CRYPTOGRAPHICAL BOOLEAN FUNCTIONS CONSTRUCTION FROM LINEAR CODES

Philippe Guillot[1]

Abstract. This paper presents an extension of the Maiorana-McFarland method for building Boolean functions with good cryptographic properties.

The original Maiorana-McFarland construction was proposed to design bent functions. Then, it was extended in [1] to build highly nonlinear resilient functions.

The classical construction splits the set of variables into two separate subsets. There, is proposed a decomposition of the whole working space into two complementary vector spaces. One of these spaces is considered as a linear code and its parameters assigns cryptographic properties to the constructed Boolean function.

The cryptographical properties we are interested in are nonlinearity, resiliency and propagation properties.

The obtained functions are linearly equivalent to those constructed by the traditional way. Thus, no improvement for affine invariant parameters such as nonlinearity is expected. On the other hand, for non affine invariant cryptographic parameters such as resiliency order or propagation order, better values are obtained.

1. Motivation

Cryptographic algorithms design is still based on confusion and diffusion principles stated by Shannon in 1949 (see [6]). Diffusion means that a bit change in the key is propagated in the whole ciphertext. It is performed by linear transformations. Confusion means that the relationship between the key, the plaintext and the

[1] Université Paris 8. email: philippe.guillot@univ-paris8.fr

ciphertext is complex and involved. It is performed by nonlinear transformations and mostly implemented as Boolean functions.

The nonlinearity may be defined in at least four ways.

First, a Boolean function is nonlinear if it is not correlated to any affine function. This is the correlation criterion. It means that the function is far from the set of affine functions.

Nonlinearity may also be defined through propagation properties. If some variables are changed, is the value changed too ? If the function has a linear structure, then the answer is always predictable : yes or no depending on which variables are changed. For cryptographic oriented functions, the answer should be unpredictable.

Third, a linear function is expressed as a n-variable polynomial of degree one. A nonlinear function should be expressed as a polynomial of degree as high as possible.

Finally, a linear function is simple. A nonlinear function is expected to be complex. The complexity may be measured by several ways : number of gates to implement it, number of nodes in a Binary Decision Diagram, and so on.

The designer has to deal with all these criteria together. It is rarely possible to optimize all of them. We are mainly interested in the sequel in a compromise between correlation and propagation criteria.

2. Spectral Analysis

The mathematical tool to explore nonlinearity of boolean functions consists in two objects: the Walsh transform and the autocorrelation function. In this section, we recall basic results and definitions which will be used in the sequel.

Let n be any integer ≥ 2 and $\mathbb{F}_2^n$ be the n-dimensional vector space over the field $\mathbb{F}_2$. For any vectors $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ in $\mathbb{F}_2^n$, the inner product of x and y is $x \cdot y = x_1 y_1 + \cdots + x_n y_n \in \mathbb{F}_2$.

A Boolean function over $\mathbb{F}_2^n$ is a mapping $\mathbb{F}_2^n \to \mathbb{F}_2$.

The Fourier transform of a Boolean function f is by definition the real valued function $\widehat{f}$ defined as

$$\forall u \in \mathbb{F}_2^n \quad \widehat{f}(u) = \sum_{x \in \mathbb{F}_2^n} f(x)(-1)^{u \cdot x}.$$

The Fourier transform of the sign function $f_\chi = (-1)^f = 1-2f$ is called the Walsh transform of f:

$$\forall u \in \mathbb{F}_2^n \quad \widehat{f_\chi}(u) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+u\cdot x}.$$

For all $u \in \mathbb{F}_2^n$, the Wash transform value $\widehat{f_\chi}(u)$ is the number of times $f(x)$ equals $u \cdot x$ minus the number of time it differs. Thus $\widehat{f_\chi}(u)$ measures the correlation between f and the linear form $\lambda_u : x \mapsto u \cdot x$. The function f is statistically independent from λ_u if and only if $\widehat{f_\chi}(u) = 0$. In particular, f is balanced if and only if $\widehat{f_\chi}(0) = 0$.

The power of this tool is based on the orthogonality relation of the so called Walsh functions $\chi_u : x \mapsto (-1)^{u\cdot x}$:

$$\begin{aligned} \forall (u,v) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \quad \sum_{x \in \mathbb{F}_2^n} \chi_u(x)\chi_v(x) &= \sum_{x \in \mathbb{F}_2^n} (-1)^{(u+v)\cdot x} \\ &= \begin{cases} 2^n & \text{if } u = v; \\ 0 & \text{elsewhere.} \end{cases} \end{aligned}$$

For any p-dimensional vector subspace E of $\mathbb{F}_2^n$, the dual of E, denoted $E^\perp$, is the $(n-p)$-dimensional vector space of linear forms that vanish on E.

$$E^\perp = \{u \in \mathbb{F}_2^n \mid \forall x \in E,\ u \cdot x = 0\}.$$

If f is defined on a vector subspace E of $\mathbb{F}_2^n$, the expression of the Fourier transform of f is given by

$$\widehat{f}(u) = \sum_{x \in E} f(x)(-1)^{u\cdot x}.$$

A first glance, $\widehat{f}$ is defined over the whole space $\mathbb{F}_2^n$, but in fact $\widehat{f}(u)$ remains unchanged when u is added to any element of $E^\perp$. In other word, $\widehat{f}$ is constant on any coset of $E^\perp$. Thus, $\widehat{f}$ may be considered as defined over the quotient space $\mathbb{F}_2^n/E^\perp$.

For convenience and easier computation, it may be useful to consider a complementary space F of E, *i.e.* such that $\mathbb{F}_2^n = E \oplus F$. The dual spaces $E^\perp$ and $F^\perp$ are complementary too and the quotient space $\mathbb{F}_2^n/E^\perp$ is isomorphic to $F^\perp$. Thus, $\widehat{f}$ is considered as defined on $F^\perp$.

The second object of the spectral analysis is the autocorrelation function. For any Boolean function f over $\mathbb{F}_2^n$, the autocorrelation function of f, denoted r_f is by definition:

$$r_f : \begin{array}{ccc} \mathbb{F}_2^n & \to & \mathbb{R} \\ u & \mapsto & \displaystyle\sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)+f(x+u)} \end{array} .$$

The value $r_f(u)$ is the number of time $f(x)$ equals $f(x+u)$ minus the number of times it differs. Thus it measure the avalanche effect of vector u.

If $r_f(u) = 0$ then the value of f is unpredictable when the variables x_i such that $u_i = 1$ are changed.

If $r_f(u) = \pm 2^n$ then the function $x \mapsto f(x) + f(x + u)$ is constant. In this case, the vector u is called a linear structure for f. The set of linear structures over $\mathbb{F}_2^n$ is the subset of Boolean function that do have a linear structure. The set of affine functions over $\mathbb{F}_2^n$ is a subset of the set of linear structures (see [4]).

3. Cryptographic criteria

In a symmetric algorithm, the Boolean function is in charge of the confusion property. Thus, it has to be highly nonlinear. The nonlinearity is measured by the distance $\delta(f)$ of the Boolean function f from the set of affine functions. It can be expressed by mean of the Walsh transform (see [4]) :

$$\delta(f) = 2^{n-1} - \frac{1}{2} \max_{u\in\mathbb{F}_2^n} \big(|\widehat{f_\chi}(u)|\big).$$

The lower is the greatest magnitude of the Walsh transform, the further is the function from the set of affine functions.

Another nonlinearity measure is given by the distance $\sigma(f)$ of the Boolean function f from the set of linear structures. It can be expressed by mean of the autocorrelation function (see [4]) :

$$\sigma(f) = 2^{n-2} - \frac{1}{4} \max_{u\in\mathbb{F}_2^n\setminus\{0\}} \big(|r_f(u)|\big).$$

Similarly, the lower is the greatest magnitude of the autocorrelation function on nonzero vectors, the further is the function from the set of linear structures.

The cryptographer should minimize maximum magnitude of both the Walsh transform and the autocorrelation function in order to design non linear functions with good cryptographic properties.

Both δ and σ are affine invariants, *i.e.* the values $\delta(f)$ and $\sigma(f)$ remain unchanged if f is composed with any invertible affine mapping on $\mathbb{F}_2^n$.

A Boolean function is said to be k-resilient, if the knowledge of any k variables does not provide any statistical information on the value of f. A function is 0-resilient means that it is balanced. Resiliency has a nice characterization by mean of the Walsh transform (see [7]).

Proposition 3.1. *A Boolean function f over $\mathbb{F}_2^n$ is k-resilient if and only if for any vector $u \in \mathbb{F}_2^n$ of weight less than or equal to k, its Walsh transform vanishes at vector u, i.e. $\widehat{f_\chi}(u) = 0$.*

A Boolean function satisfies the propagation criterion at order k, which is denoted $PC(k)$, if changing any k variables does not allow to guess if the value of f changes or not. Similarly, propagation criterion has a characterization by mean of the autocorrelation function. The following proposition is a straightforward consequence of the definition.

Proposition 3.2. *A Boolean function f over $\mathbb{F}_2^n$ satisfies $PC(k)$ if and only if for any nonzero vector $u \in \mathbb{F}_2^n \setminus \{0\}$ of weight less than or equal to k, its autocorrelation function vanishes at vector u, i.e. $r_f(u) = 0$.*

4. The Maiorana-McFarland Construction

The Maiorana-McFarland construction was originally designed to build bent function (see [3]). It has been extended in [1] to build resilient functions. Here, we extend it again according to a technique similar to those proposed in [2].

Let $n \geq 2$ be an integer and $\mathbb{F}_2^n = E \oplus F$ a decomposition into two complementary vector subspaces : E of dimension p and F of dimension $q = n - p$.

For any mapping $\pi : E \to \mathbb{F}_2^n$ and any mapping $h : E \to \mathbb{F}_2$ the Maiorana-McFarland construction defines a Boolean function f as follows :

$$f : \begin{array}{ccc} E \oplus F & \to & \mathbb{F}_2 \\ x+y & \mapsto & \pi(x)\cdot y + h(x) \end{array} .$$

The mapping π is defined onto $\mathbb{F}_2^n$, but as $\pi(x)$ is only involved by an inner product with an element of F, the value of f is unchanged when $\pi(x)$ is translated by any vector in $F^\perp$. Thus, π may be considered to be defined onto the quotient space $\mathbb{F}_2^n/F^\perp$, which is isomorphic to $E^\perp$.

The traditional definition appears to be a particular case of this definition by considering $E = \{(x_1, \ldots, x_n) \in \mathbb{F}_2^n \mid x_{p+1} = 0, \ldots, x_n = 0\}$ and $F = \{(x_1, \ldots, x_n) \in \mathbb{F}_2^n \mid x_1 = 0, \ldots, x_p = 0\}$.

Conversely, any linear equivalent of the classical Maiorana-McFarland construction may be obtained by the way presented here.

In order to establish the correlation properties of the function f, the following proposition expresses the Walsh transform.

Proposition 4.1. *For any $w \in \mathbb{F}_2^n$, let $w = u + v$ be the unique decomposition of w in the direct sum $E^\perp \oplus F^\perp$ with $u \in E^\perp$ and $v \in F^\perp$.*

$$\widehat{f_\chi}(u+v) = 2^q \sum_{x \in \pi^{-1}(u)} (-1)^{h(x)+v\cdot x} \tag{1}$$

Proof. By definition, for any $w \in \mathbb{F}_2^n$,

$$\begin{aligned} \widehat{f_\chi}(w) &= \sum_{(x,y)\in E\times F} (-1)^{\pi(x)\cdot y + h(x) + w\cdot(x+y)} \\ &= \sum_{x\in E} (-1)^{h(x)+w\cdot x} \sum_{y\in F} (-1)^{(\pi(x)+w)\cdot y} \end{aligned}$$

The latter sum equals $|F| = 2^q$ if $\pi(x) + w \in F^\perp$ and 0 elsewhere. Thus, the only nonzero terms in the above sum are those such as $\pi(x) \in w + F^\perp$. As, $x \in E$ in the sum, $w \cdot x = u \cdot x + v \cdot x = v \cdot x$. Moreover, $\pi(x) \in w + F^\perp \Leftrightarrow x \in \pi^{-1}(u)$ and the result holds. □

In order to study resiliency, we are interested in the case where the Walsh transform vanishes. This occurs in two cases : either if $\pi^{-1}(u)$ is empty or if the function $x \mapsto h(x) + v \cdot x$ is balanced on the subset $\pi^{-1}(u)$ of E. This latter property is not so easy to check in general. An interesting particular case is when $\pi^{-1}(u)$ is an affine subspace of E.

Proposition 4.2. *Let u be an element of $E^\perp$, if the preimage $\pi^{-1}(u)$ is the affine subspace of E defined by direction V_u and element x_u, then, for all $v \in F^\perp$,*

$$\widehat{f_\chi}(u+v) = 2^q(-1)^{v\cdot x_u}\widehat{(h_u)_\chi}(v),$$

where h_u denotes the Boolean function on V_n defined by $t \mapsto h(t+x_u)$.

Proof. Set $x = t + x_u$ in the sum of expression (1) and the result holds. □

In order to establish propagation properties of the function f, the following proposition expresses the autocorrelation function.

Proposition 4.3. *For any $z \in \mathbb{F}_2^n$, let $z = x + y$ the unique decomposition of z in the direct sum $E \oplus F$ with $x \in E$ and $y \in F$.*

$$r_f(x+y) = 2^q \sum_{t\in E|\pi(t)+\pi(t+x)\in F^\perp} (-1)^{h(t)+h(t+x)+\pi(t)\cdot y}.$$

Proof.

$$\begin{aligned} r_f(x+y) &= \sum_{(t,s)\in E\times F} (-1)^{\pi(t)\cdot s+h(t)+\pi(t+x)\cdot(s+y)+h(t+x)} \\ &= \sum_{t\in E}(-1)^{h(t)+h(t+x)+\pi(t+x)\cdot y}\sum_{s\in F}(-1)^{(\pi(t)+\pi(t+x))\cdot s} \end{aligned}$$

The latter sum equals $|F| = 2^q$ if $\pi(t)$ and $\pi(t+x)$ belong to the same $F^\perp$–coset, and equals 0 elsewhere. Thus, the only nonzero terms are those for which $\pi(t) + \pi(t+x) \in F^\perp$. □

If $x = 0$, then any t in E satisfies the condition $\pi(t)+\pi(t+x) = 0 \in F^\perp$. Thus for any $y \in F$,

$$r_f(y) = 2^q \sum_{t\in E}(-1)^{\pi(t)\cdot y}.$$

Let $u = \pi(t)$. For any y in F,

$$r_f(y) = 2^q \sum_{u\in E^\perp} \psi(u)(-1)^{u\cdot y} = 2^q\widehat{\psi}(y), \tag{2}$$

where, for any $u \in E^\perp$, the value $\psi(u)$ is the number of elements of the preimage $\pi^{-1}(u)$.

5. Practical constructions

5.1. π is one-to-one

We assume in this section, that for any $u \in E^\perp$, the preimage $\pi^{-1}(u)$ contains at most one element. This is possible only if $p \leq q$. If this preimage is nonempty, then the vector space V_u of proposition 4.1 is always the null vector space and $\widehat{(h_u)_\chi}(u) = \pm 1$. Consequently, for all $(u, v) \in E^\perp \times F^\perp$,

$$\widehat{f_\chi}(u+v) = \begin{cases} \pm 2^q & \text{if } \pi^{-1}(u) \neq \emptyset; \\ 0 & \text{elsewhere.} \end{cases} \tag{3}$$

The assumption on π implies that for all t and x in E,

$$\pi(t) + \pi(t+x) \in F^\perp \iff x = 0.$$

From proposition 4.3, if $x \neq 0$ then $r_f(x+y) = 0$. Finally, from relation (2), for all $(x, y) \in E \times F$,

$$r_f(x+y) = \begin{cases} 2^q \widehat{\varphi_{\pi(E)}}(y) & \text{if } x = 0; \\ 0 & \text{elsewhere,} \end{cases} \tag{4}$$

where $\varphi_{\pi(E)}$ denotes the indicator of the image $\pi(E)$ in $E^\perp$.

From relation (3), the following correlation properties of f are deduced:

- f is balanced if and only if $\widehat{f_\chi}(0) = 0$, *i.e.* $0 \notin \pi(E)$. This requires in particular $p < q$.
- If for all $x \in E$, the coset leaders of $\pi(x) + F^\perp$, which are by definition the element of lowest weight, have weight at least k, then $\widehat{f_\chi}$ vanishes for all vectors of weight $< k$. Therefore, f is $(k-1)$-resilient.
- As $\widehat{f_\chi}$ has constant magnitude equal to 2^q, the nonlinearity of f is $\delta(f) = 2^{n-1} - 2^{q-1}$.

From relation (4), the following propagation properties of f are deduced:

- As $r_f(z)$ is nonzero only for $z \in F$, if F has minimum distance d, then f satisfies the propagation criterion $PC(d-1)$.

- The distance from f to the set of linear structures depends on the nonlinearity of the $\pi(E)$ indicator $\varphi_{\pi(E)}$. Namely,

$$\sigma(f) = 2^{n-2} - 2^{q-2} \max_{u \in E^{\perp} \setminus \{0\}} |\widehat{\varphi_{\pi(E)}}(u)|.$$

In particular, if $\pi(E)$ spans the whole space $\mathbb{F}_2^n$, then no nonzero linear form is constant over $\pi(E)$ and f is non degenerate in the sense that it is not affinely equivalent to a Boolean function of strictly less variables.

Relation (4) shows that the propagation order may be increased if $\varphi_{\pi(E)}$ is chosen resilient. But on the other hand, due to the Sarkar-Maitra's bound (see [5]), this increases the greatest magnitude of the autocorrelation function and thus decreases the distance from the set of linear structures.

Note that the cryptographic properties of f only depend on the properties of the vector space F and of the image $\pi(E)$. Once the image $\pi(E)$ and the vector space chosen, choice of permutation π and Boolean function h lead to $2^p! \times 2^{2^p}$ different functions with similar cryptographic properties.

By an appropriate choice of π or h, the algebraic degree of f can be increased to the maximum value, which equals p.

Unfortunately, the following proposition states that, when π is one-to-one, no better resiliency order than the classical construction can be expected.

Proposition 5.1. *If π is one-to-one, then the maximum resiliency order k reached by such a construction satisfies*

$$2^p \leq \binom{q}{k+1} + \binom{q}{k+2} + \cdots + \binom{q}{q} \tag{5}$$

This is based on the following result:

Lemma 5.2. *Let C be any d-dimensional vector subspace of $\mathbb{F}_2^n$. For any integer k such that $0 \leq k \leq n-d$, Then there exists at least*

$$N = 1 + \binom{n-d}{1} + \cdots + \binom{n-d}{k} \tag{6}$$

coset leaders of C of weight less than or equal to k.

Proof. Without a loss of generality, one may assume that a generator matrix of C is of the systematic form

$$G = \begin{pmatrix} 1 & & & \\ & \ddots & & A \\ & & 1 & \end{pmatrix}$$

with information positions on the d first components. Each coset admits a unique element that vanishes on the information set, namely of the form $x = (0, \ldots, 0, x_{d+1}, \ldots, x_n)$. The corresponding coset leader has necessarily lower weight than x. The value of N in (6) is the number of such vector x of weight $\leq k$. □

Proof. (*of proposition 5.1*) Inequality (5) in proposition 5.1 states that the number of coset leaders of weight $> k$ given by lemma 5.2, is greater than or equal to the number of vectors in E. □

Example. Let $p = 4$ and $q = 5$ and F be the 5-dimensional vector space given by the generator matrix

$$G_F = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

This vector space has minimum distance $d = 3$, thus the function f satisfies $PC(2)$. A generator matrix of the dual space $F^\perp$ is

$$G_{F^\perp} = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

The $2^p = 16$ cosets defined by vectors $u = (u_1, \ldots, u_5, 0, 0, 0, 0)$ with $(u_1, \ldots, x_u) \in \{00011, 00101, 00110, 00111, 1001, 1011, 1100, 1110, 1111, 10001, 10010, 10101, 10110, 10111, 11000, 11001\}$ only contain vectors of weight ≥ 2. Consequently, the function f is 1-resilient.

As $\max_{u \in \mathbb{F}_2^n} |\widehat{f_\chi}(u)| = 32$, the nonlinearity of f is $\delta(f) = 2^8 - 2^4 = 240$.

For all $x \in \mathbb{F}_2^5 \setminus \{0\}$, the indicator of $\pi(E)$ satisfies, $|\widehat{\varphi_{\pi(E)}}(x)| \leq 4$, thus $\max_{z \in \mathbb{F}_2^n \setminus \{0\}} |r_f(z)| = 128$ and the distance from f to the set of linear structures is $\sigma(f) = 128 - 32 = 96$.

5.2. π is two-to-one

In this section, we assume that π is a two-to-one mapping, that is to say, for any u in $\pi(E)$, the preimage $\pi^{-1}(u)$ contains exactly two elements, namely x_u and x'_u. This implies $p + 1 \geq q$.

We first examine the Walsh transform of f in such a case. As any pair is a one-dimensional affine subspace, the proposition 4.2 is applicable. With the notations of proposition 4.2, V_u is the vector space $\{0, x_u + x'_u\}$ and for any $v \in F^\perp$,

$$\begin{aligned} \widehat{(h_u)_\chi}(v) &= (-1)^{h(x_u)+v\cdot x_u} + (-1)^{h(x'_u)+v\cdot x'_u} \\ &= \begin{cases} 0 & \text{if } h(x_u) + h(x'_u) \neq v \cdot (x_u + x'_u); \\ \pm 2 & \text{elsewhere.} \end{cases} \end{aligned}$$

For convenience, let H denote the Boolean mapping on $F^\perp$ defined by $H : x \mapsto h(x_u) + h(x'_u)$. The Walsh transform of f is expressed, for any $u \in E^\perp$ and any $v \in F^\perp$:

$$\widehat{f_\chi}(u+v) = \begin{cases} 0 & \text{if either } \pi^{-1}(u) = \emptyset \text{ or } H(u) \neq v \cdot (x_u + x'_u); \\ \pm 2^{q+1} & \text{elsewhere.} \end{cases} \tag{7}$$

In particular, f is balanced if either no vector of E maps to 0 by π or $h(x_0) \neq h(x'_0)$.

We study now the autocorrelation function of f.

For any t and x in E, if $x \neq 0$, then stating that $\pi(t)$ and $\pi(t + x)$ belong to the same $F^\perp$–coset defined by vector $u \in E^\perp$ means that $\{t, t+x\}$ is precisely the pair $\{x_u, x'_u\}$ for this coset, and $x_u + x'_u = x$. Thus, from proposition 4.3, and as the pair $\{x_u, x'_u\}$ appears for both $x_u = t$ and $x_u = t + x$, for any $x \in E \setminus \{0\}$ and any $y \in F$,

$$r_f(x + y) = 2^{q+1} \sum_{u \in E^\perp | x_u + x'_u = x} (-1)^{H(u)+u\cdot y}. \tag{8}$$

Maximizing the propagation order requires that the autocorrelation function has as many zero values as possible. If for any

$u \in E^\perp$ the sum $x_u + x'_u$ is a constant x_0 independent of u, then the sum (8) is nonzero only for $x = 0$ or $x = x_0$. Let us study this particular case now.

Relation (7) becomes, for any $u \in E^\perp$ and $v \in F^\perp$:

$$\widehat{f_\chi}(u+v) = \begin{cases} 0 & \text{if either } \pi^{-1}(u) = \emptyset \text{ or } H(u) \neq v \cdot x_0; \\ \pm 2^{q+1} & \text{elsewhere.} \end{cases} \quad (9)$$

Let F' be the vector subspace of $F^\perp$ defined by $F' = \{v \in F^\perp \mid v \cdot x_0 = 0\}$. As $x_0 \in E$, then $x_0 \notin F$. Therefore, F' is a hyperplane of $F^\perp$. Each $F^\perp$-coset is the union of two F'-cosets defined by the value ε of the linear form $v \mapsto v \cdot x_0$. Thus, each F'-coset is characterized by a vector $u \in E^\perp$ that defines a $F^\perp$-coset, and a value $\varepsilon \in \mathbb{F}_2$. If any coset defined by $u \in E^\perp$ and $\varepsilon_u \in \mathbb{F}_2$ such that $H(u) = \varepsilon_u$ only contains vectors of weight $\geq k$, then, from relation (9), the function f is $(k-1)$-resilient.

To maximize the resiliency order, for any $F^\perp$–coset F_u defined by vector $u \in E^\perp$, one may choose $h(x_u)$ at random in $\mathbb{F}_2$ and define $h(x'_u)$ such that $h(x_u) + h(x'_u) = \varepsilon_u$, where ε_u defines the F'–coset in F_u which has the greatest minimum weight.

For the propagation point of view, the autocorrelation function has to be considered. Let G be the real valued function defined for any $u \in E^\perp$ by

$$G(u) = \varphi_{\pi(E)}(u) H_\chi(u) = \begin{cases} 0 & \text{if } u \notin \pi(E); \\ 1 & \text{if } u \in \pi(E) \text{ and } H(u) = 0; \\ -1 & \text{if } u \in \pi(E) \text{ and } H(u) = 1. \end{cases} \quad (10)$$

Relation (8) becomes, for any $x \in E$ and $y \in F$:

$$r_f(x+y) = \begin{cases} 2^{q+1} \widehat{\varphi_{\pi(E)}}(y) & \text{if } x = 0, \textit{ i.e. } x + y \in F; \\ 2^{q+1} \widehat{G}(y) & \text{if } x = x_0, \textit{ i.e. } x + y \in x_0 + F; \\ 0 & \text{elsewhere.} \end{cases} \quad (11)$$

It results from this relation that, if vector space F and the coset $x_0 + F$ have minimum nonzero weight k, then f satisfies $PC(k-1)$, and also, let M be the maximum of $\max_{y \in F} |\widehat{G}(y)|$ and $\max_{y \in F \setminus \{0\}} |\widehat{\varphi_{\pi(E)}}(y)|$, the distance of f from the set of linear

structures is

$$\sigma(f) = 2^{n-2} - 2^{q-1}M.$$

Example. The following example shows the construction of a 10 variable 2-resilient and $PC(2)$ Boolean function f with $\delta(f) = 480$ and $\sigma(f) = 96$.

Let $p = 5$ and $q = 5$ and F be the 5-dimensional vector space given by the following generator matrix :

$$G_F = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

The vector space F has minimum distance $d = 4$. Let E be the complementary space of F of vectors whose 5 first components are null. Let x_0 be the element of E equal to $(0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$. All the vectors in the coset $x_0 + F$ are of weight ≥ 3, thus the constructed function f satisfies $PC(2)$.

Let $\mathcal{E}$ be the set of vectors $u = (u_1, \ldots, u_5, 0, \ldots, 0)$, with $u_1 \cdots u_5 \in \{$00000, 10100, 01100, 01010, 11010, 10110, 11110, 00001, 10101, 01101, 11101, 10011, 01011, 11011, 10111, 01111$\}$. The 16 cosets $u + F^{\perp}$, with $u \in \mathcal{E}$ are split by the linear form $t \mapsto x_0 \cdot t$, into two subsets and one of them only contains vectors of weight ≥ 3. For any $u \in \mathcal{E}$, let $\varepsilon_u \in \{0, 1\}$ be such that the coset $\{t \in u + F \mid x_0 \cdot t = \varepsilon_u\}$ only contains vectors of weight ≥ 3. The values of ε_u are respectively 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1. Thus it is possible to construct a 2-resilient function:

- define the image $\pi(E) = \mathcal{E}$, and for any $t \in E'$, choose once the same element in $\mathcal{E}$ for $\pi(t)$ and $\pi(t + x_0)$;
- for any $t \in E'$, let $u = \pi(t)$. Choose randomly $h(t)$ and define $h(t + x_0) = h(t) + \varepsilon_u$.

As $\max_{u \in \mathbb{F}_2^n} |\widehat{f_\chi}(u)| = 64$, the nonlinearity of f is $\delta(f) = 2^9 - 2^5 = 480$.

For all $x \in \mathbb{F}_2^5 \setminus \{0\}$, the indicator of $\pi(E)$ satisfies, $|\widehat{\varphi_{\pi(E)}}(x)| \leq 6$, and for all $x \in \mathbb{F}_2^5$, the function G defined by relation (10) satisfies $|\widehat{G}(x)| \leq 10$, thus $\max_{z \in \mathbb{F}_2^n \setminus \{0\}} |r_f(z)| = 640$ and the distance from f to the set of linear structures is $\sigma(f) = 256 - 160 = 96$.

6. Conclusion

We have studied a family of Boolean functions defined on a direct sum $E \oplus F$ of the whole space F_2^n, similarly to the Maiorana-McFarland construction. The cryptographic properties of the obtained functions depend on the parameters of the vector subspace F, seen as a linear code. In a particular construction, the vector space E is split as a union of affine subspaces. The two cases of affine subspaces of dimension 0 and 1 have been studied, enhancing the cryptographic properties of the constructed Boolean functions.

It remains to study other decompositions of vector space E as union of affine subspaces of greater dimension. Another research direction is to consider E as a union of quasi-disjoint vector spaces, that is to say vector spaces that intersect only on the zero vector.

Other important cryptographic parameters, such as algebraic immunity, have also to be considered and studied.

References

[1] P. Camion, C. Carlet, P. Charpin, N. Sendrier. *On Correlation Immune Functions. CRYPTO'91*, LNCS VOL. 576, pp. 86–100, 1992.

[2] C. Carlet. *Partially-bent functions*; *Designs, Codes and Cryptography* VOL. 3, pp. 135–145, 1993.

[3] J.F. Dillon. *Elementary Hadamard Difference Sets*; PhD. Thesis. University of Maryland, 1974.

[4] M. Meier, O. Staffelbach. *Nonlinearity Criteria for Cryptographic Functions*; *EUROCRYPT' 89*, LNCS VOL. 473, pp. 549–562, 1990.

[5] P. Sarkar, S. Maitra. *Nonlinearity Bounds and Constructions of Resilient Boolean Functions. CRYPTO'2000*, LNCS VOL. 1880, pp. 515–532, 2000.

[6] C.E. Shannon.; *Communication theory of Secrecy System*; Bell Sys. Tech journal VOL 28, pp. 656–715, 1949.

[7] Xiao Guo-Zhen, J.L. Massey. *A Spectral Characterization of Correlation-Immune Combining Functions. IEEE Trans. on Inf. Theory*, VOL. IT34, no 3, pp. 569–571, 1988.

.