ATINER's Conference Paper Proceedings Series
MAT2020-0185
Athens, 8 July 2020

PS^- Boolean Functions

Zoubida Jadda
Patrice Parraud

Athens Institute for Education and Research
8 Valaoritou Street, Kolonaki, 10683 Athens, Greece

ATINER's Conference Paper Proceedings Series
MAT2020-0185
Athens, 8 July 2020
ISSN: 2529-167X

Zoubida Jadda, Professor, Ecoles de Saint-Cyr Coëtquidan, France
Patrice Parraud, Professor, Ecoles de Saint-Cyr Coëtquidan, France

PS^- Boolean Functions

ABSTRACT

In [14], authors presented new results on quaternary cryptographic function and their binary projection, bringing out a new approach of functions used int the security of pseudo-random generators of stream and blocks ciphers. This projection provides a large family of $2m$-variable boolean functions (respectively $2m+1$-variable) with good cryptographic properties. In the present paper, we propose a characterization of this binary projection by disregarding the conditions imposed by the quaternary construction. We show that these $2m$-variable derived boolean functions are PS^- and their $2m+1$-variable homologous are semi bent. This characterization can be viewed as a Dillon type construction with a drastic simplification of the intern function and a large choice of suitable support according a particular partition of $\mathbb{F}_2^{2m}$ (respectively $\mathbb{F}_2^{2m+1}$).

Keywords: PS^-, boolean functions, bentness, algebraic immunity

Introduction

Boolean functions play an important role in algebraic coding, cryptography and sequences design. These functions are widely used as cryptographic primitive in pseudo-random generators of stream ciphers and in S-boxes of blocks ciphers. Obviously, the security of such a system can be jeopardized if the choice of boolean function used is not suitable. Therefore, several cryptographic properties have been defined and studied to provide resistance against known attacks. Boolean functions need to satisfy various cryptographic properties simultaneously and lead to suitable trade offs. Among all known cryptographic characteristics, we can distinguish balancedness, algebraic degree, correlation immunity and nonlinearity. Because of the improvement brought by Courtois and Meier ([6]) of the algebraic attacks on stream ciphers, the notion of algebraic immunity has been introduced, and became one of the most important cryptographic property. Moreover Courtois ([5]) introduced he fast algebraic attack on stream ciphers and had led to one more constraint, the fast algebraic immunity. It is a difficult challenge to find boolean functions achieving all of the needed criteria. The construction of such functions is hard work knowing that trade-offs between different criteria must be made. An infinite class of boolean functions with optimum algebraic immunity, optimal algebraic degrees and very high nonlinearity, was proposed by Carlet and Feng in [3]. The idea was to construct for every n, boolean functions on $\mathbb{F}_{2^n}$ whose support equals $\{0\} \cup \{\alpha^i;\ \ 0 \leq i \leq 2^{n-1}-2\}$ where α is a primitive element of $\mathbb{F}_{2^n}$. Then, Tu and Deng proposed in [25] a class of algebraic immunity optimal functions of even number variables under an assumption of a combinatoric conjecture. They construct (*construction 1*) a subclass of the *Partial Spread* functions belong to Dillon [7]. The idea was to build, for every $n = 2k$, boolean functions on $\mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ of Dillon type $f(x,y) = g(xy^{2^k-2})$ where the intern function g is the one of Carlet and Feng in [3]. With the same idea, several other Dillon type construction of boolean functions have been proposed ([12],[23]) in which the intern function has a particular support under some conditions. In parallel, motivated by the interest of studying quaternary (i.e. $\{0,1,2,3\}$-valued) objects and structures ([8],[15]), several generalizations of boolean functions to residue class ring $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$ have been proposed ([24],[16], [9],[10],[11],[21]). In [22], authors investigated the connection between quaternary and binary bent functions. The notion of balancedness and nonlinearity for quaternary functions was introduced in [13] with a formal spectral characterization of quaternary bent functions. In [2], authors showed that the notion of generalized bentness and perfect nonlinearity are closely related. They introduced a construction of perfect nonlinear functions in the particular case of $q = 4$. The constructed quaternary function F defined from a Galois ring $R = GR(4,m)$ to $\mathbb{Z}_4$ depended of an intern function h from $\mathcal{T}$ (Teichmüller set) to $\mathbb{Z}_4$. They gave conditions on h to make F bent and perfect nonlinear and a proposed a possible construction of h. In [14], authors present new results on quaternary cryptographic functions defined over Galois ring $R = GR(4, m)$. The main idea was to provide some new constructions of quaternary functions with good cryptographic properties and to obtain boolean functions with optimal cryptographic properties using any binary projection. This was a kind of response to the problem of finding optimal boolean functions.

More formally, they construct a family of m-variable quaternary bent functions F_k from R to $\mathbb{Z}_4$ using an intern function h_k defined from a subset $\mathbb{C}_k$ of R to $\mathbb{Z}_4$ and cyclotomic classes of the multiplicative group of R. They characterize the bentness of F_k with sufficient and necessary conditions on h_k. With a general result on algebraic duality, they give a modelization of h_k. Finally, using a particular binary projection map, they obtain, as the binary images of their m-variable constructed quaternary bent functions, a family of $2m$-variable boolean bent functions and a family of $2m + 1$-variable boolean plateaued functions of amplitude 2^{m+1} with nonlinearity equal to $4^m - 2^m$. In this paper, we are at the crossing of these two previous approaches, the binary one and the quaternary one. We present here a characterisation of the $2m$-variable derived boolean functions obtained in [14] and prove that these functions are PS^-. By preserving the same process of construction, we drastically simplify the inherited quaternary conditions on the intern function and propose a larger choice of suitable support according a particular partition of $\mathbb{F}_2^{2m}$. Respectively, we adjust this simplification to the $2m + 1$-variable derived boolean functions obtained in [14] and propose a similar characterization with an updated splitting of $\mathbb{F}_2^{2m+1}$. This functions can be seen as the concatenation of two $2m$-variable bent functions or as adding one variable to an $2m$-variable bent functions. Although it is known that these functions are semi bent, we give a particular proof of this result. Moreover, we discuss the algebraic immunity results obtained with an exhaustive numerical experiment performed for a wide range of values of m.

The paper is organized as follow. In the next section, we recall the necessary background on boolean functions and their cryptographic properties. In Section *Constructions and Results in [14]*, we call back the quaternary cryptographic functions construction of [14] and its derived boolean functions class. In Section *Generalization and Characterization of the derived Boolean Functions*, we present our characterizations pointing out the drastic simplification of the quaternary inheritance. In Section *Algebraic Immunity of the derived Boolean Functions*, we discuss the algebraic immunity of these new characterizations and locate our results at the crossing of what have been done in other approaches.

Boolean Functions Background

Let n be a natural integer, $\mathbb{F}_2 = \{0,1\}$ the finite field of two elements, $\mathbb{F}_2^n$ the n-dimensional vector space over $\mathbb{F}_2$ and $\mathcal{B}_n$ the set of all n-variable boolean functions. A n-variables boolean function is a mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ which can be identified by its truth table $f(0,\cdots,0),\cdots,f(1,\cdots,1)$ of length 2^n. The support of f is defined as $supp(f) = \{u \in \mathbb{F}_2^n | f(u) \neq 0\}$ and the Hamming weight $w_H(f)$ of f is the size of its support. The Hamming distance between two n-variable boolean functions f and g is $d_H(f,g) = w_H(f+g)$ where $+$ denotes the addition on $\mathbb{F}_2$. The Walsh transform of a n-variables boolean function f is the complex mapping from $\mathbb{F}_2^n$ to $\mathbb{C}$ defined by $W_f(u) = \sum_{v \in \mathbb{F}_2^n} (-1)^{<u,v>+f(v)}$ where $< u, v >$ denotes the usual inner product in $\mathbb{F}_2^n$. A n-variable boolean function f is balanced if $w_H(f) = 2^{n-1}$ that is, if its truth-table contains a equal number 1's and 0's. The nonlinearity $nl(f)$ of a n-variable boolean function f is the minimum distance between f and all affine functions, $nl(f) = \min_{g\ affine} d_H(f,g)$. On a spectral point of view, the nonlinearity of f can be expressed by $nl_2(f) = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n} |W_f(a)|$ and its blancedness by $W_f(0) = 0$. For all f in $\mathcal{B}_n$, we have $nl_2(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$. This bound is reached for bent functions [20] which are characterized by $\forall u \in \mathbb{F}_2^n,\ \ |W_f(u)| = 2^{\frac{n}{2}}$ for n even. A bent function could not be balanced. A n-variable boolean function f is said to be plateaued if its Walsh transform 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 $r \geq \frac{n}{2}$. Clearly, the nonlinearity of a plateaued function f of amplitude λ equals $2^{n-1} - \frac{\lambda}{2}$. Each boolean function $f \in \mathcal{B}_n$ has a unique representation called algebraic normal form (ANF), as a multivariate polynomial over $\mathbb{F}_2$, $f(x_1,,\cdots,x_n) = \sum_{I \subseteq \{1,\cdots,n\}} a_I \prod_{i \in I} x_i$ where the a_I's are in $\mathbb{F}_2$. The algebraic degree $deg(f)$ of a n-variable boolean function f is the maximum degree of those monomials with nonzero coefficients. The algebraic immunity $AI(f)$ of an n-variable boolean function $f \in \mathcal{B}_n$ is the lowest degree of nonzero function g such that $f.g = 0$ or $(f+1).g = 0$. The relationship between algebraic immunity and the algebraic degree was studied by Courtois ([5]) according to this theorem, for all $f \in \mathcal{B}_n$, $AI(f) \leq deg(f)$ and $AI(f) \leq min\left\{\lceil \frac{n}{2} \rceil, deg(f)\right\}$.

Constructions and Results in [14]

In the scope of finding solutions to the binary problem of optimal boolean function, in [14] is proposed a construction of a large family of m-variable quaternary bent functions for which the binary image gives a family of $2m$-variable boolean bent functions and a family of $2m+1$-variables boolean functions with maximal non-linearity equal to $4m-2m+1$ (plateaued functions of amplitude 2^{m+1}). Let $\mathbb{Z}_4=\mathbb{Z}/4\mathbb{Z}=\{0,1,2,3\}$ be the ring of integers modulo 4 which is group-isomorphic to $\mathbb{U}_4=\{\pm 1,\pm i\}$ the group of 4^{th} root of unity in $\mathbb{C}$ under the standard isomorphism $x\mapsto i^x$. Let $\mathbb{Z}_4^m$ represent the set of all m −tuples of elements in $\mathbb{Z}_4$ where m is a natural integer. An m-variable quaternary function F is a mapping from $\mathbb{Z}_4^m$ to $\mathbb{Z}_4$ which can be identified by its truth table $F(0,\cdots,0),\cdots,F(3,\cdots,3)$ of length 4^m. Let $R=GR(4,m)$ be the Galois ring of 4^m elements, that is the Galois extension of order m of $\mathbb{Z}_4$. The Galois ring R is a local ring having a unique maximal ideal $D=2R$ made up of the 2^m zero divisors. The residue class field $K=R/D$ is isomorphic to the finite field $\mathbb{F}_{2^m}$ under the canonical map $z\mapsto\bar{z}$ from R to K. There are two canonical ways to represent the 4^m elements of R, a multiplicative one and a additive one. In the multiplicative representation, each element z of R has a unique expansion $z=z_1+2z_2$ with z_1,z_2 in $\mathcal{T}$, where $\mathcal{T}$ is the Teichmüller set of roots of $x^{2^m}-x$ in R. Noting β the $(2^m-1)^{th}$ root of unity, $\mathcal{T}=\{0,1,\beta,\cdots,\beta^{2^m-2}\}$. In the additive representation, $\forall z\in R$ there exists an unique expansion $z=\sum_{l=0}^{m-1}z_l\beta^l$ with z_l in $\mathbb{Z}_4$. We refer the reader to [18] for further information about Galois rings. The multiplicative representation allowed us to define the 2^m-cyclotomic classes $(C_j)_{0\le j\le 2^m-1}$ of order 2^m-1 of the multiplicative group $R^*=R\backslash D$ of R, with $D=2R=2\mathcal{T}=\{0,2,2\beta,\cdots,2\beta^{2^m-2}\}$, by $C_j=\{\beta^l(1+2\beta^j),\ 0\le l\le 2^m-2\}, C_{2^m-1}=\{\beta^l,\ 0\le l\le 2^m-2\}$. Using these cyclotomic classes, the m-variable quaternary function F_k from R to $\mathbb{Z}_4$ can be constructed as $F_k(x)=h_k(\beta^k(1+2\beta^j))$ if $x\in C_j,\ 0\le j\le 2^m-2$. and $F_k(x)=h_k(\beta^k)$ if $x\in C_{2^m-1}\cup D$. Where $h_k\colon\mathbb{C}_k\to\mathbb{Z}_4$ and $\mathbb{C}_k=\{\beta^k\}\cup\{\beta^k(1+2\beta^j)\ ,\ 0\le j\le 2^m-2\}$ is characterized, built and modelized under strong conditions (Propositions 3, 5 and 6 in [14]). In order to obtain the binary projection of this m-variable quaternary function F_k, we need a vector representation of the element of R. As R is a vector space of dimension m over $\mathbb{Z}_4$, R is isomorphic to $\mathbb{Z}_4^m$. Let note d this isomorphism. Let us define $E=d(\mathcal{T})=\{\mathbf{0},v_0,v_1,\cdots,v_{2^m-2}\}$ the vector representation of $\mathcal{T}$, where $\mathbf{0}=d(0)$ is the all zero vector of length m and for all j in $0,2^m-2$, and $v_j=d(\beta^j)$ is the vector representation of the element β^j. The multiplicative operation on E is defined as $\forall v_i, v_j \in E^* = d(\mathcal{T}^*) = E\backslash\{\mathbf{0}\}$, $v_i \times v_j = v_{(i+j)(\mathrm{mod}2^m-1)}$ and $\forall v_j \in E,\ \mathbf{0} \times v_j = v_j \times \mathbf{0} = \mathbf{0}$. The additive operation $+$ on E is the one of $\mathbb{Z}_4^m$. As $D = 2\mathcal{T}$, the vector representation of all elements of D is $W = d(D) = 2E = \{\mathbf{0}, 2v_0, 2v_1, \cdots, 2v_{2^m-2}\}$. The vector representation of any element z of R is naturally expressed by $d(z) = u + 2v \in \mathbb{Z}_4^m$ with $u, v \in E$. In the same way, the cyclotomic classes $(C_j)_{0\le j\le 2^m-1}$ have the following vector representation $V_j = d(C_j) = \{v_l(v_0 + 2v_j),\ 0 \le l \le 2^m - 2\}$ for $0 \le j \le 2^m - 2$ and $V_{2^m-1} = d(C_{2^m-1}) = d(\mathcal{T}^*) = E^*$. That is $\mathbb{Z}_4^m = d(\cup_{j=0}^{2^m-2} C_j \cup C_{2^m-1} \cup D) = \cup_{j=0}^{2^m-2} V_j \cup V_{2^m-1} \cup W$. The vector representation of $\mathbb{C}_k$ is defined by $\mathfrak{V}_k = d(\mathbb{C}_k)$. We can define the vector representation $\bar{h}_k$ of the intern function h_k from $\mathfrak{V}_k$ to $\mathbb{Z}_4$ by $\bar{h}_k(x) = h_k(d^{-1}(x))$ and the vector representation $\bar{F}_k$ of the quaternary function F_k from $\mathbb{Z}_4^m$ to $\mathbb{Z}_4$ by $F_k(d^{-1}(x))$:

$$= \begin{cases} \bar{h}_k(v_k(v_0 + 2v_j)) & if \quad x \in V_j,\ 0 \le j \le 2^m - 2 \\ \bar{h}_k(v_k) & if \quad x \in V_{2^m-1} \cup W \end{cases} \qquad (1)$$

Let us define the 1-to-1 projection map φ from $\mathbb{Z}_4^m$ to $\mathbb{F}_2^{2m}$ with $\varphi(u + 2v) = \tilde{u}||\tilde{v}$, where denotes the component mod 2 reduction and $||$ denotes the concatenation operation. We obtain $\varphi(W) = \{\mathbf{0}||\tilde{v}_l,\ 0 \le l \le 2^m - 2\} \cup \{\mathbf{0}||\mathbf{0}\}$ and $\varphi(V_j) = \{\tilde{v}_l||\tilde{v}_{l+j},\ 0 \le l \le 2^m - 2\}$ for $0 \le j \le 2^m - 2$ and $\varphi(V_{2^m-1}) = \{\tilde{v}_l||\mathbf{0},\ 0 \le l \le 2^m - 2\}$. That is

$$\mathbb{F}_2^{2m} = \cup_{j=0}^{2^m-2} \varphi(V_j) \cup \varphi(V_{2^m-1}) \cup \varphi(W) \qquad (2)$$

Considering this vector representation $\bar{F}_k$ of F_k and the binary projection map φ from $\mathbb{Z}_4^m$ to $\mathbb{F}_2^{2m}$, the derived $2m$-variable boolean functions f_{2m} have been defined by:

$$\begin{array}{lccc} f_{2m} & : & \mathbb{F}_2^{2m} & \rightarrow & \mathbb{F}_2 \\ & & x & \mapsto & \psi_i(\bar{F}_k(\varphi^{-1}(x))) \end{array} \quad (3)$$

where $\psi_{i\in\mathbb{N}}$ is any balanced mapping from $\mathbb{Z}_4$ to $\mathbb{F}_2$.

Similarly, the derived $2m + 1$-variable boolean functions f_{2m+1} have been defined by:

$$\begin{array}{llll} f_{2m+1} & : & \mathbb{F}_2^{2m+1} & \rightarrow & \mathbb{F}_2 \\ & & x & \mapsto & \psi_\varepsilon(\bar{F}_k(\varphi^{-1}(x))) \end{array} \quad (4)$$

where ψ_ε is any balanced mapping from $\mathbb{Z}_4$ to $\mathbb{F}_2$ and ε is in $\{0,1\}$.

Generalization and Characterization of the Derived Boolean Functions

The main idea of this paper is to propose a generalization and a characterisation of the binary images obtained in [14] by disregarding the conditions imposed by the quaternary construction.

1. $n = 2m$-variable boolean functions

Let m be a natural integer, $\mathbb{F}_2$ the finite field with two elements. We identify the Galois field $\mathbb{F}_{2^m}$ and the vector space $\mathbb{F}_2^m$ in order to construct the vector space $\mathbb{F}_2^{2m} = \mathbb{F}_2^m || \mathbb{F}_2^m$, where $||$ denotes the concatenation operation of two vectors of $\mathbb{F}_2^m$. Let $p(x)$ a monic irreducible primitive divisor of $x^{2^m-1} - 1$ in $\mathbb{F}_2 x$ of degree m. The Galois field $\mathbb{F}_{2^m}$ of 2^m elements is a Galois extension of order m of $\mathbb{F}_2$ and is isomorphic to the factor field $\mathbb{F}_2 x/(p(x))$. If α is a root of $p(x)$ of order $2^m - 1$ ($\alpha^{2^m-1} - 1 = 0$) then $\mathbb{F}_{2^m}$ is the polynomial field $\mathbb{F}_2\alpha = \{0,1,\alpha,\cdots,\alpha^{2^m-2}\}$ and $\{1,\alpha,\cdots,\alpha^{m-1}\}$ is a basis of $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$. We have $\forall z \in \mathbb{F}_{2^m},\ z = \sum_{j=0}^{m-1} z_j\alpha^j,\ z_j \in \mathbb{F}_2,\ 0 \le j \le m-1$.

Let $\vartheta_i = (0,\cdots,0,\mathbf{1}_\mathbf{i},0,\cdots,0) \in \mathbb{F}_2^m,\ 0 \le i \le m-1$, ($\mathbf{1}_\mathbf{i}$ means $\mathbf{1}$ at position **i**) be the vector associated with the element $\alpha^i \in \mathbb{F}_{2^m},\ 0 \le i \le m-1$; we also denote by ϑ_m the vector associated with the element ($p(\alpha) - \alpha^m$), and recursively $\vartheta_{m+i},\ 1 \le i \le 2^m - (m+2)$ the vector associated with the element $\alpha * (\alpha^{i-1}p(\alpha) - \alpha^{m+i-1})$. In the same way, $\mathbf{0} \in \mathbb{F}_2^m$, the all zero vector of length m, is the vector associated with the element 0 of $\mathbb{F}_{2^m}$. As $\{\vartheta_0,\dots,\vartheta_{m-1}\}$ is a basis of $\mathbb{F}_2^m$, the vector space $\mathbb{F}_2^{2m} = \mathbb{F}_2^m||\mathbb{F}_2^m$ admits $\{\vartheta_i||\mathbf{0}\ ,\ 0 \le i \le m-1\} \cup \{\mathbf{0}||\vartheta_i\ ,\ 0 \le i \le m-1\}$ as a basis. The 2^m cyclotomic classes $(\Gamma_j)_{0 \le j \le 2^m-1}$ of order $2^m - 1$ of $\mathbb{F}_2^{2m}$ can be redefined as

$$\begin{cases} \Gamma_j = \{\vartheta_l||\vartheta_l \times \vartheta_j, \quad 0 \le l \le 2^m - 2\}, \forall j, \quad 0 \le j \le 2^m - 2, \\ \Gamma_{2^m-1} = \{\vartheta_l||\mathbf{0}, \quad 0 \le l \le 2^m - 2\} \\ \end{cases}$$

with $\vartheta_j \times \vartheta_l = \vartheta_{l+j\ [2^m-1]}$ and $\mathbf{0} \times \vartheta_l = v_l \times \mathbf{0} = \mathbf{0}$, to which we add the class Γ_{2^m} of order 2^m defined by $\Gamma_{2^m} = \{\mathbf{0}||\vartheta_l,\ 0 \le l \le 2^m - 2\} \cup \{\mathbf{0}||\mathbf{0}\}$.

Upon these identification, we obtain

$$\mathbb{F}_2^{2m} = \left(\cup_{j=0}^{j=2^m-2} \Gamma_j\right) \cup \Gamma_{2^m-1} \cup \Gamma_{2^m} \quad (5)$$

The derived $2m$-variable boolean bent functions $f_{2m}(x)$ obtained from (3) are generalized as $f_{2m}(x) = a_{2m-1}$ if $x \in \Gamma_{2^m-1} \cup \Gamma_{2^m}$, and $f_{2m}(x) = a_j$ if $x \in \Gamma_j$, $0 \leqslant j \leqslant 2^m - 2$, with $a_j \in \mathbb{F}_2$, $0 \leq j \leq 2^m - 1$ satisfying $\sum_{j=0}^{j=2^m-1} (-1)^{a_j} = 0$. These functions are partial spread PS^- functions.

Proof. We can see in (1) that $\bar{F}$ takes the same value on each cyclotomic classe V_j, $0 \leq j \leq 2^m - 2$ and a constant value on V_{2^m-1} and W. The intern function $\bar{h}_k$ is balanced over $\mathfrak{B}_k$ (Proposition 3 in [14]). Considering the partition (5) and the balanced mapping $\psi_{i\in\mathbb{N}}$ from $\mathbb{Z}_4$ to $\mathbb{F}_2$, we can simplify the $2m$-variable derived boolean functions defined in (3) by:

$$f_{2m}(x) = \psi_i(\bar{F}_k(\varphi^{-1}(x)))$$
$$= \begin{cases} \psi_i(\bar{h}_k(v_k(v_0 + 2v_j))) = a_j & if \quad x \in \Gamma_{j\ {}_{0\leq j\leq 2^m-2}} \\ \psi_i(\bar{h}_k(v_k)) = a_{2^m-1} & if \quad x \in \Gamma^*_{2m-1} \cup \Gamma_{2m} \end{cases}$$

with $a_j \in \mathbb{F}_2$, $0 \leq j \leq 2^m - 1$. In [14], authors use a algebraic duality result to split the Teichmüller set in order to construct the intern quaternary function h_k verifying two conditions (see Propositon 3 of [14]). Within this binary projection, only the balancedness condition is necessary, and this allows us to generalize the derived $2m$-variable boolean bent function f_{2m} as follows:

$$\begin{array}{llll} f_{2m} & : & \mathbb{F}_2^{2m} & \rightarrow \mathbb{F}_2 \\ & & x & \rightarrow \begin{cases} a_j & if \quad x \in \Gamma_{j\ {}_{0\leq j\leq 2^m-2}} \\ a_{2m-1} & if \quad x \in \Gamma^*_{2m-1} \cup \Gamma_{2m} \end{cases} \end{array}$$

with $\sum_{j=0}^{j=2^m-1} (-1)^{a_j} = 0$.

Let us recall that a Partial Spread (PS^-) function f is defined as follows:

$$\begin{array}{lll} f: & \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} & \rightarrow \mathbb{F}_2 \\ & (x,y) & \rightarrow \begin{cases} g\left(\frac{x}{y}\right) & if y \neq 0 \\ g(0) & else \end{cases} \end{array}$$

where the intern function g is a balanced boolean function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$. Using the identification of the finite field $\mathbb{F}_{2^m}$ and the vector space $\mathbb{F}_2^m$ and the splitting (1), we rewrite the PS^- definition as follows:

$$\begin{array}{cccc} f & : & \mathbb{F}_2^m || \mathbb{F}_2^m & \rightarrow & \mathbb{F}_2 \\ & & x & \rightarrow & \begin{cases} g(\alpha^{-j}) & if \quad x \in \Gamma_{j\ {}_{0 \le j \le 2^m - 2}} \\ g(0) & if \quad \in \Gamma_{2m-1}^{*} \cup \Gamma_{2m} \end{cases} \end{array}$$

This shows that our f_{2m} boolean function is PS^- with its intern function g defined as:

$$\begin{array}{ccccc} g & : & \mathbb{F}_{2^m} & \rightarrow & \mathbb{F}_2 \\ & & x & \rightarrow & \begin{cases} g(\alpha^{-j}) = a_j & , \qquad 0 \le j \le 2^m - 2 \\ g(0) = a_{2^m - 1} \end{cases} \end{array}$$

The $2m$-variable boolean function f_{2m} obtained from Proposition 1 has algebraic degree equal to m.

Proof. This is a direct consequence of the fact that f_{2m} is PS^-

This leads to a new approach of the partial spread functions, as a generalization of the $2m$-variable derived boolean functions provided in [14], with simpler restrictive conditions than the ones imposed by the quaternary approach.

2. $n = 2m + 1$-variable boolean functions

We naturally extend the case $n = 2m$ to $n = 2m + 1$ to generalize the $2m + 1$-variable derived boolean functions obtained in [14]. Similarly to the previous section, we update the definition of cyclotomic classes. Let $\varepsilon \in \mathbb{F}_2$ and write $\forall j,\ 0 \le j \le 2^m - 2$, $\Gamma_{j,\varepsilon} = \Gamma_j || \varepsilon = \{\vartheta_l || \vartheta_l \times \vartheta_j || \varepsilon,\ 0 \le l \le 2^m - 2\}$, $\Gamma_{2^m - 1,\varepsilon} = \Gamma_{2^m - 1} || \varepsilon = \{\vartheta_l || \mathbf{0} || \varepsilon,\ 0 \le l \le 2^m - 2\}$, $\Gamma_{2^m,\varepsilon} = \Gamma_{2^m} || \varepsilon = \{\mathbf{0} || \vartheta_l || \varepsilon,\ 0 \le l \le 2^m - 2\} \cup \{\mathbf{0} || \mathbf{0} || \varepsilon\}$. With this definition we have

$$\mathbb{F}_2^{2m+1} = \cup_{\varepsilon \in \{0,1\}} \left(\left(\cup_{j=0}^{j=2^m - 2} \Gamma_{j,\varepsilon} \right) \cup \Gamma_{2^m - 1,\varepsilon} \cup \Gamma_{2^m,\varepsilon} \right)$$

The derived $2m + 1$-variable boolean bent functions $\psi_\varepsilon(\bar{F}_k(\varphi^{-1}(x)))$ obtained by (4) are generalized as $f_{2m+1}(x) = a_{2^m - 1,\varepsilon}$ if $x \in \Gamma_{2^m,\varepsilon}$ and $f_{2m+1}(x) = a_{j,\varepsilon}$ if $x \in \Gamma_{j,\varepsilon}$, $0 \leqslant j \leqslant 2^m - 2$, with $\forall \epsilon \in \{0,1\}$ and

$\forall j,\ 0 \leq j \leq 2^m - 1,\ a_{j,\epsilon} \in \mathbb{F}_2$ such that $\sum_{j=0}^{j=2^m-1} (-1)^{a_{j,\epsilon}} = 0$. These functions can be seen either as a concatenation of two $2m$-variable boolean bent functions or as functions obtained through the addition of an extra variable to a $2m$-variable boolean bent function. It is shown in [?] that the concatenation of two suitably chosen semi-bent functions yields to a bent function and vice versa. Although, we prove that in our case the derived $2m+1$-variable boolean function, seen as the concatenation of two bent functions, is semi bent.

The derived $2m+1$-variable boolean function f_{2m+1} obtained from (4) is semi-bent.

Proof. We have to show that $\forall a \in \mathbb{F}_2^{2m+1},\ W_{f_{2m+1}}(a) \in \{0, \pm 2^{m+1}\}$.

Let $a = x_1||x_2||\epsilon' \in \mathbb{F}_2^{2m+1}$.

$$W_{f_{2m+1}}(a) = \sum_{b\in\mathbb{F}_2^{2m+1}} (-1)^{f_{2m+1}(b)+<a,b>}$$

$$= \sum_{\epsilon\in\{0,1\}} \left(\sum_{b\in\cup_{j=0}^{2^m-1}\Gamma_{j,\epsilon}} (-1)^{f(b)+<a,b>} + \sum_{b\in\Gamma_{2^m,\epsilon}} (-1)^{f(b)+<a,b>}\right)$$

$$= \sum_{\epsilon\in\{0,1\}} \Big(\sum_{v\in\mathbb{F}_2^m} \sum_{v_l\in\mathbb{F}_2^{m*}} (-1)^{f(v_l||v_l\times v||\epsilon)+<v_l||v_l\times v||\epsilon,x_1||x_2||\epsilon'>} + \sum_{v\mathbb{F}_2^m} (-1)^{f(0||v||\epsilon)+<0||v||\epsilon,x_1||x_2||\epsilon'>}\Big)$$

$$= \sum_{\epsilon\in\{0,1\}} \Big(\sum_{j\in\mathbb{F}_{2^m}} (-1)^{a_{j,\epsilon}} \sum_{v_l\in\mathbb{F}_2^{m*}} (-1)^{<v_l||v_l\times v||\epsilon,x_1||x_2||\epsilon'>} 1.5cm + (-1)^{a_{2^m-1,\epsilon}} \sum_{v\in\mathbb{F}_2^m} (-1)^{<0||v||\epsilon,x_1||x_2||\epsilon'>}\Big)$$

$$\overset{*}{=} \sum_{\epsilon\in\{0,1\}} (-1)^{\epsilon.\epsilon'}\Big(\sum_{j\in\mathbb{F}_{2^m}} (-1)^{a_{j,\epsilon}} \sum_{v_l\in\mathbb{F}_2^{m*}} (-1)^{<v_l||v_l\times v,x_1||x_2>} + (-1)^{a_{2^m-1,\epsilon}} \sum_{v\in\mathbb{F}_2^m} (-1)^{<0||v,x_1||x_2>}\Big)$$

$$= \sum_{\epsilon\in\{0,1\}} (-1)^{\epsilon.\epsilon'}\left(W_{f_{2^m,\epsilon}}(x_1||x_2)\right)$$

Finally, as functions $f_{2^m,\epsilon}$ are bent, we obtain $W_f(x_1||x_2||\epsilon') = \begin{cases} 0 \\ \pm 2^{m+1} \end{cases}$

[balancedness] The derived $2m+1$-variable boolean function f_{2m+1} obtained from (4) is balanced if $a_{2^m-1,0} \neq a_{2^m-1,1}$.

Proof. Using equation (*) in the previous proof with $a = x_1||x_2||\epsilon' = 0$, we have

$$W_f(0) = \sum_{\epsilon\in\{0,1\}} \left((2^m - 1)\sum_{j\in\mathbb{F}_{2^m}} (-1)^{a_{j,\epsilon}} + 2^m(-1)^{a_{2^m-1,\epsilon}}\right) = 2^m \sum_{\epsilon\in\{0,1\}} (-1)^{a_{2^m-1,\epsilon}}$$

If $a_{2^m-1,0} \neq a_{2^m-1,1}$, then $W_f(0) = 0$ and the function is balanced.

Algebraic Immunity of the Derived Boolean Functions

Let $f \in \mathcal{B}_n$, define $AN(f) = \{g \in \mathcal{B}_n, f * g = 0\}$ the set of the annihilator of f. The algebraic immunity $AI(f)$ of f is the minimum degree of all the nonzero annihilators of f and of all those of $f + 1$. The exact calculation of the algebraic immunity of boolean functions remains a difficult problem. With regard to known boolean functions constructions, this cryptographic property (as the fast algebraic immunity) appears definitively the most complicated to evaluate. It depends on the way that the boolean function is constructed and its support. In [3], due to their construction, authors managed to prove the algebraic immunity of their functions by using a general results from code theory, the well-known BCH bound ([17],[19]). Moreover, thanks to a combinatorial conjecture first established by Tu and Deng in [25] and later proved by Cohen and Flori in [4], several authors ([25], [12], [26]) were able to prove the algebraic immunity of their boolean functions.

In our case, these approach does not seem suitable as the support of our boolean functions is not standard, that is it is not composed exclusively of consecutive powers of a primitive element of the finite field used to construct them. However, we successfully have made a large exhaustive numerical experimentation and validate the following results: *the algebraic immunity of the $2m$-variable (respectively $2m + 1$-variable) Boolean function is m.*

This numerical experimentation takes into account for all values of m in the range $2 \leq m \leq 10$, all the possible values of the parameter $a_\emptyset$ (respectively $a_{\emptyset,\varepsilon}$ for $\varepsilon \in \{0,1\}$) and all the possible balanced vectors $a = (a_0, \cdots, a_{2^m-1})$ (respectively $a_\varepsilon = (a_{0,\varepsilon}, \cdots, a_{2^m-1,\varepsilon})$ for $\varepsilon \in \{0,1\}$). The numerical calculations were made within the SageMath program V6.8 (*www.sagemath.org*) under a multi-core i7 computer, 2.4 GHz, 16Gb RAM, amd64, Linux computer using the *crypto_boolean_function* library.

Although we do not have a mathematically proof of this cryptographic property, this numerical experimentation validate the right value of the algebraic immunity of our constructed boolean functions for a large range of number of variables n, that is $4 \leq n \leq 20$, which actually seems to be the most interesting range of value.

Conclusion

This paper presents a new characterization of the $2m$-variable derived Boolean functions (respectively $2m + 1$-variable) obtained in [14]. By disregarding the inherited quaternary conditions imposed on the intern function, and using a particular splitting of $\mathbb{F}_2^{2m}$, we prove that these $2m$-variable Boolean functions are PS^-. Similarly, we apply the same simplification to the $2m + 1$-variable derived Boolean functions with a suitable splitting of $\mathbb{F}_2^{2m+1}$. We show differently that these $2m+1$-variable Boolean functions are semi bent and prove that they can be balanced. Moreover, an exhaustive numerical experiment shows that our functions have optimal algebraic immunity for a large range of interesting values of m. Our approach, located at the crossing between a quaternary construction and a Dillon type construction, offers great investments opportunities and reinforce our motivation to go further, to formally characterize the algebraic immunity of these functions.

References

[1] C. Carlet, On a weakness of the Tu-Deng function and its repair, IACR, Cryptology ePrint Archive, http://eprint.iacr.org/2009/606, (2009) Finite Fields and applications, vol. 1999, pp. 81–94, (2001)

[2] C. Carlet and S. Dubuc, On generalized Bent and q $-$ary perfect nonlinear functions, Finite Fields and applications, vol. 1999, pp. 81–94, (2001)

[3] C. Carlet and K. Feng An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity, Advances in Cryptology, ASIACRYPT 2008, LNCS, vol. 5350, pp. 425-440, (2008)

[4] G. Cohen and J. P. Flori On a generalized combinatorial conjecture involving addition mod 2^k-1, IACR, Cryptology ePrint Archive, http://eprint.iacr.org/ 2011/400, (2011)

[5] N. Courtois, Fast algebraic attacks on stream ciphers with linear feedback, Advances in Cryptology, CRYPTO 2003, LNCS, vol. 2729, pp. 176–194. Springer (2003)

[6] N. Courtois and W. Meier, Algebraic attacks on stream ciphers with linear feedback, Advances in Cryptology, EUROCRYPT 2003, LNCS, vol. 2656, pp. 345–359, (2003)

[7] J. F. Dillon, Elementary Hadamard difference sets, PhD Thesis, University of Maryland, (1974)

[8] A.R. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane and P. Solé, The $\mathbb{Z}_4$ linearity of Kerdock, Preparata, Goethals and related codes, IEEE Transactions on Information Theory, vol. 40, no. 2, pp. 301–319, (1994)

[9] X. Hou, p $-$ary and q $-$ary versions of certain results about Bent functions and resilient functions, Finite Fields and applications, vol. 10, pp. 566–582, (2004)

[10] X. Hou, q $-$ary Bent functions constructed from chain rings, Finite Fields and applications, vol. 4, pp. 55–61, (1998)

[11] X-D. Hou, Bent functions, partial difference sets and quasi-Frobenius rings, Designs, Codes and Cryptography, vol. 20, pp. 251–268, (2000)

[12] Q. Jin, Z. Liu, B. Wu and X. Zhang, A general conjecture similar to T-D conjecture and its applications in constructing boolean functions with optimal algebraic immunity, IACR, Cryptology ePrint Archive, http://eprint.iacr.org/2011/515, (2011)

[13] Z. Jadda and P.Parraud, $\mathbb{Z}_4$-Nonlinearity of a constructed quaternary cryptographic functions class, In Proc. 6th SETA, pp. 81–94, (2010)

[14] Z. Jadda, P. Parraud and S. Qarboua, Quaternary cryptographic bent functions

and their binary projection, Cryptography and Communications: Discrete Structures, Boolean Functions and Sequences, Vol. 5, Issue 1, page 49-65, (2013)

[15] P.V. Kumar, T. Hellesth, A.R. Calderbank and A.R. Hammons, Large Families of Quaternary Sequences with Low Correlation, IEEE Transactions on Information Theory, vol. 42, no. 2, pp. 579–592, (1996)

[16] P. V. Kumar, R.A. Scholtz and L.R. Welch, Generalized Bent Functions and Their Properties, Journal of Combinatorial Theory, Ser. A, vol. 1, no. 40,pp. 90–107, (1985)

[17] R. Lidl and H. Niederreiter, Finite Fields, Cambridge University Press, (1996)

[18] B.R. McDonald, Finite Rings with Identity, Marcel Dekker Inc, (1974)

[19] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Mathematical Library, (1977)

[20]O.S. Rothaus, On Bent functions, Journal of Combinatorial Theory, vol. 20, pp. 300–305, (1976)

[21] D. Singh, M. Bhaintwal and B. K. Singh, Recent results on generalized q-ary bent functions, Cryptology ePrint Archives, *http://www.eprint.iacr.org/2012/037*, (2012)

[22] P. Solé and N. Tokareva Connections between quaternary and binary Bent functions, Cryptology ePrint Archives, *http://www.eprint.iacr.org/ 2009/544*, (2009)

[23] D. Tang, C. Carlet and X. Tang, Highly nonlinear boolean functions with optimal algebraic immunity and good behavior against fast algebraic attacks, IEEE Trans. Inf. Theory, vol. 59, no. 1, pp. 653–664, (2013)

[24] N. Tokareva Generalizations of bent functions, a survey to appear in Journal of Applied and industrial Mathematics, Cryptology ePrint Archives, *http://www.eprint. iacr.org/2011/111*,(2011)

[25] Z. Tu and Y. Deng, A conjecture about binary strings ans its applications on constructing boolean functions with optimal algebraic immunity, Design Codes and Cryptography, no 60:1–14, (2011)

[26] B. Wu, Z. Liu and D. Lin, Constructing boolean functions with potential algebraic immunity based on additive decomposition of finite fields, CoRR, arXiv:1401. 6604, (2014)