On plateaued functions and their constructions

Claude Carlet[1] and Emmanuel Prouff[2]

[1] INRIA, projet CODES, BP 105 - 78153, Le Chesnay Cedex, FRANCE; also member of GREYC-Caen and of the University of Paris 8 claude.carlet@inria.fr
[2] INRIA Projet CODES and University of Paris 11, Laboratoire de Recherche en Informatique, 15 rue Georges Clemenceau, 91405 Orsay Cedex, FRANCE
prouff@info.unicaen.fr

Abstract. We use the notion of covering sequence, introduced by C. Carlet and Y. Tarannikov, to give a simple characterization of bent functions. We extend it into a characterization of plateaued functions (that is bent and three-valued functions). After recalling why the class of plateaued functions provides good candidates to be used in cryptosystems, we study the known families of plateaued functions and their drawbacks. We show in particular that the class given as new by Zhang and Zheng is in fact a subclass of Maiorana-McFarland's class. We introduce a new class of plateaued functions and prove its good cryptographic properties.

Keywords : Boolean functions, Bent, Three-valued crosscorrelation, Nonlinearity, Resiliency, Stream Ciphers, Combinatorial Cryptography.

1 Introduction

In the design of cryptographic functions, there is need to consider various characteristics simultaneously (balancedness, high nonlinearity, high algebraic degree, good propagation characteristics, high order correlation immunity, non-existence of non-zero linear structures...). The importance of each characteristic depends on the choice of the cryptosytem. Balancedness and nonlinearity are most important criteria in all situations.

By achieving optimum nonlinearity, bent functions permit to resist linear attacks in the best possible way. But, being not balanced they are improper for direct cryptographic use. Moreover, they exist only in even dimensions. This led cryptographers to search for new classes of Boolean functions whose elements still have good nonlinearities and can be balanced (and moreover resilient) for both odd and even dimensions. The class of partially-bent functions was first investigated [9]. These functions are built by identifying in the space $\mathbb{F}_2^n$ two subspaces E and F whose direct sum equals $\mathbb{F}_2^n$ and by defining the functions as the sums of linear functions defined on E and of bent functions defined on F. But in spite of their potentially good properties (good nonlinearity, resiliency and propagation characteristics) partially-bent functions, when they are not bent, have by definition non-zero linear structures and so do not give full satisfaction. The class of plateaued functions [3] is a natural extension of the notion of partially bent function. It provides some examples of good trade-offs between all the properties needed for a cryptosystem. For instance, it has been shown by Sarkar and Maitra [34] that the order of resiliency and the nonlinearity of Boolean functions were strongly bounded (this result was partly also obtained by Tarannikov [36] and Zheng and Zhang [39]); the best compromise between those two properties is achieved by plateaued functions only. Tarannikov gave examples of functions achieving this best possible compromise. These examples [33] and almost all the other existing examples were obtained through iterative constructions. The functions obtained this way often have cryptographic weaknesses such as linear structures (see [4]). The only known general class of non iteratively defined plateaued functions is obtained through Maiorana-McFarland's construction (or its generalization by Carlet [12]). It contains functions which reach Sarkar et al.'s bound but only for very high resiliency orders (cf. [12]).

By extending the notion of covering sequence of balanced functions introduced by Carlet and Tarannikov [14] we give in this paper a characterization of bent functions and extend it to a characterization of plateaued functions. We recall some basic properties of plateaued functions and we give a list of all the known constructions of such functions. For each of them, we recall the main drawbacks. In the last part of this paper, we introduce and we study a new class of plateaued functions which have not the weaknesses of the Maiorana-McFarland's functions.

2 Preliminaries

We shall have to distinguish in the whole paper between the additions of integers in $\mathbb{R}$, denoted by $+$ and $\sum_i$, and the additions mod 2, denoted by $\oplus$ and $\bigoplus_i$. So all the sums computed in characteristic 0 will be denoted by $\sum_i$ and all the sums computed 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 $\mathbb{F}_2^n$ (words).

We first recall basic facts about Boolean functions. A Boolean function f in n variables is an $\mathbb{F}_2$-valued function on the space $\mathbb{F}_2^n$ of n-tuples over $\mathbb{F}_2$. We call support of f the set $\{x \in \mathbb{F}_2^n / f(x) = 1\}$ and we denote it by $Supp\,(f)$. Its size is by definition the weight of f and is denoted by $W(f)$. A Boolean function f is balanced if $W(f) = 2^{n-1}$.

[3] The term of "plateaued" was proposed by Zhang and Zheng [40] and denotes the functions which either are bent or have a Walsh spectrum with three values 0 and $\pm\lambda$. Some of these functions had been studied already in Sequence designs [2, 16, 19–21] and in Codes [31].

Every Boolean function f on $\mathbb{F}_2^n$ admits a unique representation as a polynomial over $\mathbb{F}_2$ in n binary variables of the form:

$$f(x_1, \cdots, x_n) = \bigoplus_{I \subseteq \{1, \cdots, n\}} a_I \prod_{i \in I} x_i. \tag{1}$$

This representation is called the algebraic normal form (A.N.F.) of f. We will call (algebraic) degree of f and denote by $deg\, f$ the degree of its A.N.F. and we denote by $R(d, n)$ the set of all Boolean functions on $\mathbb{F}_2^n$ whose degrees are upper bounded by d (the so-called Reed-Muller code of order d on $\mathbb{F}_2^n$).

To make easier the study of the properties of f, we classically introduce the "sign" function χ_f of f defined as $\chi_f(x) = (-1)^{f(x)}$. The Fourier transform $\widehat{\chi_f}$ of χ_f will be called the *Walsh transform* of f. By definition $\widehat{\chi_f}(b) = \sum\limits_{x \in \mathbb{F}_2^n} (-1)^{f(x)+x\cdot b}$. It satisfies Parseval's relation :

$$\sum_{b \in \mathbb{F}_2^n} \widehat{\chi_f}^2(b) = 2^{2n} \tag{2}$$

and the inverse Fourier formula,

$$\widehat{\widehat{\chi_f}} = 2^n \chi_f \tag{3}$$

(which is more generally valid for every real-valued function).

We recall now the definition of the convolutional product between two numerical functions φ and ψ on $\mathbb{F}_2^n$. It is denoted by $\varphi \otimes \psi$ and defined on $\mathbb{F}_2^n$ by:

$$(\varphi \otimes \psi)(x) = \sum_{a \in \mathbb{F}_2^n} \varphi(a)\, \psi(a + x). \tag{4}$$

A well-known fact is that the Fourier transform of $\varphi \otimes \psi$ equals the product of $\widehat{\varphi}$ and $\widehat{\psi}$, that is:

$$\widehat{\varphi \otimes \psi} = \widehat{\varphi}\widehat{\psi}. \tag{5}$$

A useful tool to study a Boolean function f is the notion of derivative. The derivative of f with respect to a vector $a \in \mathbb{F}_2^n$ is the function $D_a f : x \longrightarrow f(x) \oplus f(x + a)$. The derivatives play an important role in crytpography, related to the differential attack [1]. They are also naturally involved in the definition of the Strict Avalanche Criterion SAC and of the Propagation Criterion PC [32]. These criteria evaluate some kind of diffusion of the function.

The Hamming distance between two Boolean functions f_1 and f_2 on $\mathbb{F}_2^n$ equals by definition the weight of $f_1 \oplus f_2$. We call *nonlinearity* of f and we denote by N_f the minimum distance between f and all affine functions. The nonlinearity of a function quantifies the level of *confusion* put in the system by the Boolean function. Cryptographic functions used in stream or block ciphers must have high nonlinearities to prevent these systems from linear attacks (see [37, 27]).

For every Boolean function f, the nonlinearity N_f and the Walsh transform $\widehat{\chi_f}$ satisfy the relation:

$$N_f = 2^{n-1} - \frac{1}{2} \max_{b \in \mathbb{F}_2^n} |\widehat{\chi_f}(b)|. \tag{6}$$

Because of Parseval's relation (2), N_f is upper bounded by $2^{n-1} - 2^{n/2-1}$. This bound is tight for every n even. The functions achieving it are called *bent*.
We recall now the different known characterizations of bent functions:

Proposition 1. *A Boolean function f on $\mathbb{F}_2^n$ is bent if and only if one of the two following statements is satisfied:*
1. $\forall b \in \mathbb{F}_2^n, \widehat{\chi_f}(b) = \pm 2^{\frac{n}{2}}$,
2. $\forall a \in \mathbb{F}_2^{n*}, W(D_a f) = 2^{n-1}$.

Thus, derivatives play also a role with respect to the notion of confusion, since they permit a characterization of bent functions; recent results [5] show that they play more generally a role with respect to nonlinearity, even for non-bent functions.

Remark: the notion of bent function being invariant under addition of affine functions, it would be more natural to characterize bent functions by means of their second-order derivatives $D_a D_b f$ and not by means of their first-order derivatives $D_a f$ (indeed, the affine functions are those Boolean functions whose second-order derivatives all vanish). This will be done at Proposition 3.

3 A characterization of bent functions through their second-order derivatives

In [14], Carlet and Tarannikov introduced the notion of covering sequence of a Boolean function.

Definition 1. *A covering sequence of a function $f : \mathbb{F}_2^n \mapsto \mathbb{F}_2$ is any sequence of reals $\lambda = (\lambda_a)_{a \in \mathbb{F}_2^n}$ such that the real summation $\sum_{a \in \mathbb{F}_2^n} \lambda_a D_a f$ is equal to a constant function ρ. The value of ρ is called the level of this sequence. If $\rho \neq 0$, then we say that the covering sequence is non-trivial.*

The next proposition gives complete characterization of the balancedness of Boolean functions by means of their covering sequences.

Proposition 2. *[14] Any Boolean function f on $\mathbb{F}_2^n$ is balanced if and only if it admits a non-trivial covering sequence. The same covering sequence – the constant sequence 1 – can be taken for all balanced functions. The level of this sequence with respect to any balanced function equals 2^{n-1}.*

We denote the *second-order derivatives* of f by D_aD_bf; we have $D_aD_bf(x) = f(x) \oplus f(x+a) \oplus f(x+b) \oplus f(x+a+b)$.

As seen in Proposition 1, all the derivatives D_af, $a \neq 0$, of a bent function f are balanced and so, according to Proposition 2, satisfy:

$$\forall x \in \mathbb{F}_2^n,\ \textstyle\sum_{b\in\mathbb{F}_2^n} D_bD_af(x) = 2^{n-1}.$$

Thus, all bent functions are such that:

$$\forall x \in \mathbb{F}_2^n,\ \textstyle\sum_{a,b\in\mathbb{F}_2^n} D_bD_af(x) = 2^{2n-1} - 2^{n-1},$$

that is $\forall x \in \mathbb{F}_2^n,\ \sum_{a,b\in\mathbb{F}_2^n} (-1)^{D_bD_af(x)} = 2^n$, since $(-1)^{D_bD_af(x)} = 1 - 2D_bD_af(x)$.

Let us prove now that this necessary condition is in fact a necessary and sufficient one.

Proposition 3. *A Boolean function f defined on $\mathbb{F}_2^n$ is bent if and only if:*

$$\forall x \in \mathbb{F}_2^n,\ \sum_{a,b\in\mathbb{F}_2^n} (-1)^{D_aD_bf(x)} = 2^n. \tag{7}$$

Proof. Set $\theta = 2^n$. A Boolean function f satisfies:

$$\forall x \in \mathbb{F}_2^n, \textstyle\sum_{a,b\in\mathbb{F}_2^n} (-1)^{D_aD_bf(x)} = \theta$$

if and only if

$$\forall x \in \mathbb{F}_2^n, \textstyle\sum_{a,b\in\mathbb{F}_2^n} (-1)^{f(x+a)+f(x+b)+f(x+a+b)} = \theta(-1)^{f(x)},$$

or equivalently:

$$\forall x \in \mathbb{F}_2^n, \textstyle\sum_{a,b\in\mathbb{F}_2^n} (-1)^{f(a)+f(b)+f(x+a+b)} = \theta(-1)^{f(x)},$$

which can be rewritten using the convolutional product in the form

$$\chi_f \otimes \chi_f \otimes \chi_f = \theta\ \chi_f.$$

According to the bijectivity of the Fourier transform and according to Relation (5), this is equivalent to :

$$\forall u \in \mathbb{F}_2^n,\ \widehat{\chi_f}^3(u) = \theta\ \widehat{\chi_f}(u).$$

Thus, we have $\sum_{a,b\in\mathbb{F}_2^n} (-1)^{D_aD_bf(x)} = \theta$ if and only if, for every $u \in \mathbb{F}_2^n$, $\widehat{\chi_f}(u)$ equals $\pm\sqrt{\theta}$ or 0. Since $\theta = 2^n$ and according to Parseval's relation (2), the value 0 is then never achieved by $\widehat{\chi_f}$.

Since we could characterize those Boolean functions satisfying relation (7) as the bent functions, a natural idea is to try to characterize similarly those Boolean functions such that

$$\forall x \in \mathbb{F}_2^n,\ \sum_{a,b\in\mathbb{F}_2^n} (-1)^{D_aD_bf(x)} = \theta \tag{8}$$

where θ is no more necessarily equal to 2^n.

We shall see that this relation characterizes the class of plateaued functions.

4 Characterization of plateaued functions through their second-order derivatives

4.1 Plateaued functions

A Boolean function $f : \mathbb{F}_2^n \mapsto \mathbb{F}_2$ is said to be plateaued if its Walsh transform $\widehat{\chi_f}$ only takes the three values 0 and $\pm\lambda$, where λ is some positive integer. We shall call λ the *amplitude* of the plateaued function. Because of Parseval's relation, λ cannot be null and must be a power 2^r with $r \geq n/2$.

Clearly, the nonlinearity N_f of a plateaued function of amplitude λ equals $2^{n-1} - \frac{\lambda}{2}$.

These functions have been studied by many researchers in sequence design when they studied the cross-correlation between m-sequences and their decimations by an integer d (cf. Annex A.2) and by Canteaut, Carlet, Charpin and Fontaine [5, 6]. In the standard model of stream ciphers, a Boolean function is used to combine the outputs of n linear feedback shift registers. To resist divide-and-conquer attacks, called correlation attacks, this function called combining function, has to be balanced and to stay balanced if any m of the inputs are fixed. This property, called correlation-immunity, can be characterized by means of the Fourier transform :

Proposition 4 ([38]). *A Boolean function f on $\mathbb{F}_2^n$ is m-th order correlation immune if and only if its Walsh transform $\widehat{\chi_f}$ satisfies $\widehat{\chi_f}(u) = 0$ for every vector u in $\mathbb{F}_2^n$ such that $1 \leq w_H(u) \leq m$, where w_H denotes the Hamming weight. Balanced mth-order correlation-immune functions are called m-resilient.*

As proved in [34], [36] and [41], the resiliency order m of a Boolean function defined on $\mathbb{F}_2^n$ and its nonlinearity satisfy the relation $N_f \leq 2^{n-1} - 2^{m+1}$. Thus, the resiliency order m is upper bounded by $\log_2\left(2^{n-1} - N_f\right) -1$. Moreover, Sarkar and Maitra have shown in [34] that the values of the Walsh Transform of an n-variable, m-resilient (resp. m-th order correlation-immune) function are divisible by 2^{m+2} (resp. 2^{m+1}) if $m \leq n-2$. Thus, if an m-resilient function achieves nonlinearity $2^{n-1} - 2^{m+1}$, then the function is plateaued. Indeed, according to Relation (6), the value of $\max_{b\in\mathbb{F}_2^n} |\widehat{\chi_f}(b)|$ equals 2^{m+2}. By applying Relation (6) again, we see that the nonlinearity of plateaued functions with amplitude $\lambda = 2^r$ being equal to $2^{n-1} - 2^{r-1}$, their resiliency order is upper bounded by $r-2$. A function whose nonlinearity and resiliency order are respectively $2^{n-1} - 2^{r-1}$ and $r-2$ is a good candidate to be used in stream ciphers, since it gives a best possible tradeoff between resiliency and nonlinearity (and it has then also maximum possible algebraic degree, cf. [36]). Tarannikov and other authors exhibited some functions with non-linearity $N_f = 2^{n-1} - 2^{r-1}$ and resiliency order achieving the bound $r-2$.

4.2 The characterization

The proof of Proposition 3 (except its last sentence) extends straightforwardly to any value of θ:

Theorem 1. *A Boolean function f is plateaued on $\mathbb{F}_2^n$ if and only if there exists θ such that for every $x \in \mathbb{F}_2^n$, $\sum_{a,b\in\mathbb{F}_2^n} (-1)^{D_a D_b f(x)} = \theta$. If this condition is satisfied, then the amplitude of the plateaued function f equals $\sqrt{\theta}$, and θ is a power of 2 whose exponent is even and greater than or equal to n.*

Remark:
1. The fact that quadratic functions are plateaued is a direct consequence of Theorem 1, since their second-order derivatives are constant. And Theorem 1 gives more insight on the relationship between the nonlinearity of a quadratic function and the number of its nonzero second-order derivatives.
2. The second-order derivatives of Boolean functions of degree 3 being affine, Theorem 1 shows a relationship between the ability of constructing plateaued functions of degree 3 and producing sets of affine hyperplanes which are multi-coverings of $\mathbb{F}_2^n$. $\diamond$

In the next section, we present the different existing ways to construct plateaued functions. By identifying their drawbacks we motivate the search for new classes and exhibit one.

5 Known constructions of plateaued functions

In this section, we investigate the known constructions of Boolean functions and we determine precisely which ones allow us to obtain plateaued functions (for completeness, we list in Appendix A.2 the plateaued functions constructed in sequence designs).

5.1 Maiorana-McFarland's functions as well as others

We recall the primary contructions, in which one does not suppose the existence of previously defined functions to define new ones (see Appendix A.1 for secondary constructions).

All affine functions are plateaued, but they have null nonlinearity. All quadratic functions are also plateaued, but they are improper for cryptographic use because of their low degree (see [25, 26]).

The two main primary constructions of bent functions are given by Dillon [17] and McFarland [29] and lead to the classes called respectively PS_{ap} and Maiorana-McFarland.

For any integer n, a function in PS_{ap} takes the form $g(\frac{x}{y})$ ($\frac{x}{y} = 0$ if $x = 0$ or $y = 0$) where x and y belong to $\mathbb{F}_2^{\frac{n}{2}}$, the Galois Field of order $2^{\frac{n}{2}}$, and g is a balanced Boolean function on $\mathbb{F}_2^{\frac{n}{2}}$. We have checked that one cannot derive from

PS_{ap} a construction of plateaued functions by choosing g non-balanced instead of balanced.

Camion et al. generalized in [3] the class of Maiorana Mc-Farland's functions. We shall call $\mathcal{M}$ the generalized class defined as follows:

Definition 2. *Class $\mathcal{M}$ is the set of functions $f_{\phi,h}$ which can be written in the form:*

$$f_{\phi,h}\left(x,y\right)=x\cdot\phi\left(y\right)\oplus h\left(y\right) \tag{9}$$

where r and s are any positive integers, $n=r+s$, ϕ is any function from $\mathbb{F}_2^s$ into $\mathbb{F}_2^r$ and h is any Boolean function on $\mathbb{F}_2^s$.

Notice that for $r=1$, we obtain all Boolean functions on $\mathbb{F}_2^n$.
Let $f_{\phi,h}$ be a function in $\mathcal{M}$. For any pair $(a,b)\in\mathbb{F}_2^r\times\mathbb{F}_2^s$, the value at (a,b) of the Walsh transform $\widehat{\chi_{f_{\phi,h}}}$ of $f_{\phi,h}$ equals $2^r\sum_{y\in\phi^{-1}(a)}\left(-1\right)^{b\cdot y+h(y)}$. Then $f_{\phi,h}$ is plateaued if and only if $\sum_{y\in\phi^{-1}(a)}\left(-1\right)^{b\cdot y+h(y)}$ takes three values 0 and $\pm\lambda$ when (a,b) ranges over $\mathbb{F}_2^r\times\mathbb{F}_2^s$. The following proposition gives two sufficient conditions to ensure that a given function $f_{\phi,h}$ in $\mathcal{M}$ is plateaued.

Proposition 5. *Let $f_{\phi,h}$ be a function defined on $\mathbb{F}_2^r\times\mathbb{F}_2^s$ and belonging to $\mathcal{M}$. If ϕ is injective (resp. takes exactly 2 times each value of $Im\left(\phi\right)$), then $f_{\phi,h}$ is plateaued of amplitude 2^r (resp. 2^{r+1}).*

Proof. If ϕ is injective, then every pre-image by ϕ has cardinality 1 or 0. This implies that $\widehat{\chi_{f_{\phi,h}}}\left(a,b\right)$ is null if $\phi^{-1}\left(a\right)=\emptyset$ and equals $2^r\left(-1\right)^{b\cdot\phi^{-1}(a)+h\circ\phi^{-1}(a)}$ otherwise. We deduce that $f_{\phi,h}$ is plateaued of amplitude 2^r.
If ϕ is two-to-one, i.e. takes exactly 2 times each value of $Im\left(\phi\right)$, then $\phi^{-1}\left(a\right)$ has cardinality 2 or 0. Let a be an element of $\mathbb{F}_2^r$ such that $\#\phi^{-1}\left(a\right)=2$, we denote by $\{y_1,y_2\}$ the set $\phi^{-1}\left(a\right)$. Then, for any $b\in\mathbb{F}_2^s$, $2^r\sum_{y\in\phi^{-1}(a)}\left(-1\right)^{b\cdot y+h(y)}$ equals to $2^r[(-1)^{b\cdot y_1+h(y_1)}+(-1)^{b\cdot y_2+h(y_2)}]$ which is either 0 or $\pm2^{r+1}$.

We shall denote by $\mathcal{M}_i$ the class of plateaued functions of amplitude 2^i obtained by applying Proposition 5 ($i=r$ in the first case and $i=r+1$ in the second).
We study now the conditions in which we can achieve best tradeoff between resiliency and nonlinearity.

Proposition 6. *Let $f_{\phi,g}$ be a Maiorana-McFarland function on $\mathbb{F}_2^r\times\mathbb{F}_2^s$. Let k denote the minimum Hamming weight of elements of $\phi\left(\mathbb{F}_2^s\right)$. If ϕ is injective, the resiliency order m of $f_{\phi,g}$ equals $k-1$ and k is upper bounded by* $\max\{t\in\mathbb{N};\sum_{i=0}^{t}\binom{r}{i}\leq2^r-2^s\}+1$. *If ϕ is two-to-one, then the resiliency order m of $f_{\phi,g}$ is either equal to k or to $k-1$ and k is upper bounded by* $\max\{t\in\mathbb{N};\sum_{i=0}^{t}\binom{r}{i}\leq2^r-2^{s-1}\}+1$.

A drawback of Maiorana-McFarland functions is that their restrictions obtained by keeping y constant in their input are affine. Affine functions being cryptographically weak functions, there is a risk that this property be used in attacks. Moreover, Maiorana-McFarland functions having high divisibilities of their Fourier and Walsh spectra, there is also a risk that this property be used in attacks as it is used in [15] to attack block ciphers.

5.2 On Zhang and Zheng's class of plateaued functions

In [40], Zhang and Zheng introduce a subclass of the class of plateaued functions whose elements are not partially bent. We show that these functions belong to class $\mathcal{M}$ and satisfy the hypothesis of Proposition 5.
Before presenting the construction of Zhang and Zheng, we recall that the truth table of any Boolean function f on $\mathbb{F}_2^n$ results in the binary word of length 2^n defined by $(f(\alpha_0), f(\alpha_1), \cdots, f(\alpha_{2^n-1}))$ where $\alpha_0 = (0, 0, \cdots, 0)$, ...,$\alpha_{2^{n-1}-1} = (1, 1, \cdots, 1)$. If ξ_i and ξ_j are two binary words of length 2^n, we denote by $\xi_i\xi_j$ the word of length 2^{n+1} resulting from their concatenation. We recall now the proposition of Zheng and Zhang leading to their "new" class of plateaued functions.

Proposition 7. *[40] Let t and k be two integers such that $k < 2^t < 2^k$ and let $E \subseteq \mathbb{F}_2^k$ be a subset of 2^t elements such that any linear non null function on $\mathbb{F}_2^k$ is not constant on E. For every element e_i of E, let ξ_i denote the truth table of the linear function $x \mapsto x \cdot e_i$ on $\mathbb{F}_2^k$. Then, the Boolean function f on $\mathbb{F}_2^{k+t}$ having $\xi_0\xi_1 \cdots \xi_{2^t-1}$ for truth table is plateaued on $\mathbb{F}_2^{k+t}$ and its amplitude equals 2^k.*

Viewed as binary vectors of length 2^{k+t}, plateaued functions constructed in such a way are concatenations of distinct linear functions. We deduce that the functions constructed in Proposition 7 belong to $\mathcal{M}$ and satisfy the first hypothesis of Proposition 5. Indeed, for any subset $E \subseteq \mathbb{F}_2^k$ of 2^t elements, one can define an injective function ϕ from $\mathbb{F}_2^t$ into $\mathbb{F}_2^k$ such that $\phi(\mathbb{F}_2^t) = E$: the function f associated to E in Proposition 7 can be rewritten on the product space $\mathbb{F}_2^k \times \mathbb{F}_2^t$ in the form $f(x, y) = x \cdot \phi(y)$. Moreover, we notice that the condition $k < 2^t$ and the condition on E are not necessary to insure that f is plateaued since one only uses the fact that the cardinality of E is a power of 2 to rewrite f as an element of $\mathcal{M}_k$.

5.3 A recent class

A construction generalizing construction $\mathcal{M}$ and avoiding the drawback that these functions are the concatenations of affine functions was proposed in [12]. We shall denote it by $\mathcal{M}'$. The functions it produces are concatenations of quadratic functions (i.e. functions of degrees at most 2) instead of affine functions.

Definition 3. *Let n and r be positive integers such that $r < n$. Denote the integer part $\left\lfloor \frac{r}{2} \right\rfloor$ by t and $n - r$ by s. Let ψ be a mapping from $\mathbb{F}_2^s$ to $\mathbb{F}_2^t$ and let $\psi_1, \cdots, \psi_t$ be its coordinate functions. Let ϕ be a mapping from $\mathbb{F}_2^s$ to $\mathbb{F}_2^r$ and let $\phi_1, \cdots, \phi_r$ be its coordinate functions. Let g be a Boolean function on $\mathbb{F}_2^s$. The function $f_{\psi,\phi,g}$ is defined on $\mathbb{F}_2^n = \mathbb{F}_2^r \times \mathbb{F}_2^s$ as*

$$f_{\psi,\phi,g}(x, y) = \bigoplus_{i=1}^{t} x_{2i-1}x_{2i}\psi_i(y) \oplus x \cdot \phi(y) \oplus g(y);\ x \in \mathbb{F}_2^r,\ y \in \mathbb{F}_2^s.$$

Maiorana-McFarland's functions correspond to the case where ψ is the null mapping. The following theorem is proved in [12].

Theorem 2. *Let $f_{\psi,\phi,g}$ be defined as in Definition 3. Then for every $a \in \mathbb{F}_2^r$ and every $b \in \mathbb{F}_2^s$ we have*

$$\widehat{\chi_{f_{\psi,\phi,g}}}(a,b) = \sum_{y \in E_a} 2^{r - w_H(\psi(y))} (-1)^{\sum_{i=1}^{t} (\phi_{2i-1}(y)+a_{2i-1})(\phi_{2i}(y)+a_{2i}) + g(y) + y \cdot b},$$

where E_a is the superset of $\phi^{-1}(a)$ equal if r is even to

$$\{y \in \mathbb{F}_2^s / \ \forall i \leq t,\ \psi_i(y) = 0 \Rightarrow (\phi_{2i-1}(y) = a_{2i-1} \text{ and } \phi_{2i}(y) = a_{2i})\},$$

and if r is odd to

$$\left\{ y \in \mathbb{F}_2^s / \ \begin{cases} \forall i \leq t,\ \psi_i(y) = 0 \Rightarrow (\phi_{2i-1}(y) = a_{2i-1} \text{ and } \phi_{2i}(y) = a_{2i}) \\ \phi_r(y) = a_r \end{cases} \right\}.$$

We deduce straightfowardly:

Proposition 8. *Let $f_{\psi,\phi,g}$ be defined as in Definition 3. If ψ has constant weight and if E_a has size 0 or 1 for every a (respectively 0 or 2 for every a), then $f_{\psi,\phi,g}$ is plateaued.*

Thus, this construction easily allows us to obtain plateaued functions. A sufficient condition for $f_{\psi,\phi,g}$ being m-resilient is given in [12], as well as examples of functions achieving good tradeoffs between resiliency and nonlinearity. It seems difficult to give numerous such examples, all the more if we add this condition that E_a has size 0 or 1 (or 0 or 2) for every a. So, searching for other constructions still seems to be necessary. Notice that the examples given in [12] of functions $f_{\psi,\phi,g}$ having nonlinearities of the form $2^{n-1} - 2^i - 2^j$ with $i \neq j$ (the m-resilient functions achieving best possible nonlinearities, with $m \leq n/2 - 2$ must have such nonlinearities, at least if n is even) cannot be plateaued.

6 A new construction of Boolean functions leading to two classes of plateaued functions

Functions $f_{\psi,\phi,g}$ in the class $\mathcal{M}'$ are built as the concatenations of quadratic functions chosen in such a way that we can efficiently compute their Walsh spectra. The aim of this section is to present another way of concatenating quadratic functions, whose Walsh spectra can also be efficiently computed. As in the cases of the functions $f_{\phi,g}$ and $f_{\psi,\phi,g}$, the definition of the new class shall lead to two sufficient conditions implying two constructions of plateaued functions.

The quadratic functions we shall concatenate are those functions whose associated symplectic forms (cf. [35]) have rank at most 2:

Lemma 1. *Let r be a positive integer and let f be any Boolean function on $\mathbb{F}_2^r$ of the form $(u \cdot x)(v \cdot x) \oplus w \cdot x$, where u, v and w are three vectors in $\mathbb{F}_2^r$. Assume first that u and v are linearly independent (i.e. $u \neq 0, v \neq 0$ and $u \neq v$). Then f is balanced if and only if w does not belong to the vectorspace $< u, v >= \{0, u, v, u+v\}$ spanned by u and v. If $w \in \{0, u, v\}$, then $\sum_{x\in\mathbb{F}_2^r}(-1)^{f(x)}$ equals 2^{r-1}, and if $w = u + v$, then it equals -2^{r-1}.*
Assume now that u and v are linearly dependent. If ($u = 0$ or $v = 0$) and $w = 0$ or if $u = v = w$, then $\sum_{x\in\mathbb{F}_2^r}(-1)^{f(x)}$ equals 2^r. Otherwise, $\sum_{x\in\mathbb{F}_2^r}(-1)^{f(x)}$ is null.

Proof
Assume first that u and v are linearly independent. We have

$$\sum_{x\in\mathbb{F}_2^r}(-1)^{f(x)} = \sum_{x\in u^\perp}(-1)^{w\cdot x} + \sum_{x\in(u^\perp)^c}(-1)^{(w+v)\cdot x}.$$

The sum $\sum_{x\in u^\perp}(-1)^{w\cdot x}$ is null if $w \neq 0$ and $w \neq u$. The sum $\sum_{x\in(u^\perp)^c}(-1)^{(w+v)\cdot x}$ is null if $w \neq v$ and $w \neq u + v$. Hence if w does not belong to the vectorspace $\{0, u, v, u+v\}$, then $\sum_{x\in\mathbb{F}_2^r}(-1)^{f(x)}$ is null, and thus f is balanced. It is a simple matter to see that if $w \in \{0, u, v\}$, then $\sum_{x\in\mathbb{F}_2^r}(-1)^{f(x)}$ equals 2^{r-1} and that if $w = u + v$ then it equals -2^{r-1}.
Assume now that u and v are linearly dependent. Then f is linear. If $u = 0$ or $v = 0$ then f is null if and only if $w = 0$. If $u = v \neq 0$ then f is null if and only if w equals u. If f is not null, then it is balanced.

Remark: If $v \neq 0$ and if u, v are linearly dependent (i.e. $u = 0$ or $u = v$), then the sum $\sum_{x\in\mathbb{F}_2^r}(-1)^{f(x)}$ equals 2^r if and only if $w = u$. This observation will be useful for Proposition 9 and Corollary 2 below.

We concatenate now the functions studied in Lemma 1 and their complements :

Definition 4. *We call $\mathcal{Q}$ the class of all Boolean functions f of the form*

$$\forall(x, y) \in \mathbb{F}_2^r \times \mathbb{F}_2^s, f_{\phi_1,\phi_2,\phi_3,g}(x, y) = (x \cdot \phi_1(y)) (x \cdot \phi_2(y)) \oplus x \cdot \phi_3(y) \oplus g(y)$$

where ϕ_1, ϕ_2 and ϕ_3 are three functions from $\mathbb{F}_2^s$ into $\mathbb{F}_2^r$ and g is any Boolean function on $\mathbb{F}_2^s$.

Remark:
1. Class $\mathcal{Q}$ has a simpler definition than the class $\mathcal{M}'$ recalled at subsection 5.3. And we shall see that its Walsh spectrum is also simpler to compute. Notice that its size $\left[(2^r)^{2^s}\right]^3 \times 2^{2^s} = 2^{(3r+1)2^s}$ is larger than the size $\left[2^{2^s}\right]^t \times (2^r)^{2^s} \times 2^{2^s} = 2^{(t+r+1)2^s}$ (where $t = \lfloor \frac{r}{2} \rfloor$) of $\mathcal{M}'$.
2. The bent functions constructed in [11] (cf. Proposition 4) belong to class $\mathcal{Q}$.$\diamond$

The restrictions of $f_{\phi_1,\phi_2,\phi_3,g}$ obtained by fixing y in its input being quadratic functions of the form $(u\cdot x)(v\cdot x)\oplus w\cdot x$, as a direct consequence of Lemma 1 we have:

Proposition 9. *Let $f_{\phi_1,\phi_2,\phi_3,g}$ be a function in $\mathcal{Q}$ such that $\phi_2(y)\neq 0$ for every $y\in\mathbb{F}_2^s$. Let E be the set of all $y\in\mathbb{F}_2^s$ such that the vectors $\phi_1(y)$ and $\phi_2(y)$ are linearly independent. Then, for every $a\in\mathbb{F}_2^r$ and every $b\in\mathbb{F}_2^s$, $\widehat{\chi_{f_{\phi_1,\phi_2,\phi_3,g}}}(a,b)$ equals*

$$2^{r-1}\sum_{\substack{y\in E;\\ \phi_3(y)+a\in\{0,\phi_1(y),\phi_2(y)\}}}(-1)^{g(y)+b\cdot y}-2^{r-1}\sum_{\substack{y\in E;\\ \phi_3(y)+a=\phi_1(y)+\phi_2(y)}}(-1)^{g(y)+b\cdot y}+$$
$$2^{r}\sum_{\substack{y\in\mathbb{F}_2^s\setminus E;\\ \phi_3(y)+a=\phi_1(y)}}(-1)^{g(y)+b\cdot y}.$$

6.1 Two constructions of plateaued functions in $\mathcal{Q}$

We deduce from Proposition 9 two sufficient conditions to insure that an element in $\mathcal{Q}$ is plateaued. These conditions are used to construct two new classes $\mathcal{Q}_1$ and $\mathcal{Q}_2$ of plateaued functions.

Corollary 1. *Let $f_{\phi_1,\phi_2,\phi_3,g}$ be defined as in Definition 4. Assume that, for every $y\in\mathbb{F}_2^s$, the vectors $\phi_1(y)$ and $\phi_2(y)$ are linearly independent. If the 2-dimensional flats $\phi_3(y)+\langle\phi_1(y),\phi_2(y)\rangle$ (where y ranges over $\mathbb{F}_2^s$) are pairwisely disjoint, then $f_{\phi_1,\phi_2,\phi_3,g}$ is plateaued of amplitude 2^{r-1}.*

Proof. According to the hypothesis, for every $a\in\mathbb{F}_2^r$, there exists at most one vector $y\in\mathbb{F}_2^s$ such that a is included in $\phi_3(y)+<\phi_1(y),\phi_2(y)>$. According to Proposition 9, $\widehat{\chi_{f_{\phi_1,\phi_2,\phi_3,g}}}(a,b)$ equals then 0 or $\pm 2^{r-1}$ for every $a\in\mathbb{F}_2^r$ and every $b\in\mathbb{F}_2^s$.

Thus, from every family of 2^s pairwisely disjoint 2-dimensional flats of $\mathbb{F}_2^r$, Corollary 1 allows us to derive a plateaued function on $\mathbb{F}_2^r\times\mathbb{F}_2^s$ belonging to $\mathcal{Q}$: for every $y\in\mathbb{F}_2^s$, we choose one of these flats and we choose two distinct nonzero elements in its direction. Denote these two elements by $\phi_1(y)$ and $\phi_2(y)$ and denote by $\phi_3(y)$ any element of the same flat. The function $f_{\phi_1,\phi_2,\phi_3,g}$ satisfies then the hypothesis of Corollary 1. We denote by $\mathcal{Q}_1$ the class of those plateaued Boolean functions in $\mathcal{Q}$ constructed in this way.
Similarly, if for every $y\in\mathbb{F}_2^s$ the vectors $\phi_1(y)$ and $\phi_2(y)$ are linearly independent and if, denoting by F_a the set $\{y\in\mathbb{F}_2^s/a\in\phi_3(y)+\langle\phi_1(y),\phi_2(y)\rangle\}$, the cardinality of F_a equals 0 or 2 for every $a\in\mathbb{F}_2^r$, then $f_{\phi_1,\phi_2,\phi_3,g}$ is plateaued of amplitude 2^r.
This condition seems more difficult to satisfy than the condition obtained in Corollary 1. But since it leads to an amplitude of 2^r, we can relax the condition that the vectors $\phi_1(y)$ and $\phi_2(y)$ are linearly independent. We obtain :

Corollary 2. *Let $f_{\phi_1,\phi_2,\phi_3,g}$ be defined as in Definition 4. Assume that $\phi_2(y)$ is nonzero for every $y\in\mathbb{F}_2^s$. For every $a\in\mathbb{F}_2^r$, let F'_a be the set of all $y\in\mathbb{F}_2^s$ such* *that $\phi_1(y)$ and $\phi_2(y)$ are linearly independent and such that a belongs to the flat $\phi_3(y) + \langle\phi_1(y), \phi_2(y)\rangle$. Let F''_a be the set of all $y \in \mathbb{F}_2^s$ such that $\phi_1(y)$ and $\phi_2(y)$ are linearly dependent and $a = \phi_3(y) + \phi_1(y)$. If, for every $a \in \mathbb{F}_2^r$, the number $\#F'_a + 2\#F''_a$ equals 0 or 2, then $f_{\phi_1,\phi_2,\phi_3,g}$ is plateaued of amplitude 2^r.*

Proof. According to the hypothesis, for every $a \in \mathbb{F}_2^r$, either $F''_a = \emptyset$ and the size of F'_a equals 0 or 2, or $F'_a = \emptyset$ and F''_a has size at most 1. Thus, $f_{\phi_1,\phi_2,\phi_3,g}$ is plateaued of amplitude 2^r, according to Proposition 9.

Corollary 2 leads to a second construction of plateaued functions belonging to $\mathcal{Q}$. Let B and A be two disjoint subsets of $\mathbb{F}_2^r$ such that $\#B + 2\#A = 2^s$. Let $\mathcal{F}$ be a family of 2-dimensional flats included in A and such that, for every $a \in A$, there exist two 2-dimensional flats of $\mathcal{F}$ which contain a. We derive a plateaued function in the following way:
1. To every $a \in B$, we associate injectively $y \in \mathbb{F}_2^s$, we choose $\phi_2(y)$ in $\mathbb{F}_2^r \setminus \{0\}$, $\phi_1(y)$ in $\{0, \phi_2(y)\}$ and we set $\phi_3(y) = a + \phi_1(y)$.
2. For every $a \in A$, we consider the two flats F_1 and $\mathbb{F}_2$ in $\mathcal{F}$ which contain a and we choose injectively two vectors y_1 and y_2 among those of $\mathbb{F}_2^s$ which have not been chosen at step 1. We choose two distinct nonzero elements in the direction of F_1 (resp. $\mathbb{F}_2$). We denote these elements by $\phi_1(y_1)$ (resp. $\phi_1(y_2)$) and $\phi_2(y_1)$ (resp. $\phi_2(y_2)$). We denote by $\phi_3(y_1)$ (resp. $\phi_3(y_2)$) any element of the same flat. At the end of step 2, every $y \in \mathbb{F}_2^s$ has been affected a value for $\phi_1(y)$, $\phi_2(y)$ and $\phi_3(y)$ and the function $f_{\phi_1,\phi_2,\phi_3,g}$ satisfies the hypothesis of Corollary 2.
We call $\mathcal{Q}_2$ the class of those plateaued Boolean functions in $\mathcal{Q}$ constructed this way.

7 Study of the new classes $\mathcal{Q}_1$ and $\mathcal{Q}_2$

7.1 Algebraic degree and nonlinearity

In the next proposition, we denote by ϕ^j $(1 \le j \le r)$ the j-th component function of any function ϕ from $\mathbb{F}_2^s$ into $\mathbb{F}_2^r$.

Proposition 10. *The algebraic degree of the function $f_{\phi_1,\phi_2,\phi_3,g}$ of $\mathcal{Q}$ equals*

$$\max(\max_{i,j\le r} deg(\phi_1^j\phi_2^i \oplus \phi_1^i\phi_2^j) + 2\ ;\ \max_{i\le r} deg\left(\phi_3^i \oplus \phi_1^i\phi_2^i\right) + 1\ ;\ deg\ g). \tag{10}$$

and is upper bounded by $2 + s$.

The degree of $f_{\phi_1,\phi_2,\phi_3,g}$ equals $s + 2$ if and only if there exists a pair of distinct indices $\{i, j\}$ such that $deg(\phi_1^j\phi_2^i \oplus \phi_1^i\phi_2^j) = s$.

The nonlinearity of any Boolean function of $\mathcal{Q}_1$ (resp. $\mathcal{Q}_2$) is $2^{n-1} - 2^{r-2}$ (resp. $2^{n-1} - 2^{r-1}$), according to Equality (6) and to Corollaries 1 and 2.

7.2 Resiliency

Proposition 11. *Let $f_{\phi_1,\phi_2,\phi_3,g}$ be a Boolean function on $\mathbb{F}_2^r \times \mathbb{F}_2^s$ belonging to $\mathcal{Q}_1$ and let D_1 denote the set $\bigcup_{y\in\mathbb{F}_2^s}(\phi_3(y)+\langle\phi_1(y),\phi_2(y)\rangle)$. Let k be the minimum weight of the elements of D_1. Then, we have $k-1 \leq max\{t\in\mathbb{N}; \sum_{i=0}^{t}\binom{r}{i} \leq 2^r - 2^{s+2}\}$ and $f_{\phi_1,\phi_2,\phi_3,g}$ is exactly $(k-1)$-resilient.*

Proof. According to Proposition 9 and to Corollary 1, $\widehat{\chi_{f_{\phi_1,\phi_2,\phi_3,g}}}(a,b)$ equals $\pm 2^{r-1}$ if and only if $a\in D_1$. If (a,b) has weight smaller than or equal to $k-1$, then a has weight smaller than or equal to $k-1$ and does not belong to D_1: this implies $\widehat{\chi_{f_{\phi_1,\phi_2,\phi_3,g}}}(a,b) = 0$. Thus, $f_{\phi_1,\phi_2,\phi_3,g}$ is at least $(k-1)$-resilient. Moreover, suppose that $f_{\phi_1,\phi_2,\phi_3,g}$ has a resiliency order m larger than or equal to k, then $\widehat{\chi_{f_{\phi_1,\phi_2,\phi_3,g}}}(a,0) = 0$ for any $a\in\mathbb{F}_2^r$ having weight k wich contradicts the hypothesis on k and D_1. Since, by hypothesis, every word of weight smaller than or equal to $k-1$ belongs to D_1^c, and since D_1 is the union of 2^s pairwisely disjoint 2-dimensional flats, we deduce that $2^r - 2^{s+2} \geq \sum_{i=0}^{k-1}\binom{r}{i}$ and then $k-1 \leq max\{t\in\mathbb{N}; \sum_{i=0}^{t}\binom{r}{i} \leq 2^r - 2^{s+2}\}$.

As recalled at section 4, for every Boolean function f on $\mathbb{F}_2^n$, the nonlinearity N_f and the resiliency order m satisfy the relation $N_f \leq 2^{n-1} - 2^{m+1}$. When f is plateaued of amplitude 2^{r-1}, this relation implies that m is upper bounded by $r-3$. The functions whose nonlinearity and resiliency order equal $2^{n-1} - 2^{r-2}$ and $r-3$ respectively are good candidates to be used in stream ciphers and are proved to be necessarily plateaued by Sarkar and Maitra [34]. For this reason, it would be interesting if $\mathcal{Q}_1$ could contain such functions. The aim of the following corollary is to give a necessary condition, wich must be satisfied by any element of $\mathcal{Q}_1$ having 2^{r-1} for amplitude and $r-3$ for resiliency order.

Corollary 3. *If a Boolean function $f_{\phi_1,\phi_2,\phi_3,g}$ on $\mathbb{F}_2^r \times \mathbb{F}_2^s$ belonging to $\mathcal{Q}_1$ achieves maximum possible resiliency order $r-3$, then s is upper bounded by $\log_2(r^2+r+2)-3$ and thus have a degree upper bounded by $\log_2(r^2+r+2)-1 \leq \log_2(n^2+n+2)-1$.*

Proof. According to Proposition 11, if $f_{\phi_1,\phi_2,\phi_3,g}$ is $(r-3)$-resilient then $r-3$ is upper bounded $max\{t\in\mathbb{N}; \sum_{i=0}^{t}\binom{r}{i} \leq 2^r - 2^{s+2}\}$. We deduce that r satisfies $\sum_{i=0}^{r-3}\binom{r}{i} \leq 2^r - 2^{s+2}$. Since $\sum_{i=0}^{r-3}\binom{r}{i}$ equals $2^r - \binom{r}{0} - \binom{r}{1} - \binom{r}{2}$, we obtain $2^{s+2} \leq 1 + r + \frac{r(r-1)}{2}$ that is $s \leq \log_2(r^2+r+2)-3$.

The Walsh spectra of the elements of $\mathcal{Q}_2$ can be more complex than the Walsh spectrum of the elements of $\mathcal{Q}_1$. However, we shall see that their resiliency approximatively have the same behavior as the elements of $\mathcal{Q}_1$ with respect to their amplitude.

Proposition 12. *Let $f_{\phi_1,\phi_2,\phi_3,g}$ be a function in $\mathcal{Q}_2$. For every $a\in\mathbb{F}_2^r$, let F'_a and F''_a be the sets defined in Corollary 2. Let A denote the set $\{a\in\mathbb{F}_2^r; \#F'_a = 2\}$ and let B denote the set $\{a\in\mathbb{F}_2^r; \#F''_a = 1\}$. Let k and k' denote the minimum weights of the elements of $A\cup B$ and B respectively. Then $f_{\phi_1,\phi_2,\phi_3,g}$ is m-resilient with $\min(k'-1,k) \geq m \geq k-1$.*

Proof. Let D_2 denote the set $B \cup A$. According to Proposition 9 and to Corollary 2, if a is in D_2^c, then $\widehat{\chi_{f_{\phi_1,\phi_2,\phi_3,g}}}(a,b)$ equals zero. Thus, if (a,b) has weight smaller than or equal to $k-1$, then a has weight smaller than or equal to $k-1$ and belongs to D_2^c. This implies that $\widehat{\chi_{f_{\phi_1,\phi_2,\phi_3,g}}}(a,b) = 0$: we deduce that $f_{\phi_1,\phi_2,\phi_3,g}$ is at least $(k-1)$-resilient. We notice that, by definition, k and k' satisfy $k' \geq k$. Suppose that a is an element of B admitting k' for weight. Due to Proposition 9, for every $b \in \mathbb{F}_2^s$, $\widehat{\chi_{f_{\phi_1,\phi_2,\phi_3,g}}}(a,b) = \pm 2^r$. This implies that the resiliency of $f_{\phi_1,\phi_2,\phi_3,g}$ is upper bounded by $k'-1$.
Suppose that a is an element of A admitting k for Hamming weight and denote by y_1 and y_2 the two elements of $\mathbb{F}_2^s$ such that $a \in \phi_3(y_1) + < \phi_1(y_1), \phi_2(y_1) >$ and $a \in \phi_3(y_2) + < \phi_1(y_2), \phi_2(y_2) >$. Due to Proposition 9, the restriction of $\widehat{\chi_{f_{\phi_1,\phi_2,\phi_3,g}}}$ to $\{a\} \times \mathbb{F}_2^s$ is defined by one of the two following relations:
$\forall b \in \mathbb{F}_2^s$, $\frac{1}{2^{r-1}} \widehat{\chi_{f_{\phi_1,\phi_2,\phi_3,g}}}(a,b) = \pm[(-1)^{g(y_1)+b\cdot y_1} + (-1)^{g(y_2)+b\cdot y_2}] = \pm 2[b\cdot(y_1 + y_2) \oplus g(y_1) \oplus g(y_2) \oplus 1]$
$\forall b \in \mathbb{F}_2^s$, $\frac{1}{2^{r-1}} \widehat{\chi_{f_{\phi_1,\phi_2,\phi_3,g}}}(a,b) = \pm[(-1)^{g(y_1)+b\cdot y_1} - (-1)^{g(y_2)+b\cdot y_2}] = \pm 2[b\cdot(y_1 + y_2) \oplus g(y_1) \oplus g(y_2)]$
Since the linear function $b \mapsto b \cdot (y_1 + y_2)$ is not constant on the set $\{b \in \mathbb{F}_2^s; \omega_H(b) \leq 1\}$ when y_1 and y_2 are distinct, then there always exists an element $b \in \mathbb{F}_2^s$ of weight $\omega_H(b) \leq 1$ such that $\widehat{\chi_{f_{\phi_1,\phi_2,\phi_3,g}}}(a,b)$ is not null. This implies that the resiliency of $f_{\phi_1,\phi_2,\phi_3,g}$ is stricly upper bounded by $k+1$.

7.3 Constructions of Highly Nonlinear Resilient Functions from the class $\mathcal{Q}$

We have seen in the previous section, that the elements of $\mathcal{Q}_1$ and $\mathcal{Q}_2$ which achieve optimum tradeoff between nonlinearity and resiliency must have a low degree. We show now that it is possible to construct functions in $\mathcal{Q}$ with very good (but not optimal) characteristics.

Let r be any integer, we denote by $\overline{1}$ the vector in $\mathbb{F}_2^r$ having all its coordinates equal to 1. We construct functions in $\mathcal{Q}$ as follows: we choose two distinct elements e_1 and e_2 in the canonical basis of $\mathbb{F}_2^r$ (we recall that for every $i \leq r$, $\omega_H(e_i) = 1$) and we denote by F the flat $\overline{1} + < e_1, e_2 >$. We choose an integer t lower than or equal to $r-2$ and we denote by U_t the set $\{u \in < e_1, e_2 >^{\perp};\ \omega_H(u) \leq t\}$. By construction of the set U_t, $(u+F)_{u \in U_t}$ is a family of pairwisely disjoint 2-dimensional flats whose elements have weights greater than or equal to $r-t-2$. This family leads to construct Boolean functions in $\mathcal{Q}_1$ and $\mathcal{Q}_2$ such that the nonlinearity and the resiliency order can easily be computed.

Construction 1 Let s denote $\lfloor \log_2 \sum_{i=0}^{t} \binom{r-2}{i} \rfloor$. For every $y \in \mathbb{F}_2^s$ choose an element $u \in U_t$ and choose two distinct nonzero elements in $\{e_1, e_2, e_1 + e_2\}$ (i.e. nonzero elements in the direction of F). Denote these elements by $\phi_1(y)$ and $\phi_2(y)$ and denote by $\phi_3(y)$ any element of the flat $u + F$. For any choice of Boolean function g on $\mathbb{F}_2^s$, the function $f_{\phi_1,\phi_2,\phi_3,g}$ belongs to $\mathcal{Q}_1$. Denoting

$r+s$ by n, its nonlinearity and resiliency order equal $2^{n-1}-2^{r-2}$ and $r-t-3$ respectively (indeed the minimum weight of the elements of U_t+F equals $r-t-2$ and Propostion 11 permits to conclude).

In the following construction of highly nonlinear resilient functions from $\mathcal{Q}_2$, we choose the set B defined in Proposition 12 empty.

Construction 2 Let $s-1$ denote $\lfloor \log_2 \sum_{i=0}^{t} \binom{r-2}{i} \rfloor$. For every $u \in U_t$ such that $\omega_H(u) = t$, we choose injectively two vectors y_1 and y_2 in $\mathbb{F}_2^s$: we define $\phi_1(y_1) = \phi_2(y_2) = e_1$ and $\phi_2(y_1) = \phi_1(y_2) = e_2$; then we set $\phi_3(y_1) = \phi_3(y_2) = u + \overline{1}$. For every element u of U_t such that $\omega_H(u) < t$ we choose injectively two vectors y_1 and y_2 among those of $\mathbb{F}_2^s$ which have not been chosen at the previous step and we choose two pairs of distinct nonzero elements in $< e_1, e_2 >$: we denote these pairs by $(\phi_1(y_1), \phi_2(y_1))$ and by $(\phi_1(y_2), \phi_2(y_2))$; we denote by $\phi_3(y_1)$ and by $\phi_3(y_2)$ two elements of the same flat $u+F$. After defining a Boolean function g on $\mathbb{F}_2^s$ such that $g(y_1) = g(y_2) \oplus 1$ when $w_H[\phi_1(y_1)+\phi_2(y_1)+\phi_3(y_1)] = w_H[\phi_1(y_2)+\phi_2(y_2)+\phi_3(y_2)] = r-t-2$, we obtain a function $f_{\phi_1,\phi_2,\phi_3,g}$ in $\mathcal{Q}_2$ having $2^{n-1}-2^{r-1}$ for nonlinearity and having $r-t-2$ for resiliency.

References

1. E. Biham et A. Shamir, “Differential Cryptanalysis of DES-like Cryptosystems,” *Proceedings of CRYPTO' 90*, and *Journal of Cryptology*, Vol 4, No.1, 1991.
2. S. Botzas and P.V. Kumar, “Binary Sequences with Gold-Like Correlation but Larger Liner Span”, *IEEE Trans. on Information Theory*, vol. 40 no. 2, pp. 532-537, 1994.
3. P. Camion, C. Carlet, P. Charpin and N. Sendrier, “On Correlation-immune Functions”, *Advances in Cryptology - CRYPTO' 91, Lecture Notes in Computer Science*, Springer Verlag, v. 576, pp. 86-100, 1992.
4. P. Charpin and E. Pasalic. “On propagations characteristics of resilient functions”. *Advances in Cryptology - SAC 2002, Lecture Notes in Computer Science* to appear (2002).
5. A. Canteaut, C. Carlet, P. Charpin and C. Fontaine, ”Propagation characteristics and correlation-immunity of highly nonlinear Boolean functions”, *Advances in Cryptology - EUROCRYPT'2000, Lecture Notes in Computer Science*, Springer Verlag, v.1807, pp.507-522, 2000.
6. A. Canteaut, C. Carlet, P. Charpin and C. Fontaine. “On cryptographic properties of the cosets of $R(1,m)$”. *IEEE Transactions on Information Theory* Vol. 47, no 4, pp. 1494-1513, 2001.
7. A. Canteaut, P. Charpin and H. Dobbertin. “Binary m-sequences with three-valued crosscorrelation: a proof of Welch's conjecture”. *IEEE Transactions on Information Theory* Vol. 46, pp. 4-8, 2000.
8. A. Canteaut, P. Charpin and H. Dobbertin. “Weight divisibility of cyclic codes, highly nonlinear functions on F_{2^m}, and crosscorrelation of maximum-length sequences”, *SIAM Journal of Discrete Mathematics*, v. 13(1), pp. 105-138, 2000.
9. C. Carlet, “Partially-bent functions”, *Proceedings of CRYPTO' 92, Advances in Cryptology*, Lecture Notes in Computer Science 740, Springer Verlag, 280-291, 1993.

10. C. Carlet, “Two new classes of bent functions”, *Advances in Cryptology - Eurocrypt’93, Lecture Notes in Computer Science*, Ed. T. Helleseth, Springer-Verlag, v.765, pp.77-101, 1994.
11. C. Carlet, “Generalized Partial Spreads”, *IEEE Transactions on Information Theory*, vol 41, number 5, 1482-1487, 1995.
12. C. Carlet. “A larger Class of Cryptographic Boolean Functions via a Study of the Maiorana-McFarland Construction”. *Advances in Cryptology - CRYPT0 2002, number 2442 in Lecture Notes in Computer Science*, pp. 549-564, 2002.
13. C. Carlet and P. Sarkar, “Spectral Domain Analysis of Correlation Immune and Resilient Boolean Functions”, *Finite Fields and Their Applications 8*, pp.120-130, 2002.
14. C. Carlet and Y. Tarannikov, “Covering sequences of Boolean functions and their cryptographic significance”, *Designs Codes and Cryptography, 25*, v.25, pp. 263-279, 2002.
15. 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*, Springer-Verlag, v.2332, pp. 518-533, 2002.
16. T.W. Cusik and H. Dobbertin, “Some new three-valued crosscorrelation functions for binary m-sequences”, *IEEE Transaction of Information Theory*, vol. 42, pp. 1238-1240, 1996.
17. J. F. Dillon, “Elementary Hadamard Difference sets, *Phd Thesis, University of Maryland*, 1974.
18. H. Dobbertin, “Constructions of bent functions and balanced Boolean functions with high nonlinearity”, *Fast Software Encryption, Lecture Notes in Computer Science*, Ed. B. Preenel, Springer Verlag, 1994, v. 1008, pp.61-74.
19. R. Gold, “Maximal recursive sequences with 3-valued recursive cross-correlation functions”, *IEEE Transaction of Information Theory*, v. 14, pp. 154-156, 1968.
20. T. Helleseth, “Some results about the cross-correlation function between two maximal linear sequences”, *Discrete Mathematics*, v.16, pp. 209-232, 1976.
21. T. Helleseth, “Correlation of m-Sequences and Related Topics”, *In Sequences and their Qpplicqtions SETA 98*, pp. 49-66, 1999.
22. T. Helleseth and P. Vijay Kumar, *Sequences with low correlation* in Handbook of Coding Theory, ed. V. Pless and W.C. Huffman, pp.1765–1855, Elsevier, Amsterdam, 1998.
23. T. Helleseth, H. Martinsen, “Sequences with ideal autocorrelation and Difference sets”, *Proceedings of International Meeting on Coding Theory and Cryptography*, Septembre 1999.
24. H.D.L. Hollmann and Q. Xiang, “A proof of the Welch and Niho conjectures on crosscorrelation of binary m-sequences”, *Finite Fields and Their applications*, v. 7, 2001.
25. L.R. Knudsen. *Truncated and higher order differentials.* Fast Software Encryption, Second International Workshop, Lecture Notes in Computer Science, n 1008. pp. 196–211. – Springer-Verlag, 1995.
26. X. Lai. “Higher order derivatives and differential cryptanalysis”. *Proc. Symposium on Communication, Coding and Cryptography, in honor of J. L. Massey on the occasion of his 60’th birthday*, 1994.
27. M. Matsui, “Linear cryptanalysis method for DES cipher,” *Advances in Cryptology - EUROCRYPT’93, number 765 in Lecture Notes in Computer Science. Springer-Verlag*, pp. 386–397, 1994.

28. P. Sarkar and S. Maitra, "Nonlinearity bounds and construction pf resilient Boolean functions", *Advances in Cryptology - EUROCRYPT' 2000, Lecture Notes in Computer Science*, Springer Verlag, 1994, v. 1880, pp.512-532.
29. R. L. McFarland, "A family of noncyclic difference sets", *Journal of Combinatorial Theory*, number 15, pp. 1-10, 1973.
30. E. Pasalic, S. Maitra, T. Johanson and P. Sarkar, "New Constructions of Resilient and Correlation Immune Boolean Functions Achieving Upper Bound on Nonlinearity", *Workshop on Coding and Cryptography*, Electronic Notes in Discrete Mathematics, Ed. Elsevier, 2001.
31. V.S. Pless and W.C. Huffman, "Handbook of coding theory", Elsevier, Amsterdam, 1998.
32. B. Preneel, W. Van Leekwijck, L. Van Linden, R. Govaerts and J. Vandevalle. Propagation characteristics of Boolean functions, *Advances in Cryptology, EUROCRYPT'90, Lecture Notes in Computer Sciences, Springer Verlag* n° 473, pp. 161-173, 1991.
33. P. Sarkar, S. Maitra, "Constructions of nonlinear Boolean functions with important cryptographic properties", *Advanced in Cryptology: Eurocrypt 2000, Proceedings, Lecture Notes in Computer Science*, Springer Verlag, v. 1807, pp. 485-506, 2000.
34. P. Sarkar, S. Maitra, "Nonlinearity bounds and constructions of resilient Boolean functions", *Advanced in Cryptology: Crypto 2000, Proceedings, Lecture Notes in Computer Science*, v. 1880, pp. 515-532, 2000.
35. Mac Williams, F. J. and N. J. Sloane (1977). *The theory of error-correcting codes*, Amsterdam, North Holland.
36. Y. Tarannikov, "On resilient Boolean functions with maximum nonlinearity", *Proceedings of INDOCRYPT 2000, Lecture Notes in Computer Science*, Ed. Bimal K. Roy and Eiji Okamoto, Springer Verlag, v. 1977, pp.19-30, 2000.
37. G.-Z. Xiao, C. Ding and W. Shan. *The stability theory of stream ciphers*, vol. LNCS 561, Springer Verlag, 1991.
38. Xiao Guo-Zhen and J. L. Massey. "A Spectral Characterization of Correlation-Immune Combining Functions". *IEEE Trans. Inf. Theory*, Vol IT 34, n° 3 (1988), pp. 569-571.
39. Y. Zheng and X. Zhang, "Improved upper bound on the nonlinearity of high order correlation immune functions", *Proceedings of Selected Areas in Cryptography 2000, Lecture Notes in Computer Science*, Springer Verlag, 2001, v.2012, pp. 262-274, 2000.
40. Y. Zheng and X. M. Zhang, "Plateaued functions", *Advances in Cryptology - ICICS'99, Lecture Notes in Computer Science*, Heidelberg, Ed., Springer-Verlag, v.1726, pages 284-300, 1999.
41. Y. Zheng X. M. Zhang, "Improved upper bound on the nonlinearity of high order correlation immune functions", *Selected Areas in Cryptography, 7th Annual International Workshop, SAC 2000, Lecture Notes in Computer Science*, Springer-Verlag, v. 2012, pp.264-274, 2001.

A Other constructions of plateaued functions

A.1 Secondary constructions

A first construction is given in [17]. Let $g : \mathbb{F}_2^r \mapsto \mathbb{F}_2$ and $h : \mathbb{F}_2^s \mapsto \mathbb{F}_2$ be two plateaued functions. The function f defined on $\mathbb{F}_2^{r+s}$ by $f(x, y) = g(x) \oplus h(y)$

is plateaued on $\mathbb{F}_2^{r+s}$. Indeed we have

$$\widehat{\chi_f}(a,b) = \widehat{\chi_g}(a) \times \widehat{\chi_h}(b).$$

But such function f does not have good cryptographic properties. For instance, the degree of f is upper bounded by $\max(deg\ g, deg\ h)$. And J. Dillon himself says that the "decomposable" functions this construction produces are not satisfactory.

Two other secondary constructions of plateaued functions can be adapted from classical secondary constructions of resilient functions (cf. [3, 30, 36]).

Proposition 13. *1. Let g and h be two plateaued Boolean functions on $\mathbb{F}_2^n$ of the same amplitude 2^r.*
The functions defined by $f(x_1, \cdots, x_n, x_{n+1}) = g(x_1, \cdots, x_{n-1}, x_n \oplus x_{n+1})$ and $f'(x_1, \cdots, x_n, x_{n+1}) = g(x_1, \cdots, x_{n-1}, x_n \oplus x_{n+1}) \oplus x_n$ are plateaued of amplitude 2^{r+1} on $\mathbb{F}_2^{n+1}$. If g is mth-order correlation immune (resp. m-resilient) then f is mth-order correlation immune (resp. m-resilient) and f' is m-resilient. If $\widehat{\chi_g}(a_1, \ldots, a_{n-1}, 1) = 0$ for every $((a_1, \ldots, a_{n-1})$, then f' is $(m+1)$-resilient.
2. If for all $a \in \mathbb{F}_2^n$, the numbers $\widehat{\chi_g}(a)$ and $\widehat{\chi_h}(a)$ either are both null or are both nonzero, then the function $f''(x_1, \cdots, x_n, x_{n+1}) = (x_{n+1} \oplus 1)g(x_1, \cdots, x_n) \oplus x_{n+1}h(x_1, \cdots, x_n)$ is plateaued of amplitude 2^{r+1} on $\mathbb{F}_2^{n+1}$.
If for all $a \in \mathbb{F}_2^n$, at least one of the numbers $\widehat{\chi_g}(a)$ and $\widehat{\chi_h}(a)$ is null, then the function $f''(x_1, \cdots, x_n, x_{n+1})$ is plateaued of amplitude 2^r on $\mathbb{F}_2^{n+1}$.
If g and h are m-resilient then f'' is m-resilient.

Proof. 1. For every $(a_1, \ldots, a_{n+1}) \in \mathbb{F}_2^{n+1}$, we have

$$\widehat{\chi_f}(a_1, \ldots, a_{n+1}) = \sum_{(x_1,\ldots,x_{n+1}) \in \mathbb{F}_2^{n+1}} (-1)^{\bigoplus_{i=1}^{n+1} a_i x_i \oplus g(x_1,\ldots,x_{n-1},x_n \oplus x_{n+1})} =$$

$$\sum_{(x_1,\ldots,x_{n+1}) \in \mathbb{F}_2^{n+1}} (-1)^{\bigoplus_{i=1}^{n-1} a_i x_i \oplus a_n(x_n \oplus x_{n+1}) \oplus a_{n+1}x_{n+1} \oplus g(x_1,\ldots,x_n)} =$$

$$\sum_{(x_1,\ldots,x_{n+1}) \in \mathbb{F}_2^{n+1}} (-1)^{\bigoplus_{i=1}^{n} a_i x_i \oplus (a_n \oplus a_{n+1})x_{n+1} \oplus g(x_1,\ldots,x_n)}.$$

Thus, $\widehat{\chi_f}(a_1, \ldots, a_{n+1})$ equals $2\widehat{\chi_g}(a_1, \ldots, a_n)$ if $a_n = a_{n+1}$ and 0 otherwise. Consequently, $\widehat{\chi_{f'}}(a_1, \ldots, a_{n+1})$ equals $2\widehat{\chi_g}(a_1, \ldots, a_n)$ if $a_n = a_{n+1} \oplus 1$ and 0 otherwise. The consequences are then straightforward.
2. For every $(a_1, \ldots, a_{n+1}) \in \mathbb{F}_2^{n+1}$, we have $\widehat{\chi_{f''}}(a_1, \ldots, a_{n+1}) = \widehat{\chi_g}(a_1, \ldots, a_n) + (-1)^{a_{n+1}}\widehat{\chi_h}(a_1, \ldots, a_n)$. Thus, $\widehat{\chi_{f''}}(a_1, \ldots, a_{n+1})$ equals 0 or $\pm 2^{r+1}$ (resp. $\pm 2^r$) thanks to the condition on $\widehat{\chi_g}$ and $\widehat{\chi_h}$.

The classes of Boolean functions these constructions permit to build are small. Moreover, f and f' have the nonzero linear structure $(0, \ldots, 0, 1, 1)$ which can be used to attack the system in which it is implemented.

A.2 Plateaued Functions from Sequence Designs

An important problem in sequence designs is to study the cross-correlation between a binary maximum-length sequence (called m-sequence) and its decimation by an integer d. Let $s\left[1\right] = \left(s_0, s_1, s_2, \ldots, s_j, \ldots\right)$ denote a binary m-sequence of length $2^n - 1$ and let $s\left[d\right] = \left(s_0, s_d, s_{2d}, \ldots, s_{jd}, \ldots\right)$ denote its decimation by an integer d, co-prime with $2^n - 1$. We denote by $C_d\left(t\right)$ the cross-correlation function between the m-sequences $s\left[1\right]$ and $s\left[d\right]$, defined by $C_d\left(t\right) = \sum_{j=0}^{2^n-2} \left(-1\right)^{s_{jd}+s_{j+t}}$ for $t = 0, 1, \ldots, 2^n - 2$. These cross-correlations are known to take at least three different values. The special case when exactly three values occur was the subject of many works [7, 16, 19, 20].

The study of binary sequences can be related to Boolean functions through their trace representation. Let $Tr : F_{2^n} \mapsto \mathbb{F}_2$ denote the usual trace function on the Galois Field F_{2^n} and let α be a primitive element of F_{2^n}. Since the cross-correlation spectrum only depends on d and not on the choice of the m-sequence $s\left[1\right]$, we may assume with no loss of generality that $s\left[1\right]$ is given by $s_j = Tr\left(\alpha^j\right)$. Then to each sequence obtained by decimating $s\left[1\right]$ by an integer d, one can associate its trace representation i.e. the function $f_d : x \mapsto Tr\left(x^d\right)$. When t varies in $\{0, \cdots, 2^n - 2\}$, the functions associated to the sequences s_{j+t} are the functions of the form $x \mapsto Tr\left(\beta x\right)$ where $\beta = \alpha^t$ that is all the non-zero linear functions on F_{2^n}. The Walsh transform of the function f_d and the cross-correlation C_d of $s\left[1\right]$ are connected through the relation:

$$\widehat{\chi_{f_d}}\left(u\right) = C_d\left(t\right) + 1 \tag{11}$$

where $u = \alpha^t$ is in $F_{2^n}^*$

The Boolean function f_d is plateaued on F_{2^n} if and only if the associate sequence has a three-valued cross-correlation function.

In [22], T. Helleseth and P. V. Kumar give the list of all the values d known at that time for which C_d is three-valued. We recall here this list and add the two constructions presented in [7] and [24]:

1. $d = 2^k + 1$, $n/gcd\left(n, k\right)$ odd,
2. $d = 2^{2k} - 2^k + 1$, $n/gcd\left(n, k\right)$ odd,
3. $d = 2^{\frac{n}{2}} + 2^{\frac{n+2}{4}} + 1$, $n \equiv 2\left(mod\ 4\right)$,
4. $d = 2^{\frac{n+2}{2}} + 3$, $n \equiv 2\left(mod\ 4\right)$,
5. $d = 2^{\frac{n-1}{2}} + 3$, n odd,
6. $$d = \begin{cases} 2^{\frac{n-1}{2}} + 2^{\frac{n-1}{4}} - 1 \text{ if } n \equiv 1\left(mod\ 4\right) \\ 2^{\frac{n-1}{2}} + 2^{\frac{3n-1}{4}} - 1 \text{ if } n \equiv 3\left(mod\ 4\right) \end{cases}$$

From cryptographic viewpoint, these classes are too small to provide satisfaction. In the case 1, introduced by Gold [19], the algebraic normal form has degree 2 and the constructed trace function belong to $R\left(2, n\right)$ which was already known to be a set of plateaued functions. In the other cases respectively found by Kasami, Cusick and Dobbertin [16], Canteaut-Charpin-Dobbertin [7] and Hollmann and Xiang [24], the algebraic degree of the functions is greater than 2 but it equals 3 in the cases 4 and 5. It is a hard problem to test cryptographic properties as resiliency on these functions and more generally on Boolean functions defined on the field F_{2^n}.