x,x) where x ranges over $\mathbb{F}_2^n$. Hence the condition when $F(a) = b$ means that these particular triples are the only solutions of the system $\left\{ \begin{array}{rcl} x+y+z & = & a \\ F(x)+F(y)+F(z) & = & F(a) \end{array} \right.$. This is equivalent to saying that F is APN. And, by denoting $c = F(a) + b$, we have:

Proposition 9 *Let n be any positive integer and F any APN (n,n)-function. Then F is AB if and only if, for every $c \neq 0$ and every a in $\mathbb{F}_2^n$, the equation $F(x)+F(y)+F(a)+F(x+y+a) = c$ has $2^n - 2$ solutions.*

Note that, assuming that F is APN, this condition is also equivalent to saying that the weight of the function $z \to \gamma_F(a+z, b+F(z))$ equals $2^{n-1}-1$, for every (a,b) such that $F(a) \neq b$.

Summarizing, let $\mathcal{A}_2$ be the set of 2-dimensional flats of $\mathbb{F}_2^n$ and $\Phi_F : A \in \mathcal{A}_2 \to \sum_{x\in A} F(x) \in \mathbb{F}_2^n$. Then F is APN if and only if Φ_F is valued in $\mathbb{F}_2^n \setminus \{0\}$ and F is AB if and only if Φ_F has additionally the property that, for every $a \in \mathbb{F}_2^n$, the restriction of Φ_F to those flats which contain a is balanced from this set to $\mathbb{F}_2^n \setminus \{0\}$, that is, is a $\frac{2^{n-1}-1}{3}$-to-1 function. Note that, for every APN function F and any two distinct vectors a and a', the restriction of Φ_F to those flats which contain a and a' is injective, since for two such distinct flats $A = \{a, a', x, x + a + a'\}$ and $A' = \{a, a', x', x' + a + a'\}$, we have $\Phi_F(A) + \Phi_F(A') = F(x) + F(x + a + a') + F(x') + F(x' + a + a') = \Phi_F(\{x, x + a + a', x', x' + a + a'\}) \neq 0$. But Φ_F cannot be balanced since the number of flats containing a and a' equals $2^{n-1}-1$, that is less than 2^n-1.

Remark: Other characterizations can be derived with the same method. For instance, F is AB if and only if, for every $v \in \mathbb{F}_2^{n*}$ and every $u \in \mathbb{F}_2^n$, we have $\left(\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x}\right)^4 = 2^{n+1}\left(\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x}\right)^2$. By applying again the Fourier transform and dividing by 2^{2n}, we deduce that F is AB if and only if, for every (a, b), we have

$$\left|\left\{(x, y, z, t) \in \mathbb{F}_2^{4n} / \left\{ \begin{array}{l} x + y + z + t = a \\ F(x) + F(y) + F(z) + F(t) = b \end{array} \right\}\right| - 2^{2n} =$$

$$2^{n+1}\left|\left\{(x, y) \in \mathbb{F}_2^{2n} / \left\{ \begin{array}{l} x + y = a \\ F(x) + F(y) = b \end{array} \right\}\right| - 2^{n+1}.$$

Hence, F is AB if and only if the system $\left\{ \begin{array}{lcl} x + y + z + t & = & a \\ F(x) + F(y) + F(z) + F(t) & = & b \end{array} \right.$ admits $3 \cdot 2^{2n} - 2^{n+1}$ solutions if $a = b = 0$ (this is equivalent to saying that F is APN), $2^{2n} - 2^{n+1}$ solutions if $a = 0$ and $b \neq 0$ (note that this condition corresponds to adding all the conditions of Proposition 9 with c fixed to b and with a ranging over $\mathbb{F}_2^n$), and $2^{2n} + 2^{n+2}\gamma_F(a, b) - 2^{n+1}$ solutions if $a \neq 0$ (indeed, F is APN; note that this gives a new necessary condition).

• It is a simple matter to show (see [36]) a relationship between the properties for an (n, n)-function of being APN or AB, and properties of related codes.

Proposition 10 *Let F be any (n, n)-function such that $F(0) = 0$. Let H be the matrix $\begin{bmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{2^n-2} \\ F(1) & F(\alpha) & F(\alpha^2) & \dots & F(\alpha^{2^n-2}) \end{bmatrix}$, where α is a primitive element of the field $\mathbb{F}_{2^n}$, and where each symbol stands for the column of its coordinates with respect to a basis of the $\mathbb{F}_2$-vectorspace $\mathbb{F}_{2^n}$. Let C_F be the*

*linear code admitting H for parity-check matrix. Then, F is APN if and only if C_F has minimum distance 5, and F is AB if and only if $C_F^\perp$ (*i.e.* the code admitting H for generator matrix) has weights $0, 2^{n-1} - 2^{\frac{n-1}{2}}, 2^{n-1}$ and $2^{n-1} + 2^{\frac{n-1}{2}}$ (the weight distribution being then imposed by Parseval's relation and equal to that of the dual of the 2-error-correcting BCH code of length $2^n - 1$).*

Indeed, C_F being a subcode of the Hamming code, it has minimum distance at least 3, and the fact that it has no codeword of weight 3 or 4 is by definition equivalent to the APNness of F. The characterization of ABness through the weight distribution of $C_F^\perp$ is by definition too.
Moreover, if F is APN on $\mathbb{F}_{2^n}$ and $n > 2$, then the code $C_F^\perp$ has dimension $2n$, *i.e.*, the code of generator matrix $\left[\begin{array}{ccccc} F(1) & F(\alpha) & F(\alpha^2) & \dots & F(\alpha^{2^n-2}) \end{array} \right]$, which can be seen as the code $\{tr(bF(x);\, b \in \mathbb{F}_{2^n}\}$, has dimension n and intersects the simplex code $\{tr(ax);\, a \in \mathbb{F}_{2^n}\}$ (whose generator matrix is equal to $\left[\begin{array}{ccccc} 1 & \alpha & \alpha^2 & \dots & \alpha^{2^n-2} \end{array} \right]$) only in the null vector. Equivalently:

Proposition 11 *Let F be an APN function in $n > 2$ variables. Then the nonlinearity of F cannot be null and the code $C_F^\perp$ has dimension $2n$.*

Proof. Suppose there exists $b \neq 0$ such that $b \cdot F$ is affine. Without loss of generality (by composing F with an appropriate linear automorphism and adding an affine function to F), we can assume that $b = (0, \cdots, 0, 1)$ and that $b \cdot F$ is null. Then, every derivative of F is 2-to-1 and has null last coordinate. The $(n, n-1)$ function obtained by erasing the last coordinate of $F(x)$ has therefore balanced derivatives; hence it is a bent $(n, n-1)$-function, a contradiction with Nyberg's result, since $n - 1 > n/2$. □
Note that for $n = 2$, the nonlinearity can be null. An example is the function $(x_1, x_2) \to (x_1 x_2, 0)$.

J. Dillon (private communication) observed that this property of the dimension of $C_F^\perp$, valid for every APN function, implies that, for every nonzero $c \in \mathbb{F}_{2^n}$, the equation $F(x) + F(y) + F(z) + F(x + y + z) = c$ must have a solution (that is, the function Φ_F introduced after Proposition 9 is onto $\mathbb{F}_2^n \setminus \{0\}$). Indeed, otherwise $F(x) + cg(x)$ would be APN for every Boolean function $g(x)$. In particular, for $g(x) = tr(b_0 F(x))$ with $b_0 \notin c^\perp$, we would have $tr(b_0[F(x) + cg(x)]) = tr(b_0 F(x)) + tr(b_0 c)g(x) = 0$, a contradiction with the fact that $C_{F+cg}^\perp$ has dimension $2n$ (since $F + cg$ is APN).

• We have seen that all AB functions are APN. The converse is false, in general. But if n is odd and if F is APN, then there exists a nice necessary

and sufficient condition, for F being AB: the weights of $C_F^{\perp}$ are all divisible by $2^{\frac{n-1}{2}}$ (see [30], where the divisibilities for several types of such codes are calculated, where tables of exact divisibilities are computed and where proofs are given that a great deal of power functions are not AB). In other words:

Proposition 12 *Let F be an APN (n,n)-function, n odd. Then F is AB if and only if all the values $\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x}$ of the Walsh spectrum of F are divisible by $2^{\frac{n+1}{2}}$.*

As shown in [29, 26], this can be proved easily:
Proof. The condition is clearly necessary. Conversely, assume that F is APN and that all the values $\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x}$ are divisible by $2^{\frac{n+1}{2}}$. Writing $\left(\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x}\right)^2 = 2^{n+1}\lambda_{u,v}$, where all $\lambda_{u,v}$'s are integers, Relation (12) implies then

$$\sum_{v\in\mathbb{F}_2^{n*},u\in\mathbb{F}_2^n}(\lambda_{u,v}^2-\lambda_{u,v})=0, \tag{13}$$

and since all the integers $\lambda_{u,v}^2-\lambda_{u,v}$ are non-negative ($\lambda_{u,v}$ being an integer), we deduce that, for every $v\in\mathbb{F}_2^{n*}, u\in\mathbb{F}_2^n$, $\lambda_{u,v}^2=\lambda_{u,v}$, *i.e.* $\lambda_{u,v}\in\{0,1\}$. $\diamond$

Hence, if an APN function F is plateaued, or more generally if $F=F_1\circ F_2^{-1}$ where F_2 is a permutation and where the linear combinations of the component functions of F_1 and F_2 are plateaued, then F is AB. Indeed, the sum $\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x}=\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F_1(x)\oplus u\cdot F_2(x)}$ is then divisible by $2^{\frac{n+1}{2}}$. This allows to deduce easily the AB property of Gold and Kasami functions (see their definitions below) from their APN property, since the Gold functions are quadratic and the Kasami functions are equal, when n is odd, to $F_1\circ F_2^{-1}$ where $F_1(x)=x^{2^{3k}+1}$, $x\in BbbF_{2^n}$ and $F_2(x)=x^{2^k+1}$ are quadratic.

• A necessary condition dealing with *quadratic terms in the ANF of any APN function* has been observed in [5]. Given any APN function F (quadratic or not), every quadratic term x_ix_j $(1\le i<j\le n)$ must appear with a non-null coefficient in the algebraic normal form of F. Indeed, we know that the coefficient of any monomial $\prod_{i\in I}x^i$ in the ANF of F equals $a_I=\sum_{x\in\mathbb{F}_2^n/\ supp(x)\subseteq I}F(x)$ (this sum being calculated in $\mathbb{F}_2^n$). Applied for instance to $I=\{n-1,n\}$, this gives $a_I=F(0,\ldots,0,0,0)+F(0,\ldots,0,0,1)+F(0,\ldots,0,1,0)+F(0,\ldots,0,1,1)$, and F being APN, this vector can not be

null. Note that, since the notion of almost perfect nonlinearity is affinely invariant (see below), this condition must be satisfied by all of the functions $L \circ F \circ L'$, where L and L' are affine automorphisms of $\mathbb{F}_2^n$. Extended this way, the condition becomes necessary and sufficient (indeed, for every distinct x, y, z in $\mathbb{F}_2^n$, there exists an affine automorphism L' of $\mathbb{F}_2^n$ such that $L'(0, \ldots, 0, 0, 0) = x$, $L'(0, \ldots, 0, 1, 0) = y$ and $L'(0, \ldots, 0, 0, 1) = z$).

In the case n even: If F is APN and plateaued, then Relation (13) again shows that there must exist $v \in \mathbb{F}_2^{n*}, u \in \mathbb{F}_2^n$ such that $\sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot F(x) \oplus u \cdot x}$ is not divisible by $2^{(n+2)/2}$, that is, equals $\pm 2^{n/2}$. Indeed, otherwise, all the numbers $\lambda_{u,v}^2 - \lambda_{u,v}$ are non-negative and at least one is strictly positive. Hence there must exist $v \in \mathbb{F}_2^{n*}$ such that the Boolean function $v \cdot F$ is bent. *Note that this implies that F cannot be a permutation*, according to Proposition 1 and since a bent Boolean function is never balanced. More precisely, the numbers $\lambda_{u,v}$ involved in Equation (13) can be divided into two categories: those such that the function $v \cdot F$ is bent (for each such v, we have $\lambda_{u,v} = 1/2$ for every u and therefore $\sum_{u \in \mathbb{F}_2^n} (\lambda_{u,v}^2 - \lambda_{u,v}) = -2^{n-2}$); and those such that $v \cdot F$ is not bent (then $\lambda_{u,v} \in \{0, 2^i\}$ for some $i \geq 1$ and we have, thanks to Parseval's relation: $\sum_{u \in \mathbb{F}_2^n} (\lambda_{u,v}^2 - \lambda_{u,v}) = \frac{2^{2n}}{2^{n+1}}(2^i - 1) = 2^{n-1}(2^i - 1) \geq 2^{n-1}$). Equation (13) implies then that the number B of those v such that $v \cdot F$ is bent satisfies $-B\, 2^{n-2} + (2^n - 1 - B)\, 2^{n-1} \leq 0$, which implies that *the number of bent functions among the functions $v \cdot F$ is at least* $\frac{2}{3}(2^n - 1)$.
In the case of the Gold functions $F(x) = x^{2^i+1}$, $gcd(i, n) = 1$ (see Subsection 2.1.6), the number of bent functions among the functions $tr(vF(x))$ equals $\frac{2}{3}(2^n - 1)$. Indeed, the function $tr(vF(x))$ is bent if and only if there is no nonzero $x \in \mathbb{F}_{2^n}$ such that $tr(vx^{2^i} y + vxy^{2^i}) = 0$ for every $y \in \mathbb{F}_{2^n}$ (see the chapter "Boolean Functions for Cryptography and Error Correcting Codes", Subsections 5.1 and 6.2), *i.e.*, the equation $vx^{2^i} + (vx)^{2^{n-i}} = 0$ has no nonzero solution. Raising this equation to the 2^i-th power gives $v^{2^i} x^{2^{2i}} + vx = 0$ and $2^i - 1$ being co-prime with $2^n - 1$, it is equivalent, after dividing by vx (when $x \neq 0$) and taking the $(2^i - 1)$th root, to $vx^{2^i+1} \in \mathbb{F}_2$. Hence, the function $tr(vF(x))$ is bent if and only if v is not the $(2^i + 1)$-th power of an element of $\mathbb{F}_{2^n}$, that is (since $gcd(2^i + 1, 2^n - 1) = 3$), v is not the third power of an element of $\mathbb{F}_{2^n}$.
Note that, given an APN plateaued function F, saying that the number of bent functions among the functions $tr(vF(x))$ equals $\frac{2}{3}(2^n - 1)$ is equivalent to saying, according to the observations above, that F has nonlinearity

$2^{n-1}-2^{n/2}$ and it is also equivalent to saying that F has the same extended Walsh spectrum as the Gold functions. Note that it can be characterized by using the same method as for proving Proposition 9: an APN function F has same extended Walsh spectrum as the Gold functions if and only if, for every $v \in \mathbb{F}_2^{n*}$ and every $u \in \mathbb{F}_2^n$, denoting $W_{v\cdot F}(u) = \sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x}$, we have $W_{v\cdot F}(u)\left(W_{v\cdot F}^2(u)-2^{n+1}\right)\left(W_{v\cdot F}^2(u)-2^n\right)=0$, that is, $W_{v\cdot F}^5(u)-3\cdot 2^n W_{v\cdot F}^3(u)+2^{2n+1}W_{v\cdot F}(u)=0$; applying the Fourier transform and dividing by 2^{2n}, this is equivalent to the fact that

$$\left|\left\{(x_1,\cdots,x_5)\in\mathbb{F}_2^{5n}/\left\{\begin{array}{l}\sum x_i=a\\ \sum F(x_i)=b\end{array}\right\}\right|-2^{3n}-$$

$$3\cdot 2^n\left(\left|\left\{(x_1,\cdots,x_3)\in\mathbb{F}_2^{3n}/\left\{\begin{array}{l}\sum x_i=a\\ \sum F(x_i)=b\end{array}\right\}\right|-2^n\right)+$$

$$2^{2n+1}\left(\left|\left\{x\in\mathbb{F}_2^n/\left\{\begin{array}{l}x=a\\ F(x)=b\end{array}\right\}\right|-2^{-n}\right)=0$$

for every $a,b\in\mathbb{F}_2^n$. A necessary condition is (taking $b=F(a)$ and using that F is APN) that, for every $a,b\in\mathbb{F}_2^n$, we have

$$\left|\left\{(x_1,\cdots,x_5)\in\mathbb{F}_2^{5n}/\left\{\begin{array}{l}\sum x_i=a\\ \sum F(x_i)=b\end{array}\right\}\right|=$$

$$2^{3n}+3\cdot 2^n(3\cdot 2^n-2-2^n)-2^{2n+1}(1-2^{-n})=$$

$$2^{3n}+2^{2n+2}-2^{n+2}.$$

There exist APN quadratic functions whose Walsh spectra are different from the Gold functions. For instance, K. Browning *et al.* [12] have exhibited such function in 6 variables: $F(x)=x^3+u^{11}x^5+u^{13}x^9+x^{17}+u^{11}x^{33}+x^{48}$, where u is a primitive element in the field. For this function, we get the following spectrum: 46 functions $tr(vF(x))$ are bent, 16 are plateaued with amplitude 16 and one is plateaued with amplitude 32. □

2.1.3 The particular case of power functions

We have seen that the notion of AB function being independent of the choice of the inner product, we can identify $\mathbb{F}_2^n$ with the field $\mathbb{F}_{2^n}$ and take $x\cdot y=tr(xy)$ for inner product, where tr is the trace function from this field to $\mathbb{F}_2$. This allows to consider those particular (n,n)-functions which have the form $F(x)=x^d$, called *power functions* (and sometimes, monomial functions).

When F is a power function, it is enough to check the APN property for $a = 1$ only, since changing, for every $a \neq 0$, the variable x into ax in the equation $F(x) + F(x + a) = b$ gives $F(x) + F(x + 1) = \frac{b}{F(a)}$. Moreover, checking the AB property $\sum_{x\in\mathbb{F}_{2^n}}(-1)^{tr(vF(x)+ux)} \in \{0, \pm 2^{\frac{n+1}{2}}\}$, for every $u, v \in \mathbb{F}_{2^n}$, $v \neq 0$, is enough for $u = 0$ and $u = 1$ (and every $v \neq 0$), since changing x into $\frac{x}{u}$ (if $u \neq 0$) in this sum gives $\sum_{x\in\mathbb{F}_{2^n}}(-1)^{tr(v'F(x)+x)}$, for some $v' \neq 0$. If F is a permutation, then checking the AB property is enough for $v = 1$ (and every u), since changing x into $\frac{x}{F^{-1}(v)}$in this sum gives $\sum_{x\in\mathbb{F}_{2^n}}(-1)^{tr\left(F(x)+\frac{ux}{F^{-1}(v)}\right)}$.
Also, when F is an APN power function, we have additional information on its bijectivity. The author, Charpin and Zinoviev proved in [36] that, when n is even, no APN function exists in a class of permutations including power permutations, that we describe now. Let $k = \frac{2^n-1}{3}$ (which is an integer, since n is even) and let α be a primitive element of the field $\mathbb{F}_{2^n}$. Then $\beta = \alpha^k$ is a primitive element of $\mathbb{F}_4$. Hence, $\beta^2 + \beta + 1 = 0$. For every j, the element $\beta^{2j} + \beta^j = (\beta+1)^j + \beta^j$ equals 1 if j is coprime with 3 (since β^j is then also a primitive element of $\mathbb{F}_4$), and is null otherwise. Let $F(x) = \sum_{j=0}^{2^n-1} \delta_j x^j$, ($\delta_j \in \mathbb{F}_{2^n}$) be an (n, n)-function. According to the observations above, β and $\beta+1$ are the solutions of the equation $F(x)+F(x+1) = \sum_{gcd(j,3)=1} \delta_j$. Also, the equation $F(x)+F(x+1) = \sum_{j=1}^{2^n-1} \delta_j$ admits 0 and 1 for solutions. Thus, if F is APN, then $\sum_{i=1}^{k} \delta_{3i} \neq 0$. If F is a power function, then it can not be a permutation.
H. Dobbertin gives in [64] a result valid only for power functions but slightly more precise, and he completes it in the case when n is odd: if a power function $F(x) = x^d$ is APN, then its kernel (when we view F as an endomorphism of $\mathbb{F}_{2^n}^*$) is the intersection of $\mathbb{F}_4$ with $\mathbb{F}_{2^n}^*$; in other words, $x^d = 1$ if and only if $x^3 = 1$, that is, $gcd(d, 2^n - 1)$ equals 1 if n is odd and equals 3 if n is even; thus *APN power functions are permutations of* $\mathbb{F}_{2^n}^*$ *if* n *is odd, and are three-to-one if* n *is even.* Indeed, suppose that $x^d = 1$ with $x \neq 1$. Then there is a (unique) y in $\mathbb{F}_{2^n}$, $y \neq 0, 1$, such that $x = (y + 1)/y$. The equality $x^d = 1$ implies then $(y + 1)^d + y^d = 0 = (y^2 + 1)^d + (y^2)^d$. By the APN property and since $y^2 \neq y$, we conclude $y^2 + y + 1 = 0$. Thus, y, and therefore x, are in $\mathbb{F}_4$ and $x^3 = 1$. Conversely, if $x \neq 1$ is an element of $\mathbb{F}_{2^n}^*$ such that $x^3 = 1$, then 3 divides $2^n - 1$ and n must be even. Then, since d must then be divisible by 3 (indeed, otherwise, the restriction of x^d to $\mathbb{F}_4$ is linear and therefore x^d is not APN), $x^d = 1$.

A. Canteaut proves in [27] that for n even, if a power function $F(x) = x^d$ on $\mathbb{F}_{2^n}$ is not a permutation (*i.e.* if $gcd(d, 2^n - 1) > 1$), then the nonlin-

earity of F is upper bounded by $2^{n-1} - 2^{n/2}$ (she also studies the case of equality). Indeed, denoting $gcd(d, 2^n - 1)$ by d_0, for every $v \in \mathbb{F}_{2^n}$, the sum $\sum_{x\in\mathbb{F}_{2^n}}(-1)^{tr(vx^d)}$ equals $\sum_{x\in\mathbb{F}_{2^n}}(-1)^{tr(vx^{d_0})}$ which implies that $\sum_{v\in\mathbb{F}_{2^n}}\left(\sum_{x\in\mathbb{F}_{2^n}}(-1)^{tr(vx^d)}\right)^2$ equals $2^n\,|\{(x,y),\ x,y \in \mathbb{F}_{2^n},\ x^{d_0} = y^{d_0}\}|$. The number of elements in the image of $\mathbb{F}_{2^n}^*$ by the mapping $x \to x^{d_0}$ is $(2^n - 1)/d_0$ and every element of this image has d_0 pre-images. Hence, $\sum_{v\in\mathbb{F}_{2^n}^*}\left(\sum_{x\in\mathbb{F}_{2^n}}(-1)^{tr(vx^d)}\right)^2$ equals $2^n[(2^n - 1)d_0 + 1] - 2^{2n} = 2^n(2^n - 1)(d_0 - 1)$ and $\max_{v\in\mathbb{F}_{2^n}^*}\left(\sum_{x\in\mathbb{F}_{2^n}}(-1)^{tr(vx^d)}\right)^2 \geq 2^n(d_0 - 1) \geq 2^{n+1}$.
The possible values of the sum $\sum_{x\in\mathbb{F}_{2^n}}(-1)^{tr(vx^d)}$ are determined in [4] for APN power functions in an even number of variables.

If F is a power function, then the linear codes C_F and $C_F^\perp$ (viewed in Proposition 10) are *cyclic*, that is, invariant under cyclic shifts of their coordinates (see [90]). Indeed, $(c_0, \ldots, c_{2^n-2})$ belongs to C_F if and only if $c_0 + c_1\alpha + \ldots + c_{2^n-2}\alpha^{2^n-2} = 0$ and $c_0 + c_1\alpha^d + \ldots + c_{2^n-2}\alpha^{(2^n-2)d} = 0$; this implies $c_{2^n-2} + c_0\alpha + \ldots + c_{2^n-3}\alpha^{2^n-2} = 0$ and $c_{2^n-2} + c_0\alpha^d + \ldots + c_{2^n-3}\alpha^{(2^n-2)d} = 0$. Cyclic codes have been extensively studied in coding theory. They have very useful properties, that we briefly recall: representing each codeword $(c_0, \ldots, c_{2^n-2})$ by the polynomial $c_0+c_1X+\ldots+c_{2^n-2}X^{2^n-2}$, we obtain an ideal of the quotient algebra $\mathbb{F}_2[X]/(X^{2^n-1} + 1)$ (viewed as a set of polynomials of degrees at most $2^n - 2$, each element of the algebra being identified to its minimum degree representent). This algebra is a principal domain, and any (linear) cyclic code has a unique element having minimal degree, called its *generator polynomial*. The generator polynomial being (as easily shown) a divisor of $X^{2^n-1} + 1$, its roots all belong to $\mathbb{F}_{2^n}^*$. The code equals the set of all those polynomials which include the roots of the generator polynomial among their own roots. The generator polynomial having all its coefficients in $\mathbb{F}_2$, its roots are of the form $\{\alpha^i,\ i \in I\}$ where $I \subseteq \mathbb{Z}/(2^n - 1)\mathbb{Z}$ is a union of cyclotomic classes of 2 modulo $2^n - 1$. The set I is called the *defining set* of the code. The generator polynomial of $C^\perp$ is the reciprocal of the quotient of $X^{2^n-1} + 1$ by the generator polynomial of C, and its defining set therefore equals $\{2^n - 1 - i;\ i \in \mathbb{Z}/(2^n - 1)\mathbb{Z} \setminus I\}$. In the case of C_F, the defining set I is precisely the union of the two cyclotomic classes of 1 and d.
A very efficient bound on the minimum distance of cyclic codes is the *BCH bound* [90]: if I contains a string $\{l+1, \ldots, l+k\}$ of length k in $\mathbb{Z}/(2^n-1)\mathbb{Z}$, then the cyclic code has minimum distance greater than or equal to $k + 1$. This bound shows for instance directly that the function $x^{2^{\frac{n-1}{2}}+1}$, n odd, is

AB: by definition, the defining set I of C_F equals the union of the cyclotomic classes of 1 and $2^{\frac{n-1}{2}}+1$, that is

$$\{1, 2, \cdots, 2^{n-1}\} \cup \{2^{\frac{n-1}{2}}+1, 2^{\frac{n+1}{2}}+1, 2^{\frac{n+1}{2}}+2, \cdots, 2^{n-1}+2^{\frac{n-1}{2}}\}.$$

The defining set of $C_F^{\perp}$ equals then $\mathbb{Z}/(2^n-1)\mathbb{Z} \setminus \{-i,\ i \notin I\}$ (this property is valid for every cyclic code, see [90]). Since there is no element equal to $2^{n-1}+2^{\frac{n-1}{2}}+1, \cdots, 2^n-1$ in I, the defining set of $C_F^{\perp}$ contains then a string of length $2^{n-1}-2^{\frac{n-1}{2}}-1$. Hence the nonzero codewords of this code have weight at least $2^{n-1}-2^{\frac{n-1}{2}}$ which means that the function is AB.
The powerful *McEliece Theorem* (see *e.g.* [90]) gives the exact divisibility of the codewords of cyclic codes. Translated in terms of vectorial functions, it says that if d is relatively prime to 2^n-1, the exponent e_d of the greatest power of 2 dividing all the Walsh coefficients of the power function x^d is given by $e_d = \min\{w_2(t_0)+w_2(t_1),\ 1 \leq t_0,\ t_1 < 2^n-1;\ t_0+t_1 d \equiv 0 \pmod{2^n-1}\}$. It can be used in relationship with Proposition 12. This led to the proof, by Canteaut, Charpin and Dobbertin, of a several decade old conjecture due to Welch (see below).

Note finally that, if F is a power function, then the Boolean function γ_F seen in Proposition 8 is within the framework of Dobbertin's triple construction [57].

2.1.4 Stability of APN and AB properties

The right and left compositions of an APN (resp. AB) function by an affine permutation are APN (resp. AB). Two functions are called *affine equivalent* if one is equal to the other, composed by such affine permutations. Adding an affine function to an APN (resp. AB) function respects its APN (resp. AB) property. Two functions are called *extended affine equivalent* (EA-equivalent) if one is affine equivalent to the other, added with an affine function.
The inverse of an APN (resp. AB) permutation is APN (resp. AB).
There exists a notion of equivalence between two functions F and G which respects APNness and ABness and which is more general than the EA-equivalence between F and G or between F and G^{-1} (if G is a permutation) or *vice versa* or between F^{-1} and G^{-1} (if F and G are permutations). Let F_1 be a permutation on $\mathbb{F}_2^n$, and let F_2 be a function from $\mathbb{F}_2^n$ to itself. By definition, $F_2 \circ {F_1}^{-1}$ is APN if and only if, for any nonzero element (a,b) of $(\mathbb{F}_2^n)^2$, the system: $\begin{cases} F_2 \circ {F_1}^{-1}(x) + F_2 \circ {F_1}^{-1}(y) &= b \\ x+y &= a \end{cases}$ admits at most

two solutions (x, y).
Changing x and y into $F_1(x)$ and $F_1(y)$, we obtain that the function $F_2 \circ {F_1}^{-1}$ is APN if and only if the system: $\begin{cases} F_2(x) + F_2(y) &= b \\ F_1(x) + F_1(y) &= a \end{cases}$ admits at most two solutions. We then deduce:

Proposition 13 *Let F be an APN (resp. AB) function on $\mathbb{F}_2^n$ and L_1, L_2 be two affine functions from $\mathbb{F}_2^{2n}$ to $\mathbb{F}_2^n$. Assume that (L_1, L_2) is a permutation on $\mathbb{F}_2^{2n}$ and that the function $F_1(x) = L_1(x, F(x))$ is a permutation on $\mathbb{F}_2^n$. Then, denoting $F_2(x) = L_2(x, F(x))$, the function $F_2 \circ F_1^{-1}$ is APN (resp. AB) and $\gamma_{F_2 \circ F_1^{-1}}$ equals $\gamma_F \circ L^{-1}$, where L is linear and $(L_1, L_2) = L + cst$.*

Proof. The value $\gamma_{F_2 \circ F_1^{-1}}(a, b)$ equals 1 if and only if $a \neq 0$ and there exists (x, y) in $\mathbb{F}_2^n \times \mathbb{F}_2^n$ such that $F_1(x) + F_1(y) = a$ and $F_2(x) + F_2(y) = b$. Thus, $\gamma_{F_2 \circ F_1^{-1}}$ is equal to $\gamma_F \circ L^{-1}$. The function $\gamma_{F_2 \circ F_1^{-1}}$ is therefore bent (resp. has weight $2^{2n-1} - 2^{n-1}$) if and only if γ_F is bent (resp. has weight $2^{2n-1} - 2^{n-1}$). Proposition 8 completes the proof. □

Proposition 13 can also be stated in the following way:
- If the graphs $\{(x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \mid y = F(x)\}$ and $\{(x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \mid y = G(x)\}$ of two functions F and G are affine equivalent, then F is APN (resp. AB) if and only if G is APN (resp. AB). According to the terminology introduced in [13], the functions F and G are then called *CCZ-equivalent*.
- Given a function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ and an affine automorphism $L = (L_1, L_2)$ of $\mathbb{F}_2^n \times \mathbb{F}_2^n$, the image of the graph of F by L is the graph of a function if and only if the function $F_1(x) = L_1(x, F(x))$ is a permutation.

All the transformations we have seen previously to Proposition 13, that respect APN (resp. AB) property, are particular cases of this general one:
- if $(L_1, L_2)(x, y) = (y, x)$, then $F_2 \circ F_1^{-1}$ is equal to F^{-1};
- if $L_1(x, y)$ and $L_2(x, y)$ only depend on x and y, respectively, this corresponds to the right and left compositions of F by linear permutations;
- if $L_2(x, y) = y + L(x)$ and $L_1(x, y) = x$ where L is any affine function from $\mathbb{F}_2^n$ to itself, then we obtain $F(x) + L(x)$.

CCZ-equivalence does not preserve crookedness.

2.1.5 Known AB functions

Power functions: Until recently, the only known examples of AB functions were (up to EA-equivalence) the power functions $x \mapsto x^d$ on the field

$\mathbb{F}_{2^n}$ (n odd) corresponding to the following values of d, and the inverses of these power functions:

• $d = 2^h + 1$ with $\gcd(h, n) = 1$ and $1 \leq h \leq \frac{n-1}{2}$ (proved by Gold, see [67, 94]). These power functions are called *Gold functions*.
• $d = 2^{2h} - 2^h + 1$ with $\gcd(h, n) = 1$ and $2 \leq h \leq \frac{n-1}{2}$ (the AB property of this function is equivalent to a result by Kasami [80], historically due to Welch, but never published by him; see another proof in [59]). These power functions are called *Kasami functions*.
• $d = 2^{(n-1)/2} + 3$ (conjectured by Welch and proved by Canteaut, Charpin and Dobbertin, see [29, 30, 60]). These power functions are called *Welch function*.
• $d = 2^{(n-1)/2} + 2^{(n-1)/4} - 1$, where $n \equiv 1 \pmod 4$ (conjectured by Niho, proved by Hollman and Xiang, after the work by Dobbertin, see [74, 61]).
• $d = 2^{(n-1)/2} + 2^{(3n-1)/4} - 1$, where $n \equiv 3 \pmod 4$ (idem). The power functions in these two last cases are called *Niho functions*.
The conditions "$1 \leq h \leq \frac{n-1}{2}, \ldots$" are made to avoid equivalent exponents.

It was proved [16] that Gold functions are pairwise CCZ-inequivalent and that they are in general CCZ-inequivalent to Kasami and Welch functions.

The proof of the fact that the Gold function is AB is easy, either by using Proposition 12 of the present chapter, or by using the properties of quadratic functions recalled in the chapter "Boolean Functions for Cryptography and Error Correcting Codes", at Subsection 5.1. The value at a of the Walsh transform of the Gold Boolean function $tr(x^{2^h+1})$ equals $\pm 2^{\frac{n+1}{2}}$ if $tr(a) = 1$ and is null otherwise, since $tr(x^{2^h}y + xy^{2^h}) = tr((x^{2^h} + x^{2^{n-h}})\, y)$ is null for every y if and only if $x \in \mathbb{F}_2$, and since $tr(x^{2^h+1} + ax)$ is constant on $\mathbb{F}_2$ if and only if $tr(a) = 1$. This gives easily the magnitude (but not the sign; partial results on the sign are given in [86]) of the Walsh transform of the vectorial Gold function, this function being a permutation (see Subsection 2.1.3). The proofs of the almost bentness of the other functions can be derived from their almost perfect nonlinearity (see below) and from Proposition 12 (and McEliece's Theorem in the case of the Welch function). More can be said in the case of the Kasami function: it has been proved in [55, Theorem 15] that, if $3h$ is congruent with 1 mod n, then the Walsh support of the Kasami Boolean function $tr(x^{2^{2h}-2^h+1})$ equals the support of the Gold Boolean function $tr(x^{2^h+1})$ (*i.e.* the set $\{x \in \mathbb{F}_{2^n} \,|\, tr(x^{2^h+1}) = 1\}$) if n is odd and equals the set $\{x \in \mathbb{F}_{2^n} \,|\, Tr_{n/2}(x^{2^h+1}) = 0\}$ if n is even, where $Tr_{n/2}$ is the trace

function from $\mathbb{F}_{2^n}$ to the field $\mathbb{F}_{2^2}$: $Tr_{n/2}(x) = x + x^4 + x^{4^2} + \ldots + x^{4^{n/2-1}}$. When n is odd, this gives the magnitude (but not the sign) of the Walsh transform of the vectorial Kasami function, this function being a permutation. Note that this gives also an information on the autocorrelation of the Kasami Boolean function: the Fourier transform of the function $a \to \mathcal{F}(D_a f) = \sum_{x \in \mathbb{F}_2^n} (-1)^{D_a f(x)}$, where f is the Kasami Boolean function, equals the square of the Walsh transform of f. According to Dillon's and Dobbertin's result recalled above, and since we know that the Kasami function is almost bent when n is odd, the value at b of the square of the Walsh transform of f equals then 2^{n+1} if $tr(x^{2^h+1}) = 1$ and equals zero otherwise. Hence, by applying the inverse Fourier transform (that is, by applying the Fourier transform again and dividing by 2^n), $\mathcal{F}(D_a f)$ equals twice the Fourier transform of the function $tr(x^{2^h+1})$. We deduce that, except at the zero vector, $\mathcal{F}(D_a f)$ equals the opposite of the Walsh transform of the function $tr(x^{2^h+1})$.

Remark. There is a close relationship between AB functions and *sequences* used for radars and for spread-spectrum communications. A binary sequence which can be generated by an LFSR, or equivalently which satisfies a linear recurrence relation $s_i = a_1 s_{i-1} \oplus \ldots \oplus a_n s_{i-n}$, is called *maximum-length* if its period equals $2^n - 1$, which is the maximum possible value. Such a sequence has the form $tr(\lambda \alpha^i)$, where $\lambda \in \mathbb{F}_{2^n}$ and α is some primitive element of $\mathbb{F}_{2^n}$, and where tr is the trace function on $\mathbb{F}_{2^n}$. Consequently, its autocorrelation values $\sum_{i=0}^{2^n-2} (-1)^{s_i \oplus s_{i+t}}$ $(1 \leq t \leq 2^n - 2)$ are equal to -1, that is, are optimum. Such a sequence, also called an *m-sequence*, can be used for radars and for code division multiple access (CDMA) in telecommunications, since it allows to send a signal which can be easily distinguished from any time-shifted version of itself. Finding an AB power function x^d on the field $\mathbb{F}_{2^n}$ allows to have a d-decimation[5] $s'_i = tr(\lambda \alpha^{di})$ of the sequence, whose crosscorrelation values $\sum_{i=0}^{2^n-2} (-1)^{s_i \oplus s'_{i+t}}$ $(0 \leq t \leq 2^n - 2)$ have minimum overall magnitude[6] [70]. The conjectures that the power functions above were AB have been stated (before being proved later) in the framework of sequences for this reason.

[5] Another m-sequence if d is co-prime with $2^n - 1$.

[6] This allows, in code division multiple access, to give different signals to different users (one for each such decimation) which can be easily distinguished from any other signal and its time-shifted versions.

Non-power functions: It was conjectured that all AB functions were affinely equivalent to power functions. This conjecture was later disproved:

Functions CCZ-equivalent to power functions:

• Using the stability of the AB property by CCZ-equivalence and the fact that the Gold function is AB, two new infinite classes of AB functions have been introduced in [13], which disprove the conjecture:
1. The function $F(x) = x^{2^i+1} + (x^{2^i} + x)\, tr(x^{2^i+1} + x)$, where $n > 3$ is odd and $gcd(n, i) = 1$, is AB. It is EA-inequivalent to any power function and it is EA-inequivalent to any permutation (at least for $n = 5$).
2. For n odd and divisible by m, $n \neq m$ and $\gcd(n, i) = 1$, the following function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$:

$$x^{2^i+1} + tr_{n/m}(x^{2^i+1}) + x^{2^i} tr_{n/m}(x) + x\ tr_{n/m}(x)^{2^i} +$$
$$[tr_{n/m}(x)^{2^i+1} + tr_{n/m}(x^{2^i+1}) + tr_{n/m}(x)]^{\frac{1}{2^i+1}} (x^{2^i} + tr_{n/m}(x)^{2^i} + 1) +$$
$$[tr_{n/m}(x)^{2^i+1} + tr_{n/m}(x^{2^i+1}) + tr_{n/m}(x)]^{\frac{2^i}{2^i+1}} (x + tr_{n/m}(x))$$

where $tr_{n/m}$ denotes the relative trace function $tr_{n/m}(x) = \sum_{i=0}^{n/m-1} x^{2^{mi}}$, is an AB function of algebraic degree $m+2$ which is EA-inequivalent to any power function; the question of knowing whether it is inequivalent to any permutation is open.

Functions CCZ-inequivalent to power functions:

• The problem of knowing whether there exist AB functions which are CCZ-inequivalent to power functions remained open after the introduction of the two functions above. Also, it was conjectured that any quadratic APN function is EA-equivalent to Gold functions and this problem remained open.
A paper by Edel, Kyureghyan and Pott [65] introduced two quadratic functions from $\mathbb{F}_{2^{10}}$ (resp. $\mathbb{F}_{2^{12}}$) to itself. The first one is proved to be CCZ-inequivalent to any power function.
These two (quadratic) functions were isolated and this left open the question of knowing whether a whole infinite class of APN functions being not CCZ-equivalent to power functions could be exhibited. Such existence was proved in [14, 15]. A new class of AB functions was found:

Proposition 14 *Let s and k be positive integers with* $\gcd(s, 3k) = 1$ *and*

$t \in \{1,2\}$, $i = 3-t$. *Furthermore let* $d = 2^{ik} + 2^{tk+s} - (2^s+1)$,

$$g_1 = \gcd(2^{3k}-1, d/(2^k-1)),$$

$$g_2 = \gcd(2^k-1, d/(2^k-1)).$$

If $g_1 \neq g_2$ *then the function*

$$\begin{array}{rcl} F : \mathbb{F}_{2^{3k}} & \to & \mathbb{F}_{2^{3k}} \\ x & \mapsto & \alpha^{2^k-1} x^{2^{ik}+2^{tk+s}} + x^{2^s+1} \end{array}$$

where α *is primitive in* $\mathbb{F}_{2^{3k}}$ *is AB when* k *is odd and APN when* k *is even.*

It could be proved in [14, 15] that some of these functions are EA-inequivalent to power functions and CCZ-inequivalent to some AB power functions, and this was sufficient to deduce that they are CCZ-inequivalent to all power functions for some values of n:

Proposition 15 *Let* s *and* $k \geq 4$ *be positive integers such that* $s \leq 3k-1$, $\gcd(k,3) = \gcd(s,3k) = 1$, *and* $i = sk \bmod 3$, $t = 2i \bmod 3$, $n = 3k$. *If* $a \in \mathbb{F}_{2^n}$ *has the order* $2^{2k}+2^k+1$ *then the function* $F(x) = x^{2^s+1} + ax^{2^{ik}+2^{tk+s}}$ *is an AB permutation on* $\mathbb{F}_{2^n}$ *when* n *is odd and is APN when* n *is even. It is EA-inequivalent to power functions and CCZ-inequivalent to Gold and Kasami mappings.*

• It has been shown in [18] by L. Budaghyan, C. Carlet and G. Leander that for every odd positive integer, the function $x^3 + tr(x^9)$ is AB on $\mathbb{F}_{2^n}$. This function is the only example, with the function x^3, of a function which is AB for ant odd n.

2.1.6 Known APN functions

We list now the known APN functions (in addition to the AB functions listed above).

Power functions: The so-called *inverse* power permutation $x \mapsto F(x) = x^{2^n-2}$ (which equals $\frac{1}{x}$ if $x \neq 0$, and 0 otherwise) is APN if n is odd [5, 94]. Indeed, the equation $x^{2^n-2} + (x+1)^{2^n-2} = b$ ($b \neq 0$, since the inverse function is a permutation) admits 0 and 1 for solutions if and only if $b = 1$; and it (also) admits (two) solutions different from 0 and 1 if and only if there exists $x \neq 0, 1$ such that $\frac{1}{x} + \frac{1}{x+1} = b$, that is, $x^2 + x = \frac{1}{b}$. It is well-known that such existence is equivalent to the fact that $tr\left(\frac{1}{b}\right) = 0$. Hence, F is

APN if and only if $tr(1) = 1$, that is, if n is odd.
Consequently, the functions $x \mapsto x^{2^n-2^i-1}$, which are linearly equivalent to F (through the linear isomorphism $x \mapsto x^{2^i}$) are also APN, if n is odd.
If n is even, then the equation $x^{2^n-2} + (x+1)^{2^n-2} = b$ admits at most 2 solutions if $b \neq 1$ and admits 4 solutions (the elements of $\mathbb{F}_4$) if $b = 1$, which means that F opposes a good (but not optimal) resistance against differential cryptanalysis. Its nonlinearity equals $2^{n-1} - 2^{n/2}$ when n is even and it equals the highest even number upper bounded by this number, when n is odd (see [43]; Lachaud and Wolfmann proved in [85] that the set of values of its Walsh spectrum equals the set of all integers $s \equiv 0 \pmod 4$ in the range $[-2^{n/2+1} + 1; 2^{n/2+1} + 1]$; see more in [73]). Knowing whether there exist (n, n)-functions with nonlinearity strictly greater than this value when n is even is an open question (even for power functions). These are reasons the function $x \mapsto x^{2^n-2}$ has been chosen for the S-boxes of the AES (see more details in [94, 49]).
Until recently, the only known examples of APN and non-AB functions were (up to affine equivalence and to the addition of an affine function) the power functions $x \mapsto x^d$ corresponding to the following values of d:

• $d = 2^n - 2$, n odd (inverse function);
• $d = 2^h + 1$ with $\gcd(h, n) = 1$, n even and $1 \leq h \leq \frac{n-2}{2}$ (*Gold functions*, see [67, 94]);
• $d = 2^{2h} - 2^h + 1$ with $\gcd(h, n) = 1$, n even and $2 \leq h \leq \frac{n-2}{2}$ (*Kasami functions*, see [77], see also [59]);
• $d = 2^{\frac{4n}{5}} + 2^{\frac{3n}{5}} + 2^{\frac{2n}{5}} + 2^{\frac{n}{5}} - 1$, with n divisible by 5 (*Dobbertin functions*, see [62]). It has been shown by Canteaut, Charpin and Dobbertin [30] that this function can not be AB: they showed that $C_F^{\perp}$ contains words whose weights are not divisible by $2^{\frac{n-1}{2}}$.

The proof of the fact that the first of these functions is APN (whatever is the parity of n) is easy: the equality $F(x)+F(x+1) = F(y)+F(y+1)$ is equivalent to $(x+y)^{2^h} = (x+y)$, and thus implies that $x+y = 0$ or $x+y = 1$, since h and n are co-prime. Hence, any equation $F(x)+F(x+1) = b$ admits at most two solutions.
The proofs of the facts that the second and third functions are APN are difficult. They come down to showing that some mappings are permutations. H. Dobbertin gives in [63] a nice and general method for this.
The Gold and Kasami functions, for n even, have the best known nonlinearity too [67, 80], but not the Dobbertin functions. See [30] for a list of all

known *permutations* with best known nonlinearity. See also [56].
Inverse and Dobbertin functions are inequivalent to all other known APN functions because of their peculiar Walsh spectra.

Non-power functions: As for AB functions, it had been conjectured that all APN functions were EA-equivalent to power functions.

Functions CCZ-equivalent to power functions:

• Using also the stability properties recalled at Subsection 2.1.4, two more infinite classes of APN functions have been introduced in [13] and disprove this conjecture:
1. The function $F(x) = x^{2^i+1} + (x^{2^i} + x + 1)\, tr(x^{2^i+1})$, where $n \geq 4$ is even and $gcd(n, i) = 1$ is APN and is EA-inequivalent to any power function.
2. For n even and divisible by 3, the function $F(x)$ equal to

$$[x + tr_{n/3}(x^{2(2^i+1)} + x^{4(2^i+1)}) + tr(x)\, tr_{n/3}(x^{2^i+1} + x^{2^{2i}(2^i+1)})]^{2^i+1},$$

where $gcd(n, i) = 1$, is APN and is EA-inequivalent to any known APN function.

Functions CCZ-inequivalent to power functions:

• The functions viewed at Proposition 14 are APN when n is even and some of them can be proven CCZ inequivalent to Gold and Kasami mappings, as seen at Proposition 15. A similar class but with n divisible by 4 was later given in [17]. As observed by J. Bierbrauer, a common framework exists partially for these two classes:

Theorem 2 *Let:*
- $n = tk$ be a positive integer, with $t \in \{3, 4\}$, and s be such that t, s, k are pairwise coprime and such that t is a divisor of $k + s$,
- α be a primitive element of $\mathbb{F}_{2^n}$ and $w = \alpha^e$, where e is a multiple of $2^k - 1$, coprime with $2^t - 1$,
then the function

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

is APN.

For $n \geq 12$, these functions are EA-inequivalent to power functions and CCZ-inequivalent to Gold and Kasami mappings.

In particular, for $n = 12$, 20, 24, 28 they are CCZ-inequivalent to all power functions.

Proposition 14 has been partly generalized[7] in [9] by C. Bracken, E. Byrne, N. Markin and G. McGuire:

$$F(x) = u^{2^k} x^{2^{-k}+2^{k+s}} + ux^{2^s+1} + vx^{2^{-k}+1} + wu^{2^k+1} x^{2^{k+s}+2^s}$$

is APN on $\mathbb{F}_{2^{3k}}$, when $3 \,|\, k+s$, $(s, 3k) = (3, k) = 1$ and u is primitive in $\mathbb{F}_{2^{3k}}$, $v \neq w^{-1} \in \mathbb{F}_{2^k}$.
The same authors in the same paper obtained another generalization:

$$F(x) = bx^{2^s+1} + b^{2^k} x^{2^{k+s}+2^k} + cx^{2^k+1} + \sum_{i=1}^{k-1} r_i x^{2^{i+k}+2^i}$$

where k, s are odd and coprime, $b, c \in \mathbb{F}_{2^{2k}} \setminus \mathbb{F}_{2^k}$, $r_i \in \mathbb{F}_{2^k}$ is APN on $\mathbb{F}_{2^{2k}}$.
The extended Walsh spectrum of these functions is the same as for Gold function, see [10].

• The AB functions observed by L. Budaghyan, C. Carlet and G. Leander in [18] generalize to APN functions for n even:
Let n be any positive integer. Then the function $x^3 + tr(x^9)$ is APN on $\mathbb{F}_{2^n}$.
This function is CCZ-inequivalent to any Gold function on $\mathbb{F}_{2^n}$ if $n \geq 7$ and $n > 2p$ where p is the smallest positive integer different from 1 and 3 and coprime with n.
The extended Walsh spectrum of this function is the same as for the Gold functions as shown in [8].

• An idea of *J. Dillon* [53] was that functions of the form:

$$F(x) = x(Ax^2 + Bx^q + Cx^{2q}) + x^2(Dx^q + Ex^{2q}) + Gx^{3q},$$

where $q = 2^{n/2}$, n even, have good chances to be differentially 4-uniform.
L. Budaghyan and C. Carlet, pushing further Dillon's idea, obtained in [19] the following result:
Let n be even and i be co-prime with $n/2$. Set $q = 2^{n/2}$ and let $c, b \in \mathbb{F}_{2^n}$ be such that $c^{q+1} = 1$, $c \notin \{\lambda^{(2^i+1)(q-1)}, \lambda \in \mathbb{F}_{2^n}\}$, $cb^q + b \neq 0$. Then the function

$$F(x) = x^{2^{2i}+2^i} + bx^{q+1} + cx^{q(2^{2i}+2^i)}$$

[7] To be sure this is actually a generalization, we would need to have an example of a function of this class which would be CCZ-inequivalent to the functions of Proposition 14.

is APN on $\mathbb{F}_{2^n}$.
Such vectors b, c *do exist if and only if* $\gcd(2^i+1, q+1) \neq 1$. *For* $n/2$ *odd, this is equivalent to saying that* i *is odd.*

• L. Budaghyan and C.Carlet obtained in this same paper [19]:
Let n *be even and* i *be co-prime with* $n/2$. *Set* $q = 2^{n/2}$ *and let* $c \in \mathbb{F}_{2^n}$ *and* $s \in \mathbb{F}_{2^n} \setminus \mathbb{F}_q$. *If the polynomial*

$$X^{2^i+1} + cX^{2^i} + c^q X + 1$$

is irreducible over $\mathbb{F}_{2^n}$, *then the function*

$$F(x) = x(x^{2^i} + x^q + cx^{2^i q}) + x^{2^i}(c^q x^q + sx^{2^i q}) + x^{(2^i+1)q}$$

is APN on $\mathbb{F}_{2^n}$.
They checked with a computer that some of the functions of the present case and of the previous one are CCZ-inequivalent to power functions on $\mathbb{F}_{2^6}$. It remains open to prove the same property for every even $n \geq 6$.

Remark. The APN power functions listed above are not permutations when n is even. The question of knowing whether there exist APN permutations when n is even is open. We have seen that the answer is "no" for all plateaued functions (this was first observed in [96] when all the component functions of F are partially-bent; Nyberg generalized there a result given without a complete proof in [101], which was valid only for quadratic permutations). We have also seen above at Subsection 2.1.3 that the answer is "no" for a class of permutations including power permutations. And X.-d. Hou proved in [75] that it is also "no" for permutations with coefficients in $\mathbb{F}_2$ (more generally in $\mathbb{F}_{2^{n/2}}$).

3 Conclusion

The design of the AES has been partly founded on the studies (by K. Nyberg and others) on the notions of nonlinearity (for the resistance to linear attacks) and almost perfect nonlinearity (for the resistance to differential attacks). This has allowed the AES to use S-boxes working on bytes (it would not have been possible to find a good 8-bit-to-8-bit S-box by a computer search as this had been done for the 6-bit-to-4-bit S-boxes of the DES). However, from these studies, very few mappings emerged. The Gold functions, all the other recently found quadratic functions and the Welch

functions have too low algebraic degrees for being widely chosen for the design of new S-boxes. The Kasami functions themselves seem too closely related to quadratic functions. The inverse function has many very nice properties: large Walsh spectrum and good nonlinearity, differential uniformity of order at leat 4, fast implementation. But it has a potential weakness, which did not lead yet to efficient attacks, but may in the future: denoting its input by x and its output by y, the bilinear expression xy equals 1 for every nonzero x. As we can see, the candidates for future block ciphers not using the inverse function as an S-box are the Niho and Dobbertin functions. But the Niho functions exist only in odd numbers of variables, which is not convenient for implementation, and the Dobbertin function needs n to be divisible by 5. So further studies seem indispensable for the future designs of SP networks.

3.1 Main remaining open problems

1. Find a better bound than the covering radius bound for:
- n odd and $m < n$;
- n even and $n/2 < m < n$.
2. Find new primary (or secondary) constructions of perfect nonlinear (bent) functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^{n/2}$.
3. Find secondary constructions of APN and AB functions.
Observation: the construction of Proposition 4 can give functions $F_{\psi,H} : \mathbb{F}_2^n \to \mathbb{F}_{2^r}$ with extended Walsh spectrum $\{0, \pm 2^{\frac{n+1}{2}}\}$ but with $r \leq \frac{n}{3}$.
4. Derive constructions of APN/AB functions from perfect nonlinear functions, and *vice versa*.
5. Find classes of APN functions by using CCZ-equivalence with Kasami (resp. Welch, Niho, Dobbertin) functions.
6. Find classes of APN functions CCZ-inequivalent to power functions and to quadratic functions.
7. Find APN permutations with n even, or prove they cannot exist.
Observation: If APN permutations exist for n even, they are neither power functions, nor in $\mathbb{F}_{2^{n/2}}[x]$, nor plateaued.
8. Classify the extended Walsh spectra, or at least the nonlinearities, of APN functions.
Observations:
For n odd, the known APN functions have three possible spectra:

- the spectrum of the AB functions (e.g. the Gold functions) which gives a nonlinearity of $2^{n-1} - 2^{\frac{n-1}{2}}$,

- the spectrum of the inverse function[8], which takes any value divisible by 4 in $[-2^{n/2+1}+1; 2^{n/2+1}+1]$ and gives a nonlinearity close to $2^{n-1}-2^{n/2}$,
- the spectrum of the Dobbertin function which is more complex (it is divisible by $2^{n/5}$ and not divisible by $2^{2n/5+1}$); its nonlinearity seems equal to $2^{n-1}-2^{3n/5-1}-2^{2n/5-1}$.

For n even, the spectra may be more diverse:

- the Gold functions,
- the Dobbertin function,
- As soon as $n \geq 6$, we find (quadratic) functions with different spectra.

The nonlinearities seem also lower bounded by approximately $2^{n-1}-2^{3n/5-1}-2^{2n/5-1}$.
Open question: is this situation general to all APN functions or specific to the APN functions found so far?

Observation:

Proposition 16 *Let F be an APN function in $n > 2$ variables. For all real numbers a and b such that $a \leq b$, let $N_{a,b}$ be the number of ordered pairs $(u, v) \in F_2^n \times (F_2^n \setminus \{0\})$ such that $W_{v\cdot F}^2(u) \in]2^n+a; 2^n+b[$, where $W_{v\cdot F}(u) = \sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x}$. Then the nonlinearity of F is lower bounded by*

$$2^{n-1} - \frac{1}{2}\sqrt{2^n + \frac{1}{2}(b + a + \sqrt{\Delta_{a,b}})},$$

where $\Delta_{a,b} = (N_{a,b}+1)(b-a)^2 + a\,b\,2^{n+2}(2^n-1) + 2^{4n+2} - 2^{3n+2}$.

Proof: Relation (11) or (12) shows that for all real numbers a, b we have

$$\sum_{\substack{u\in F_2^n,\\ v\in F_2^n\setminus\{0\}}} (W_{v\cdot F}^2(u)-2^n-a)(W_{v\cdot F}^2(u)-2^n-b) = 2^{4n}-2^{3n}+a\,b\,2^n(2^n-1), \quad (14)$$

since $\sum_{u\in F_2^n, v\in F_2^n\setminus\{0\}}(W_{v\cdot F}^2(u) - 2^n) = 0$. Since the expression $(x-a)(x-b)$ takes its minimum at $x = \frac{b+a}{2}$ and this minimum is $-\frac{(b-a)^2}{4}$, we have $(W_{v\cdot F}^2(u) - 2^n - a)(W_{v\cdot F}^2(u) - 2^n - b) \geq -\frac{(b-a)^2}{4}$ for these $N_{a,b}$ ordered pairs

[8]Whose values are called Kloosterman sums.

and $(W^2_{v\cdot F}(u) - 2^n - a)(W^2_{v\cdot F}(u) - 2^n - b) \geq 0$ for all the others. Hence we have $-\frac{(b-a)^2}{4} \leq (W^2_{v\cdot F}(u) - 2^n - a)(W^2_{v\cdot F}(u) - 2^n - b) \leq 2^{4n} - 2^{3n} + a\,b\,2^n(2^n - 1) + N_{a,b}\frac{(b-a)^2}{4}$ for any $(u, v) \in F_2^n \times (F_2^n \setminus \{0\})$, that is, $(W^2_{v\cdot F}(u) - 2^n)^2 - (b + a)(W^2_{v\cdot F}(u) - 2^n) + ab - (2^{4n} - 2^{3n} + a\,b\,2^n(2^n - 1) + N_{a,b}\frac{(b-a)^2}{4}) \leq 0$, which implies

$$\frac{1}{2}(b + a - \sqrt{\Delta_{a,b}}) \leq W^2_{v\cdot F}(u) - 2^n \leq \frac{1}{2}(b + a + \sqrt{\Delta_{a,b}}),$$

where $\Delta_{a,b} = (b + a)^2 - 4(a\,b - 2^{4n} + 2^{3n} - a\,b\,2^n(2^n - 1) - N_{a,b}\frac{(b-a)^2}{4}) = (N_{a,b} + 1)(b - a)^2 + a\,b\,2^{n+2}(2^n - 1) + 2^{4n+2} - 2^{3n+2}$. This implies that the nonlinearity of F is lower bounded by

$$2^{n-1} - \frac{1}{2}\sqrt{2^n + \frac{1}{2}(b + a + \sqrt{\Delta_{a,b}})}.$$

□

Consequences:
- taking $b = -a = 2^n$, we see that if $W^2_{v\cdot F}(u)$ does not take values in the range $]0; 2^{n+1}[$, then F is AB (this was known).
- more generally, taking $a = -\frac{2^{2n}}{b}$, we see that if $W^2_{v\cdot F}(u)$ does not take values in the range $]2^n - \frac{2^{2n}}{b}; 2^n + b[$ for some b (which is necessarily greater than or equal to 2^n), the nonlinearity of F is lower bounded by $2^{n-1} - \frac{1}{2}\sqrt{2^n + b}$.

As observed by G. Leander (private communication), if F is an APN power function, then in the case where n is odd it is a bijection and thus all functions $v \cdot F$ have the same Walsh spectrum. Thus we have

$$\max_{v\neq 0,u} W^4_{v\cdot F}(u) \leq \frac{\sum_{v\neq 0,u} W^4_{v\cdot F}(u)}{2^n - 1} = 2^{3n+1}.$$

Thus

$$max_{v\neq 0,u}|W_{v\cdot F}(u) \leq 2^{3/4n+1/4}.$$

In the even case we have that not all the functions $v \cdot F$ are the same, but they are divided in two classes. Thus we get something similar there.

A first attempt to study the behavior of highly nonlinear S-boxes with respect to Differential Power Attacks can be found in [99].

3.2 Nonlinearity of S-boxes in stream ciphers

The notion of nonlinearity given in Definition 1 for block ciphers is not relevant to those S-boxes used in the pseudo-random generators of stream ciphers. Indeed, in the case of block ciphers, due to their iterative structure, the knowledge of a nonlinear combination of the outputs to F with a low nonlinearity does not necessarily lead to an attack, unless (at the least) its degree is very low. On the contrary, since the structure of the pseudo-random generators using combining or filtering functions is not iterative, all of the m binary sequences produced by an (n, m)-function can be combined by a linear or nonlinear (but non-constant) m-variable Boolean function g to perform correlation attacks. Consequently, a second generalization to (n, m)-functions of the notion of nonlinearity has been introduced (in [41], but the definition was based on the observations of Zhang and Chan in [111]).

Definition 6 *Let F be an (n, m)-function. The* unrestricted nonlinearity *$U\mathcal{NL}(F)$ of F is the minimum Hamming distance between all non-constant affine functions and all Boolean functions $g \circ F$, where g is any non-constant Boolean function on m variables.*

If $U\mathcal{NL}(F)$ is small, then one of the linear or nonlinear (non-constant) combinations of the output bits to F has high correlation to a non constant affine function of the input, and a correlation attack is feasible.

Remark.
1. In Definition 6, the considered affine functions are non-constant, because the minimum distance between all Boolean functions $g \circ F$ (g non-constant) and all constant functions equals $\min_{b \in \mathbb{F}_2^m} |F^{-1}(b)|$ (each number $|F^{-1}(b)|$ is indeed equal to the distance between the null function and $g \circ F$, where g equals the indicator of the singleton $\{b\}$); it is therefore an indicator of the balancedness of F. It is upper bounded by 2^{n-m} (and it equals 2^{n-m} if and only if F is balanced), since the mean of $|F^{-1}(b)|$ is equal to 2^{n-m}. If we did not restrict ourselves to non-constant affine functions, $U\mathcal{NL}(F)$ would equal most often $\min_{b \in \mathbb{F}_2^m} |F^{-1}(b)|$ and would have no real relationship with correlation attacks.
2. We can replace "non constant affine functions" by "nonzero linear functions" in the statement of Definition 6 (replacing g by $g \oplus 1$, if necessary).
3. Thanks to the fact that the affine functions considered in Definition 6 are non-constant, *we can relax the condition that g is non-constant*: the distance between a constant function and a non-constant affine function equals 2^{n-1},

and $U\mathcal{NL}(F)$ is clearly always smaller than 2^{n-1}.

The unrestricted nonlinearity of any (n,m)-function F is obviously unchanged when F is right-composed with an affine invertible mapping. Moreover, if A is a surjective linear (or affine) function from $\mathbb{F}_2^p$ (where p is some positive integer) into $\mathbb{F}_2^n$, then it is easily shown that $U\mathcal{NL}(F \circ A) = 2^{p-n}U\mathcal{NL}(F)$. Also, for every (m,p)-function ϕ, we have $U\mathcal{NL}(\phi \circ F) \geq U\mathcal{NL}(F)$ (indeed, the set $\{g \circ \phi,\ g \in \mathcal{BF}_p\}$, where $\mathcal{BF}_p$ is the set of p-variable Boolean functions, is included in $\mathcal{BF}_m$), and if ϕ is a permutation on $\mathbb{F}_2^m$, then we have $U\mathcal{NL}(\phi \circ F) = U\mathcal{NL}(F)$ (by applying the inequality above to $\phi^{-1} \circ F$).

A further generalization of this attack, called the *generalized correlation attack* has been introduced recently in [39]: considering implicit equations which are linear in the input variable x and of any degree in the output variable $z = F(x)$, the following probability is considered, for any nonconstant function g:

$$Pr(g(z) + w_1(z)x_1 + w_2(z)x_2 + \cdots + w_n(z)x_n = 0), \tag{15}$$

where $z = F(x)$, $w_i : \mathbb{F}_2^m \to \mathbb{F}_2$ and x uniformly ranges over $\mathbb{F}_2^n$.
The knowledge of such approximation g with a probability significantly higher than $1/2$ leads to an attack, because $z = F(x)$ corresponding to the output keystream which is known, $g(z)$ and $w_i(z)$ are known for all $i = 1, \ldots, n$.
This led to a new notion of generalized nonlinearity:

Definition 7 *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$. The* generalized Hadamard transform *$\hat{F} : (\mathbb{F}_2^{2^m})^{n+1} \to \mathbb{R}$ is defined as:*

$$\hat{F}(g(\cdot), w_1(\cdot), \ldots, w_n(\cdot)) = \sum_{x \in \mathbb{F}_2^n} (-1)^{g(F(x)) + w_1(F(x))x_1 + \cdots w_n(F(x))x_n},$$

where the input is an $(n+1)$-tuple of Boolean functions $g, w_i : \mathbb{F}_2^m \to \mathbb{F}_2$, $i = 1, \ldots, n$.
Let $\mathcal{W}$ be the set of all n-tuple functions $w(\cdot) = (w_1(\cdot), \ldots, w_n(\cdot))$, where w_i is an m-variable Boolean function and such that $w(z) = (w_1(z), \ldots, w_n(z)) \neq (0, \ldots, 0)$ for all $z \in \mathbb{F}_2^m$.
The generalized nonlinearity *is defined as:*

$$GN_F = \min\{\min_{0 \neq u \in \mathbb{F}_2^m}(wt(u \cdot F), 2^n - wt(u \cdot F)), nonlin_{gen}F\},$$

where

$$nonlin_{gen}F = 2^{n-1} - \frac{1}{2} \max_{g\in\mathcal{G}, w\in\mathcal{W}} \hat{F}(g(\cdot), w_1(\cdot), \ldots, w_n(\cdot)). \qquad (16)$$

The generalized nonlinearity is clearly not greater than the other nonlinearity measures and thus provides linear approximations with better bias for correlation attack.

3.2.1 Relations to the Fourier/Walsh transforms and lower bounds

The unrestricted nonlinearity of F can be related to the values of the discrete Fourier transforms of the functions φ_b, and a lower bound (observed in [111]) depending on $\mathcal{NL}(F)$ can be directly deduced:

Proposition 17 *For every (n,m)-function, we have*

$$U\mathcal{NL}(F) = 2^{n-1} - \frac{1}{2} \max_{u\in\mathbb{F}_2^{n*}} \sum_{b\in\mathbb{F}_2^m} |\widehat{\varphi_b}(u)|\,, \qquad (17)$$

and:

$$U\mathcal{NL}(F) \geq 2^{n-1} - 2^{m/2}\left(2^{n-1} - \mathcal{NL}(F)\right). \qquad (18)$$

Relation (17) allows to prove that any non-constant affine function A from $\mathbb{F}_2^n$ into $\mathbb{F}_2^m$ has null unrestricted nonlinearity[9]: we assume without loss of generality that A is linear; let E be a vectorspace whose direct sum with its kernel $Ker\ A$ equals $\mathbb{F}_2^n$. For every $b \in Im\ A$, there exists a unique vector $a \in E$ such that $A^{-1}(b) = a + Ker\ A$. We deduce that, for every $u \in \mathbb{F}_2^n$, the sum $\sum_{b\in\mathbb{F}_2^m} |\widehat{\varphi_b}(u)| = \sum_{b\in\mathbb{F}_2^m} |\sum_{x\in A^{-1}(b)}(-1)^{u\cdot x}|$ equals $2^{\dim(ImA)} \left|\sum_{x\in Ker\ A}(-1)^{u\cdot x}\right|$. Since A is nonzero, $Ker\ A$ has dimension at most $n-1$, and there exists $u \in \mathbb{F}_2^{n*}$, such that $Ker\ A \subseteq u^{\perp}$; hence $U\mathcal{NL}(A) \leq 2^{n-1} - \frac{1}{2}\cdot 2^{\dim(Im\ A)+\dim(Ker\ A)} = 0$.
This implies that, for every non-constant affine (n,m)-function A and for every permutation ϕ on $\mathbb{F}_2^m$, the unrestricted nonlinearity of the (n,m)-function $\phi \circ A$ is null.
If A is constant, the result is no more true, but there is no need to consider its unrestricted nonlinearity, since it has no cryptographic interest.

We shall see that the lower bound (18) is far from giving a good idea of the best possible unrestricted nonlinearities: even if $\mathcal{NL}(F)$ is close to the

[9] If A is surjective (that is, balanced) then this can be directly deduced from Inequality (19) below.

nonlinearity of bent functions, that is $2^{n-1}-2^{n/2-1}$, it implies that $U\mathcal{NL}(F)$ is approximately greater than $2^{n-1}-2^{\frac{n+m}{2}-1}$, whereas we shall construct a balanced $(n, n/2)$-function F such that $U\mathcal{NL}(F) = 2^{n-1} - 2^{n/2}$.

Proposition 18 *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ and let $w(\cdot)$ denote the n-tuple of m-bit Boolean functions $(w_1(\cdot), \ldots, w_n(\cdot))$. Then*

$$nonlin_{gen}F = 2^{n-1} - 1/2 \sum_{z \in \mathbb{F}_2^m} \max_{w(z) \in \mathbb{F}_2^n - \{0\}} |\widehat{\varphi_b}(w(z))| .$$

Corollary 1

$$nonlin_{gen}F = 2^{n-1} - \frac{1}{2^{m+1}} \sum_{z \in GF(2)^m} \max_{\substack{0 \neq w(z) \in \\ GF(2)^n}} \left| \sum_{v \in GF(2)^m} (-1)^{v \cdot z} \widehat{(v \cdot F)}_\chi(w(z)) \right|,$$

where $\widehat{(v \cdot F)}_\chi$ denotes the Walsh transform of the Boolean function $v \cdot F$. Hence

$$GN_F \geq 2^{n-1} - (2^m - 1) \left(2^{n-1} - \mathcal{NL}(F)\right).$$

3.2.2 Upper bounds

To have a better evaluation of what can be a good unrestricted nonlinearity, we need upper bounds. Recall that $\mathcal{NL}(F)$ is the minimum Hamming distance between all Boolean functions $g \circ F$ where g is any nonzero linear function, and all affine functions (including the constant ones). Note that, if F is balanced, this minimum distance can not be achieved with constant affine functions, because $g \circ F$, which is then a Boolean balanced function, has distance 2^{n-1} to constant functions. Hence:

Proposition 19 (covering radius bound) *For every balanced S-box F, we have:*

$$U\mathcal{NL}(F) \leq \mathcal{NL}(F). \tag{19}$$

This implies $U\mathcal{NL}(F) \leq 2^{n-1} - 2^{n/2-1}$.

Another upper bound:

$$U\mathcal{NL}(F) \leq 2^{n-1} - \frac{1}{2}\left(\frac{2^{2m} - 2^m}{2^n - 1} + \sqrt{\frac{2^{2n} - 2^{2n-m}}{2^n - 1} + \left(\frac{2^{2m} - 2^m}{2^n - 1} - 1\right)^2} - 1 \right)$$

has been obtained in [41]. It improves upon the covering radius bound only for $m \geq n/2 + 1$, and the question of knowing whether it is possible

to improve upon the covering radius bound for $m \leq n/2$ is open. In any case, this improvement will not be dramatic, at least for $m = n/2$, since it is shown (by using Relation (17)) in this same paper that the balanced function $F(x,y) = \begin{cases} \frac{x}{y} & \text{if } y \neq 0 \\ x & \text{if } y = 0 \end{cases}$ satisfies $U\mathcal{NL}(F) = 2^{n-1} - 2^{n/2}$ (see other examples of S-boxes in [81], whose unrestricted nonlinearities seem low, however). It is pretty astonishing that an S-box with such high unrestricted nonlinearity exists; but it can be shown that this balanced function does not contribute to a good resistance to algebraic attacks (it is not resilient either, but this is not a problem if it is used as a filtering function).

Proposition 20 *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$. Then the following inequality holds.*

$$nonlin_{gen}F \leq 2^{n-1} - \frac{1}{4} \sum_{z \in \mathbb{F}_2^m} \sqrt{\frac{2^{n+2}|F^{-1}(z)| - 4|F^{-1}(z)|^2}{2^n - 1}}.$$

Furthermore if $F(x)$ is balanced, then we have:

$$GN_F \leq 2^{n-1} - 2^{n-1}\sqrt{\frac{2^m - 1}{2^n - 1}}$$

This upper bound is much lower than the covering radius bound $2^{n-1} - 2^{n/2-1}$ and the upper bound for UN_F.

It is proved in [40] that the balanced function $F(x,y) = \begin{cases} \frac{x}{y} & \text{if } y \neq 0 \\ x & \text{if } y = 0 \end{cases}$ has null generalized nonlinearity. Hence, a vectorial function may have very high unrestricted nonlinearity and have zero generalized nonlinearity. Some functions with good generalized nonlinearity are given in [40]:

1. $F(x) = Tr_m^n(x^k)$ where $k = 2^r + 1$, $\gcd(r,n) = 1$
2. $F(x) = Tr_m^n(x^k)$ where $k = 2^{2r} - 2^r + 1$, $3r \equiv 1 \pmod{n}$,

where m divides n and n is odd, and where Tr_m^n is the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$, have generalized nonlinearity satisfying $GN_F \geq 2^{n-1} - 2^{(n-1)/2+m-1}$.

4 Resilient functions

Resilient Boolean functions have been studied in the chapter "Boolean Functions for Cryptography and Error Correcting Codes". The notion, when

extended to vectorial functions, is relevant, in cryptology, to quantum cryptographic key distribution [2] and to pseudo-random sequence generation for stream ciphers.

Definition 8 *Let n and m be two positive integers. Let t be an integer such that $0 \leq t \leq n$. An (n,m)-function $F(x)$ is called t-th order* correlation-immune *if its output distribution does not change when at most t coordinates x_i of x are kept constant. It is called t-*resilient *if it is balanced and t-th order correlation-immune, that is if it stays balanced when at most t coordinates x_i of x are kept constant*

This notion has a relationship with another notion which plays also a role in cryptography: an (n,m)-function F is called a *multipermutation* (see [106]) if any two ordered pairs $(x, F(x))$ and $(x', F(x'))$, $x \neq x' \in \mathbb{F}_2^n$, differ on at least $m+1$ distinct positions; such (n,m)-function ensures then a perfect diffusion; an (n,m)-function is a multipermutation if and only if the indicator of its graph $\{(x, F(x));\, x \in \mathbb{F}_2^n\}$ is an n-th order correlation-immune Boolean function (see [22]).
Since S-boxes must be balanced, we shall focus on resilient functions, but most of the results below can also be stated for correlation-immune functions.
We call an (n,m) function which is t-resilient an (n,m,t)-function. Clearly, if such a function exists, then $m \leq n-t$ (*i.e.* $t \leq n-m$), since balanced (n,m)-functions can exist only if $m \leq n$. This bound is weak (it is tight if and only if $m=1$ or $t=1$). It is shown in [47] (see also [6]) that, if an (n,m,t)-function exists, then $m \leq n - \log_2 \left[\sum_{i=0}^{t/2} \binom{n}{i}\right]$ if t is even and $m \leq n - \log_2 \left[\binom{n-1}{(t-1)/2} + \sum_{i=0}^{(t-1)/2} \binom{n}{i}\right]$ if t is odd. This can be deduced from a classical bound on orthogonal arrays, due to Rao [100]. But, as shown in [6] (see also [88]), potentially better bounds can be deduced from the linear programming bound due to Delsarte [51]: $t \leq \left\lfloor \frac{2^{m-1}n}{2^m-1} \right\rfloor - 1$ and $t \leq 2\left\lfloor \frac{2^{m-2}(n+1)}{2^m-1} \right\rfloor - 1$.
Note that composing a t-resilient (n,m)-function by a permutation on $\mathbb{F}_2^m$ does not change its resiliency order (this obvious result was first observed in [109]). Also, the t-resiliency of S-boxes can be expressed by means of the t-resiliency of Boolean functions:

Proposition 21 *Let F be an (n,m) function. Then F is t-resilient if and only if one of the following conditions is satisfied :*
1. for every nonzero vector $v \in \mathbb{F}_2^m$, the Boolean function $v \cdot F(x)$ is t-resilient,

2. for every balanced m-variable Boolean function g, the n-variable Boolean function $g \circ F$ is t-resilient.

Equivalently, F is t-resilient if and only if, for every vector $u \in \mathbb{F}_2^n$ such that $w_H(u) \leq t$, one of the following conditions is satisfied :
(i). $\sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot F(x) + u \cdot x} = 0$, for every $v \in \mathbb{F}_2^{m*}$,
(ii). $\sum_{x \in \mathbb{F}_2^n} (-1)^{g(F(x)) + u \cdot x} = 0$, for every balanced m-variable Boolean function g.

Finally, F is t-resilient if and only if, for every vector $b \in \mathbb{F}_2^m$, the Boolean function φ_b is t-th order correlation-immune and has weight 2^{n-m}.

Proof. According to the characterization recalled in the previous chapter, at Proposition 12, Condition 1 (resp. Condition 2) is equivalent to the fact that Condition (i) (resp. Condition (ii)) is satisfied for every vector $u \in \mathbb{F}_2^n$ such that $w_H(u) \leq t$.
Let us prove now that the t-resiliency of F implies Condition 2, which implies Condition 1, which implies that, for every vector $b \in \mathbb{F}_2^m$, the Boolean function φ_b is t-th order correlation-immune and has weight 2^{n-m}, which implies that F is t-resilient. If F is t-resilient, then, for every balanced m-variable Boolean function g, the function $g \circ F$ is t-resilient, by definition; hence Condition 2 is satisfied; this clearly implies Condition 1, since the function $g(x) = v \cdot x$ is balanced for every nonzero vector v. Relation (3) implies then that, for every vector $u \in \mathbb{F}_2^n$ such that $w_H(u) \leq t$ and for every $b \in \mathbb{F}_2^m$, we have $\widehat{\varphi_b}(u) = 2^{-m} \sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot (F(x)+b) + u \cdot x} = 0$. Hence, Condition 1 implies that φ_b is t-th order correlation-immune for every b. Also, according to Proposition 1, Condition 1 implies that F is balanced, *i.e.* φ_b has weight 2^{n-m}, for every b. These two conditions obviously imply, by definition, that F is t-resilient. ◇

Consequently, the t-resiliency of vectorial functions is invariant under the same transformations as for Boolean functions.

4.1 Constructions

4.1.1 Linear or affine resilient functions

The construction of t-resilient linear functions is easy: Bennett et al. [2] and Chor et al. [47] established the connection between linear resilient functions and linear codes (correlation-immune functions being related to orthogonal arrays, see [24, 23], we should in fact refer to Delsarte [52] for this relationship). There exists a linear (n, m, t)-function if and only if there exists a linear $[n, m, t+1]$ code.

Proposition 22 *Let G be a generating matrix for an $[n, k, d]$ linear code C. Define $L : \mathbb{F}_2^n \mapsto \mathbb{F}_2^k$ by the rule $L(x) = x \times G^T$, where G^T is the transpose of G. Then L is an $(n, k, d-1)$-function.*

Indeed, for every nonzero $v \in \mathbb{F}_2^m$, the vector $v \cdot L(x) = v \cdot (x \times G^t)$ has the form $x \cdot u$ where $u = v \times G$ is a nonzero element of C. Hence, u having weight at least d, the linear function $v \cdot L$ is $(d-1)$-resilient, since it has at least d independent terms of degree 1 in its ANF.
The converse of Proposition 22 is clearly also true.
Proposition 22 is still trivially true if L is affine instead of linear, that is $L(x) = x \times G^t + a$, where a is a vector of $\mathbb{F}_2^k$.
Stinson [103] considered the equivalence between resilient functions and what he called large sets of orthogonal arrays. According to Proposition 21, an (n, m)-function is t-resilient if and only if there exists a set of 2^m disjoint binary arrays of dimensions $2^{n-m} \times n$, such that, in any t columns of each array, every one of the 2^t elements of $\mathbb{F}_2^t$ occurs in exaclty 2^{n-m-t} rows and no two rows are identical.
The construction of t-resilient functions by Proposition 22 can be generalized by considering nonlinear codes of length n (that is subsets of $\mathbb{F}_2^n$) whose dual distance $d^\perp$ is greater than or equal to $t+1$ (see [104]). As recalled in the chapter "Boolean Functions for Cryptography and Error Correcting Codes", the *dual distance of a code* C of length n is the smallest nonzero integer i such that the coefficient of the monomial $X^{n-i}Y^i$ in the polynomial $\sum_{x,y \in C}(X+Y)^{n-w_H(x+y)}(X-Y)^{w_H(x+y)}$ is nonzero (when the code is linear, the dual distance is equal to the minimum Hamming distance of the dual code, according to MacWilliams' identity). The nonlinear code needs also to be *systematic* (that is, that there exists a subset I of $\{1, \cdots, n\}$ called an *information set* of C, such that every possible tuple occurs in exactly one codeword within the specified coordinates x_i; $i \in I$) to allow the construction of a $(d^\perp - 1)$-resilient function. It is deduced in [104] that, for every $r \geq 3$, a $(2^{r+1}, 2^{r+1} - 2r - 2, 5)$-resilient function exists (the construction is based on the Kerdock code), and that no affine resilient function with these parameters exists.

4.1.2 Maiorana-MacFarland resilient functions

The idea of designing resilient vectorial functions by generalizing the Maiorana-MacFarland construction is natural. One can find a first reference of such construction in a paper by Nyberg [92], but for generating perfect nonlinear functions. This technique has been used by Kurosawa et al. [83],

Johansson and Pasalic [78], Pasalic and Maitra [98] and Gupta and Sarkar [68] to produce functions having high resiliency and high nonlinearity[10].

Definition 9 *The class of* Maiorana-McFarland (n, m)*-functions is the set of those functions* F *which can be written in the form:*

$$F(x, y) = x \times \begin{pmatrix} \varphi_{11}(y) & \cdots & \varphi_{1m}(y) \\ \vdots & \ddots & \vdots \\ \varphi_{r1}(y) & \cdots & \varphi_{rm}(y) \end{pmatrix} + H(y),\ (x, y) \in \mathbb{F}_2^r \times \mathbb{F}_2^s \quad (20)$$

where r *and* s *are two integers satisfying* $r+s = n$*,* H *is any* (s, m)*-function and, for every index* $i \leq r$ *and every index* $j \leq m$*,* φ_{ij} *is a Boolean function on* $\mathbb{F}_2^s$*.*

The concatenation of t-resilient functions being still t-resilient, if the transpose matrix of the matrix involved in Equation (20) is the generator matrix of a linear $[r, m, d]$-code for every vector y ranging over $\mathbb{F}_2^s$, then the (n, m)-function F is $(d-1)$-resilient.

Any Maiorana-McFarland's (n, m)-function F can be written in the form:

$$F(x, y) = \left(\bigoplus_{i=1}^{r} x_i \varphi_{i1}(y) \oplus h_1(y), \ldots, \bigoplus_{i=1}^{r} x_i \varphi_{im}(y) \oplus h_m(y) \right) \quad (21)$$

where $H = (h_1, ..., h_m)$.

After denoting, for every $i \leq m$, by ϕ_i the (s, r)-function which admits the Boolean functions φ_{1i}, ..., φ_{ri} for coordinate functions, we can rewrite Relation (21) as :

$$F(x, y) = \left(x \cdot \phi_1(y) \oplus h_1(y), \ldots, x \cdot \phi_m(y) \oplus h_m(y) \right). \quad (22)$$

- Resiliency: As a direct consequence of Proposition 22, we have (equivalently to what is written above in terms of codes):

Proposition 23 *Let* n*,* m*,* r *and* s *be three integers such that* $n = r + s$*. Let* F *be a Maiorana-McFarland's* (n, m)*-function defined as in Relation (22) and such that, for every* $y \in \mathbb{F}_2^s$*, the family* $(\phi_i(y))_{i \leq m}$ *is a basis of an* m*-dimensional subspace of* $\mathbb{F}_2^r$ *having* $t + 1$ *for minimum Hamming weight, then* F *is at least* t*-resilient.*

[10] But, as recalled at Section 3.2, this notion of nonlinearity is not relevant to S-boxes for stream ciphers. The unrestricted nonlinearity of resilient functions and of Maiorana-MacFarland functions has to be further studied.

- Nonlinearity: According to the known facts about the Walsh transform of the Boolean Maiorana-MacFarland functions, the nonlinearity $\mathcal{NL}(F)$ of any Maiorana-McFarland's (n,m)-function defined as in Relation (22) satisfies

$$\mathcal{NL}(F) = 2^{n-1} - 2^{r-1} \max_{(u,u') \in \mathbb{F}_2^r \times \mathbb{F}_2^s, v \in \mathbb{F}_2^{m*}} \left| \sum_{y \in E_{u,v}} (-1)^{v \cdot H(y) + u' \cdot y} \right| \tag{23}$$

where $E_{u,v}$ denotes the set $\{y \in \mathbb{F}_2^s;\ \sum_{i=1}^m v_i \phi_i(y) = u\}$.
The bounds proved in the chapter "Boolean Functions for Cryptography and Error Correcting Codes", Subsection 7.3.1, for the nonlinearities of Maiorana-McFarland's Boolean functions imply that the nonlinearity $\mathcal{NL}(F)$ of a Maiorana-McFarland's (n,m)-function defined as in Relation (22) satisfies

$$2^{n-1} - 2^{r-1} \max_{u \in \mathbb{F}_2^r, v \in \mathbb{F}_2^{m*}} |E_{u,v}| \leq \mathcal{NL}(F) \leq 2^{n-1} - 2^{r-1} \left\lceil \sqrt{\max_{u \in \mathbb{F}_2^r, v \in \mathbb{F}_2^{m*}} |E_{u,v}|} \right\rceil .$$

If, for every element y, the vectorspace spanned by the vectors $\phi_1(y)$, ..., $\phi_m(y)$ admits m for dimension and has a minimum Hamming weight strictly greater than k (so that F is t-resilient with $t \geq k$), then we have

$$\mathcal{NL}(F) \leq 2^{n-1} - 2^{r-1} \left\lceil \frac{2^{s/2}}{\sqrt{\sum_{i=k+1}^r \binom{r}{i}}} \right\rceil . \tag{24}$$

The nonlinearity can be exactly calculated in two situations (at least): if, for every vector $v \in \mathbb{F}_2^{m*}$, the (s,r)-function $y \mapsto \sum_{i \leq m} v_i \phi_i(y)$ is injective, then F admits $2^{n-1} - 2^{r-1}$ for nonlinearity; and if, for every vector $v \in \mathbb{F}_2^{m*}$, this same function takes exactly two times each value of its image set, then F admits $2^{n-1} - 2^r$ for nonlinearity.
Johansson and Pasalic described in [78] a way to specify the vectorial functions ϕ_1, ..., ϕ_m so that this kind of condition is satisfied. Their result can be generalized in the following form:

Lemma 1 *Let C be a binary linear $[r, m, t+1]$ code. Let $\beta_1, \ldots, \beta_m$ be a basis of the $\mathbb{F}_2$-vectorspace $\mathbb{F}_{2^m}$, and let L_0 be a linear isomorphism between $\mathbb{F}_{2^m}$ and C. Then the functions $L_i(z) = L_0(\beta_i z)$, $i = 1, \ldots, m$, have the property that, for every vector $v \in \mathbb{F}_2^{m*}$, the function $z \in \mathbb{F}_{2^m} \mapsto \sum_{i=1}^m v_i L_i(z)$ is a bijection from $\mathbb{F}_{2^m}$ into C.*

Proof. For every vector v in $\mathbb{F}_2^m$ and every element z of $\mathbb{F}_{2^m}$, we have $\sum_{i=1}^m v_i L_i(z) = L_0\left((\sum_{i=1}^m v_i\beta_i)z\right)$. If the vector v is nonzero, then the element $\sum_{i=1}^m v_i\beta_i$ is nonzero. Hence, the function $z \in \mathbb{F}_{2^m} \mapsto \sum_{i=1}^m v_i L_i(z)$ is a bijection. $\diamond$

Since the functions $L_1, L_2, \cdots, L_m$ vanish at $(0, \ldots, 0)$, they do not satisfy the hypothesis of Proposition 23 (i.e. the vectors $L_1(z)$, ..., $L_m(z)$ are not linearly independent for every $z \in \mathbb{F}_{2^m}$). A solution to derive a family of vectorial functions also satisfying the hypothesis of Proposition 23 is then to right-compose the functions L_i with a same injective (or two-to-one) function π from $\mathbb{F}_2^s$ into $\mathbb{F}_{2^m}^*$. Then, for every nonzero vector $v \in \mathbb{F}_2^{m*}$, the function $y \in \mathbb{F}_2^s \mapsto \sum_{i=1}^m v_i L_i[\pi(y)]$ is injective from $\mathbb{F}_2^s$ into C^*.
This gives the following construction[11]:
Given two integers m and r ($m < r$), construct an $[r, m, t+1]$-code C such that t is as large as possible (Brouwer gives in [11] a precise overview of the best known parameters of codes). Then, define m linear functions L_1, ..., L_m from $\mathbb{F}_{2^m}$ into C as in Lemma 1. Choose an integer s strictly lower than m (resp. lower than or equal to m) and define an injective (resp. two-to-one) function π from $\mathbb{F}_2^s$ into $\mathbb{F}_{2^m}^*$. Choose any (s, m)-function $H = (h_1, \ldots, h_m)$ and denote $r + s$ by n. Then the (n, m)-function F whose coordinate functions are defined by $f_i(x, y) = x \cdot [L_i \circ \pi](y) \oplus h_i(y)$ is t-resilient and admits $2^{n-1} - 2^{r-1}$ (resp. $2^{n-1} - 2^r$) for nonlinearity.
All the primary constructions presented in [78, 83, 98, 93] are based on this principle. Also, the recent construction of (n, m, t)-functions defined by Gupta and Sarkar in [68] is also a particular application of this construction, as shown in [42].

4.1.3 Other constructions

Constructions of highly nonlinear resilient vectorial functions, respectively based on elliptic curves theory and on the trace of some power functions $x \mapsto x^d$ on finite fields, have been designed respectively by Cheon [46] and by Khoo, Gong and Nyberg [82, 92, 93, 94]. However, it is still an open problem to design highly nonlinear functions with high algebraic degrees and high resiliency orders with Cheon's method. On the other hand, the

[11] Another construction based on Lemma 1 is given by Johansson and Pasalic in [78]. It involves a family of *nonintersecting codes*, that is a family of codes having the same parameters (same length, same dimension and same minimum distance) and whose pairwise intersections are reduced to the null vector. However, this construction is often worse for large resiliency orders, as shown in [42].

number of functions which can be designed by these methods are very small. Zhang and Zheng proposed in [109, 110] a secondary construction consisting in the composition $F = G \circ L$ of a linear resilient (n, m, t)-function L with a highly nonlinear (m, k)-function. F is obviously t-resilient, admits $2^{n-m}\mathcal{NL}(G)$ for nonlinearity where $\mathcal{NL}(G)$ denotes the nonlinearity of G and its degree is the same as that of G. Taking for function G the inverse function $x \mapsto x^{-1}$ on the finite Field $\mathbb{F}_{2^m}$ studied by Nyberg in [94] (and later used for designing the S-boxes of the AES), Zhang and Zheng obtained t-resilient functions having a nonlinearity larger than or equal to $2^{n-1}-2^{n-m/2}$ and having $m-1$ for algebraic degree. But the linear (n, m)-functions involved in the construction of Zhang and Zheng introduce a weakness: their *unrestricted nonlinearity* being null, this kind of functions can not be used as a multi-output combination function in stream ciphers. Nevertheless, this drawback can be avoided by concatenating such functions (recall that the concatenation of t-resilient functions gives t-resilient functions, and a good nonlinearity can be obtained by concatenating functions with disjoint Walsh supports). We obtain this way a modified Maiorana-McFarland's construction, that should be investigated.

Other secondary constructions of resilient vectorial functions can be derived from the secondary constructions of resilient Boolean functions. (see *e.g.* [23, 35]).

Acknowledgement

We thank Anne Canteaut and Lilya Budaghyan for useful comments and Caroline Fontaine for her careful reading of a previous draft of this chapter.

References

[1] F. Armknecht and M. Krause. Constructing single- and multi-output boolean functions with maximal immunity. Proceedings of *ICALP 2006*, Lecture Notes of Computer Science 4052, Springer, pp. 180-191, 2006.

[2] C. H. Bennett, G. Brassard and J. M. Robert. Privacy amplification by public discassion. *SIAM J. Computing 17*, pp. 210-229, 1988.

[3] T. Bending and D. Fon-Der-Flass. Crooked functions, bent functions and distance regular graphs. *Electron. J. Comb.* 5 (R. 34), 14, 1998.

[4] T. Berger, A. Canteaut, P. Charpin and Y. Laigle-Chapuy. On almost perfect nonlinear functions. *IEEE Trans. Inform. Theory*, pp. 4160-4170, 2006.

[5] T. Beth and C. Ding, On almost perfect nonlinear permutations. *Advances in Cryptology – Eurocrypt' 93, Lecture Notes in Computer Science*, 765, New York, Springer-Verlag, pp. 65-76, 1994.

[6] J. Bierbrauer, K. Gopalakrishnan and D.R. Stinson. Orthogonal arrays, resilient functions, error-correcting codes, and linear programming bounds. *SIAM J. Discrete Math.*, Vol. 9, No. 3, pp. 424-452, 1996.

[7] E. Biham and A. Shamir. Differential Cryptanalysis of DES-like Cryptosystems. *Journal of Cryptology*, Vol 4, No.1, pp. 3-72, 1991.

[8] C. Bracken, E. Byrne, N. Markin and G. McGuire. On the Extended Walsh Spectrum of a New APN Function. IMA conference on Cryptography and Coding , Cirencester, England, December 2007. To appear, 2007.

[9] C. Bracken, E. Byrne, N. Markin and G. McGuire. New families of quadratic almost perfect nonlinear trinomials and multinomials. To appear in FFA, 2007.

[10] C. Bracken, E. Byrne, N. Markin and G. McGuire. Determining the Nonlinearity of a New Family of APN Functions. AAECC-17 Conference, Bangalore, India, December 2007. To appear, 2007.

[11] A.E. Brouwer, Bounds on the minimum distance of linear codes (Table of the best known codes). URL: http://www.win.tue.nl/ aeb/voorlincod.html.

[12] K. Browning, J. F. Dillon, R. E. Kibler and M. McQuistan. APN polynomials and related codes. Preprint, 2006.

[13] L. Budaghyan, C. Carlet and A. Pott. New Classes of Almost Bent and Almost Perfect Nonlinear Polynomials. Proceedings of the Workshop on Coding and Cryptography 2005, Bergen, pp. 306-315, 2005.

[14] L. Budaghyan, C. Carlet, P. Felke and G. Leander. An infinite class of quadratic APN functions which are not equivalent to power functions. Proceedings of IEEE International Symposium on Information Theory (ISIT) 2006.

[15] L. Budaghyan, C. Carlet and G. Leander. Two classes of quadratic APN binomials inequivalent to power functions. To appear in IEEE Trans. Inf. Th., 2008.

[16] L. Budaghyan, C. Carlet and G. Leander. On inequivalence between known power APN functions. Proceedings of the conference BFCA 2008, Copenhagen.

[17] L. Budaghyan, C. Carlet and G. Leander. Another class of quadratic APN binomials over F_{2^n}: the case n divisible by 4. Workshop on Coding and Cryptography, pp. 49-58, 2007.

[18] L. Budaghyan, C. Carlet and G. Leander. Constructing new APN functions from known ones. To appear in Finite Fields and Applications, 2008.

[19] L. Budaghyan and C. Carlet. Classes of Quadratic APN Trinomials and Hexanomials and Related Structures. To appear in *IEEE Trans. Inform. Theory*, 2007.

[20] E. Byrne and G. McGuire. On the non-existence of crooked functions on finite fields. *Proceedings of the Workshop on Coding and Cryptography* 2005, Bergen, pp. 316-324, 2005.

[21] P. Camion and A. Canteaut. Construction of t-resilient functions over a finite alphabet, *Advances in Cryptology, EUROCRYPT'96, Lecture Notes in Computer Sciences, Springer Verlag* no. 1070, pp. 283-293, 1996.

[22] P. Camion and A. Canteaut. Generalization of Siegenthaler inequality and Schnorr-Vaudenay multipermutations. *Advances in Cryptology - CRYPTO'96*, Lecture Notes in Computer Science no. 1109, pp. 372–386 Springer-Verlag, 1996.

[23] P. Camion and A. Canteaut. Correlation-immune and resilient functions over finite alphabets and their applications in cryptography. *Designs, Codes and Cryptography* 16, pp. 121-149, 1999.

[24] P. Camion, C. Carlet, P. Charpin, N. Sendrier. On correlation-immune functions, *Advances in Cryptology: Crypto '91, Proceedings, Lecture Notes in Computer Science*, vol. 576, pp. 86-100, 1991.

[25] A. Canteaut. Differential cryptanalysis of Feistel ciphers and differentially uniform mappings . *Selected Areas on Cryptography, SAC'97*, pp. 172-184, Ottawa, Canada, 1997.

[26] A. Canteaut. Cryptographic functions and design criteria for block ciphers. *Progress in Cryptology - INDOCRYPT 2001, Lecture Notes in Computer Science* 2247, pp. 1-16. Springer-Verlag, 2001.

[27] A. Canteaut. Analysis and design of symmetric ciphers. Habilitation for directing Theses, University of Paris 6, 2006.

[28] A. Canteaut, P. Charpin, and H. Dobbertin. A new characterization of almost bent functions. *Fast Software Encryption 99, Lecture Notes in Computer Science* 1636, L. Knudsen, editor, pp. 186-200. Springer-Verlag, 1999.

[29] A. Canteaut, P. Charpin, and H. Dobbertin. Binary m-sequences with three-valued crosscorrelation: A proof of Welch's conjecture. *IEEE Trans. Inform. Theory*, 46 (1), pp. 4-8, 2000.

[30] A. Canteaut, P. Charpin, and H. Dobbertin. Weight divisibility of cyclic codes, highly nonlinear functions on GF(2^m) and crosscorrelation of maximum-length sequences. *SIAM Journal on Discrete Mathematics*, 13(1), pp. 105–138, 2000.

[31] A. Canteaut, P. Charpin, and M. Videau. Cryptanalysis of block ciphers and weight divisibility of some binary codes. *Information, Coding and Mathematics (Workshop in honor of Bob McEliece's 60th birthday).* Kluwer, pp. 75-97, 2002.

[32] A. Canteaut and M. Videau. Degree of composition of highly nonlinear functions and applications to higher order differential cryptanalysis. *Advances in Cryptology - EUROCRYPT 2002, Lecture Notes in Computer Science*, pp. 518-533, Springer-Verlag, 2002.

[33] C. Carlet. A construction of bent functions. *Finite Fields and Applications, London Mathematical Society*, Lecture Series 233, Cambridge University Press, pp. 47-58, 1996.

[34] C. Carlet. On the confusion and diffusion properties of Maiorana-McFarland's and extended Maiorana-McFarland's functions. *Special Issue "Complexity Issues in Coding and Cryptography", dedicated to Prof. Harald Niederreiter on the occasion of his 60th birthday, Journal of Complexity* 20, pp. 182-204, 2004.

[35] C. Carlet. On the secondary constructions of resilient and bent functions. Proceedings of the Workshop on Coding, Cryptography and Combinatorics 2003, published by Birkhäuser Verlag, K. Feng, H. Niederreiter and C. Xing Eds., pp. 3-28, 2004.

[36] 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.

[37] C. Carlet and C. Ding. Highly Nonlinear Mappings. *Special Issue "Complexity Issues in Coding and Cryptography", dedicated to Prof. Harald Niederreiter on the occasion of his 60th birthday, Journal of Complexity* 20, pp. 205-244, 2004.

[38] C. Carlet and C. Ding. Nonlinearities of S-boxes. *Finite Fields and its Applications* Vol. 13 Issue 1, pp. 121-135, January 2007.

[39] C. Carlet, K. Khoo, C.-W. Lim and C-W Loe. Generalized correlation analysis of vectorial Boolean functions. Proceedings of FSE 2007. Lecture Notes in Computer Science 4593, pp. 382-398, 2007.

[40] C. Carlet, K. Khoo, C.-W. Lim and C-W Loe. On an improved correlation analysis of stream ciphers using multi-output Boolean functions and the related generalized notion of nonlinearity. Preprint.

[41] C. Carlet and E. Prouff. On a new notion of nonlinearity relevant to multi-output pseudo-random generators. *Proceedings of Selected Areas in Cryptography 2003, Lecture Notes in Computer Science* 3006,pp. 291–305, 2004.

[42] C. Carlet and E. Prouff. Vectorial Functions and Covering Sequences. *Proceedings of Finite Fields and Applications, Fq7, Lecture Notes in Computer Science* 2948, G. L. Mullen, A. Poli and H. Stichtenoth edts, pp. 215-248, 2004.

[43] L. Carlitz and S. Uchiyama. Bounds for exponential sums. Duke Math. Journal 1, pp. 37-41, 1957.

[44] F. Chabaud and S. Vaudenay. Links between Differential and Linear Cryptanalysis. *EUROCRYPT'94, Advances in Cryptology, Lecture Notes in Computer Science* 950, Springer Verlag, pp. 356-365, 1995.

[45] S. Chanson, C. Ding and A. Salomaa. Cartesian authentication codes from functions with optimal nonlinearity. *Theoretical Computer Science* 290, pp. 1737-1752, 2003.

[46] J. H. Cheon. Nonlinear Vector Resilient Funcions. *Advances in Cryptology - CRYPTO 2001*, Lecture Notes in Computer Science 2139, Springer-Verlag, pp. 458-469, 2001.

[47] B. Chor, O. Goldreich, J. Hastad, J. Friedman, S. Rudich and R. Smolensky. The bit extraction problem or t-resilient functions. *Proc. 26th IEEE Symp. on Foundations of Computer Science*, pp. 396-407, 1985.

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

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

[50] 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.

[51] P. Delsarte. Bounds for unrestricted codes, by linear programming. *Philips Research Reports* 27, pp. 272-289, 1972.

[52] P. Delsarte. An algebraic approach to the association schemes of coding theory. PhD thesis. Université Catholique de Louvain, 1973.

[53] J. F. Dillon. APN polynomials and related codes. Banff Conference, November 2006.

[54] J. F. Dillon. Multiplicative difference sets via additive characters. *Designs, Codes and Cryptography* 17, pp. 225-235, 1999.

[55] J. F. Dillon and H. Dobbertin. New cyclic difference sets with Singer parameters. *Finite Fields and Applications* 10, pp. 342-389, 2004.

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

[57] H. Dobbertin. Construction of bent functions and balanced Boolean functions with high nonlinearity. *Fast Software Encryption, Second International Workshop*, Lecture Notes in Computer Science 1008, pp. 61-74, 1995.

[58] H. Dobbertin. Kasami power functions, permutation polynomials and cyclic difference sets. *Proceedings of the NATO-A.S.I. Workshop "Difference sets, sequences and their correlation properties"*, Bad Windsheim, Kluwer Verlag, pp. 133-158, 1998.

[59] H. Dobbertin. Another proof of Kasami's Theorem. *Designs, Codes and Cryptography* 17, pp. 177-180, 1999.

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

[61] H. Dobbertin, Almost perfect nonlinear power functions on $GF(2^n)$: The Niho case, *Information and Computation* 151, pp. 57-72, 1999.

[62] H. Dobbertin. Almost perfect nonlinear power functions on GF(2^n): a new case for n divisible by 5. D. Jungnickel and H. Niederreiter Eds. *Proceedings of Finite Fields and Applications* Fq5, Augsburg, Germany, Springer, pp. 113-121, 2000.

[63] H. Dobbertin. Uniformly representable permutation polynomials. *Proceedings of Sequences and their Applications, SETA 01*, Springer, pp. 1-22, 2002.

[64] H. Dobbertin. Private communication, 1998.

[65] Y. Edel, G. Kyureghyan and A. Pott. A new APN function which is not equivalent to a power mapping. *IEEE Trans. Inform. Theory* 52, pp. 744-747, 2006.

[66] J. Friedman. The bit extraction problem. *Proc. 33th IEEE Symp. on Foundations of Computer Science*, pp. 314-319, 1992.

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

[68] K. Gupta and P. Sarkar. Improved Construction of Nonlinear Resilient S-Boxes, *Advances in Cryptology - ASIACRYPT 2002*, Lecture Notes in Computer Science 2501, pp. 466-483, 2002.

[69] K. Gupta and P. Sarkar. Construction of perfect nonlinear and maximally nonlinear multiple-output Boolean functions satisfying higher order strict avalanche criteria. *IEEE Transactions on Inform. Theory* 50, pp. 2886-2894, 2004.

[70] T. Helleseth and P. V. Kumar. Sequences with low correlation. In *Handbook of Coding Theory*, V. Pless and W.C. Huffman Eds. Amsterdam, The Netherlands: Elsevier, vol. II, pp. 1765-1854, 1998.

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

[72] T. Helleseth, C. Rong and D. Sandberg. New families of almost perfect nonlinear power mappings. *IEEE Transactions on Inform. Theory* 45, pp. 475-485, 1999.

[73] T. Helleseth and V. Zinoviev. On $\mathbb{Z}_4$-linear Goethals codes and Kloosterman sums. *Designs, Codes and Cryptography* 17, pp. 269-288, 1999.

[74] H. Hollman and Q. Xiang. A proof of the Welch and Niho conjectures on crosscorrelations of binary m-sequences. *Finite Fileds and Their Applications* 7, pp. 253-286, 2001.

[75] X.-d. Hou. Affinity of permutations of $\mathbb{F}_2^n$. *Proceedings of the Workshop on Coding and Cryptography* 2003, Augot, Charpin and Kabatianski eds, pp. 273-280, 2003.

[76] T. Jakobsen and L.R. Knudsen. The interpolation attack on block ciphers. *Fast Software Encryption'97, Lecture Notes in Computer Science* 1267, pp. 28-40, 1997.

[77] H. Janwa and R. Wilson, Hyperplane sections of Fermat varieties in P^3 in char. 2 and some applications to cyclic codes. *Proceedings of AAECC-10, Lecture Notes in Computer Science*, vol. 673, Berlin, Springer-Verlag, pp. 180–194, 1993.

[78] T. Johansson and E. Pasalic, A construction of resilient functions with high nonlinearity, *Proceedings of the IEEE International Symposium on Information Theory* Sorrente, Italy, 2000.

[79] D. Jungnickel and A. Pott. Difference sets: An introduction. In *Difference sets, Sequences and their Autocorrelation Properties*, A. Pott,

P.V. Kumar, T. Helleseth and D. Jungnickel, Eds. Amsterdam, The Netherlands: Kluwer, pp. 259-295, 1999.

[80] T. Kasami, The weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes, *Information and Control* 18, pp. 369-394, 1971.

[81] K. Khoo, G. Gong and D. Stinson. Highly nonlinear S-boxes with reduced bound on maximum correlation. *Proceedings of 2003 IEEE International Symposium on Information Theory*, 2003. http://www.cacr.math.uwaterloo.ca/techreports/2003/corr2003-12.ps

[82] K. Khoo and G. Gong. New constructions for resilient and highly nonlinear Boolean functions. *Proceedings of 8th Australasian Conference, ACISP 2003, Wollongong, Australia, Lecture Notes in Computer Science* 2727 Springer, pp. 498-509, 2003.

[83] K. Kurosawa, T. Satoh and K. Yamamoto, Highly Nonlinear t-Resilient Functions, *Journal of Universal Computer Science* vol. 3, no 6, pp. 721–729, 1997.

[84] G. Kyureghyan. Differentially affine maps. *Proceedings of the Workshop on Coding and Cryptography* 2005, Bergen, pp. 296-305, 2005.

[85] G. Lachaud and J. Wolfmann. The Weights of the Orthogonals of the Extended Quadratic Binary Goppa Codes. *IEEE Trans. Inform. Theory*, vol. 36, pp. 686-692, 1990.

[86] J. Lahtonen, G. McGuire and H. Ward. Gold and Kasami-Welch functions, quadratic forms and bent functions. *Advances of Mathematics of Communication*, vol. 1, pp. 243-250, 2007.

[87] X. Lai. Higher order derivatives and differential cryptanalysis. *Proc. of the "Symposium on Communication, Coding and Cryptography", in honor of J. L. Massey on the occasion of his 60'th birthday.* 1994.

[88] V. I. Levenshtein. Split Orthogonal Arrays and Maximum Independent Resilient Systems of Functions. *Des. Codes Cryptography* 12(2), pp. 131-160, 1997.

[89] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications, vol. 20, Addison-Wesley, Reading, Massachussetts (1983)

[90] F. J. MacWilliams and N. J. Sloane. *The theory of error-correcting codes*, Amsterdam, North Holland. 1977.

[91] M. Matsui. Linear cryptanalysis method for DES cipher. *Advances in Cryptology - EUROCRYPT'93, no. 765 in Lecture Notes in Computer Science. Springer-Verlag*, pp. 386-397, 1994.

[92] K. Nyberg. Perfect non-linear S-boxes, *Advances in Cryptology, EUROCRYPT' 91, Springer Verlag, Lecture Notes in Computer Science* 547, pp. 378-386, 1992.

[93] K. Nyberg. On the construction of highly nonlinear permutations. *Advances in Cryptology, EUROCRYPT' 92, Springer Verlag, Lecture Notes in Computer Science* 658, pp. 92-98, 1993.

[94] K. Nyberg. Differentially uniform mappings for cryptography. *Advances in Cryptology, EUROCRYPT' 93, Lecture Notes in Computer Science* 765, pp. 55-64, 1994.

[95] K. Nyberg. New bent mappings suitable for fast implementation. *Fast Software Encryption 1993, Lecture Notes in Computer Science* 809, pp. 179-184, 1994.

[96] K. Nyberg. S-boxes and Round Functions with Controllable Linearity and Differential Uniformity. *Proceedings of Fast Software Encryption 1994, Lecture Notes in Computer Science* 1008, pp. 111-130, 1995.

[97] K. Nyberg. Multidimensional Walsh transform and a characterization of bent functions. Information Theory Workshop, Bergen, Norway, July 2007.

[98] E. Pasalic and S. Maitra. Linear Codes in Generalized Construction of Resilient Functions with Very High Nonlinearity, *IEEE Transactions on Information Theory*, Vol. 48, pp. 2182- 2191, 2002, and *Proceedings of Selected Areas in Cryptography, 8th Annual International Workshop, SAC 2001*, Lecture Notes in Computer Science 2259, pp. 60-74, 2002.

[99] E. Prouff. DPA attacks and S-boxes. *Fast Software Encryption 2005, Lecture Notes in Computer Science* 3557, pp. 424-442, 2005.

[100] C. R. Rao. Factorial experiments derivable from combinatorial arrangements of arrays. *J. Royal Statist. Soc.* 9, pp. 128-139, 1947.

[101] J. Seberry, X.-M. Zhang and Y. Zheng. Relationship among Nonlinearity Criteria. *Advances in Cryptography - EUROCRYPT'94, Lecture Notes in Computer Science*, 950, Springer - Verlag, Berlin, Heidelbeg, New York, pp. 376-388, 1995.

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

[103] D.R. Stinson. Resilient functions and large sets of orthogonal arrays. *Congressus Numer.*, vol 92, pp. 105-110, 1993.

[104] D.R. Stinson and J.L. Massey. An infinite class of counterexamples to a conjecture concerning nonlinear resilient functions. *Journal of Cryptology*, vol 8, n° 3, pp. 167-173, 1995.

[105] A. Tardy-Corfdir and H. Gilbert. A known plaintext attack on feal-4 and feal-6. In *Advances in Cryptology - CRYPTO'91, Lecture Notes in Computer Science* 576, Springer-Verlag, pp. 172-181, 1991.

[106] S. Vaudenay. On the need for multipermutations: cryptanalysis of MD4 and SAFER. *Fast Software Encryption, Lecture Notes in Computer Science* 1008, pp. 286-297, 1995.

[107] T. Wadayama, T. Hada, K. Wagasugi and M. Kasahara. Upper and lower bounds on the maximum nonlinearity of n-input m-output Boolean functions, *Designs, Codes and Cryptography* 23, pp. 23–33, 2001.

[108] A.F. Webster and S.E. Tavares. On the design of S-boxes. In *Advances in Cryptology - CRYPTO'85, Lecture Notes in Computer Science* 219, pp. 523–534. Springer-Verlag, 1985.

[109] X.-M. Zhang and Y. Zheng. On Nonlinear Resilient Functions. *Advances in Cryptology - EUROCRYPT '95, Lecture Notes in Computer Science* 921, pp. 274-288, Springer, 1995.

[110] X.-M. Zhang and Y. Zheng. Cryptographically Resilient Functions. *IEEE Transactions on Information Theory*, vol. 43, pp. 1740-1747, 1997.

[111] M. Zhang and A. Chan. Maximum correlation analysis of nonlinear S-boxes in stream ciphers. *Advances in Cryptology - CRYPTO 2000*, volume 1880 of *Lecture Notes in Computer Science*, pp. 501-514, Springer, Berlin, 2000.

Index