CONSTRUCTED QUATERNARY CRYPTOGRAPHIC FUNCTIONS CLASS

ZOUBIDA JADDA AND PATRICE PARRAUD

ABSTRACT. New results on quaternary ($\mathbb{Z}_4 = \{0, 1, 2, 3\}$-valued) cryptographic functions are presented. We define and characterize completely the $\mathbb{Z}_4$-balancedness and the $\mathbb{Z}_4$-nonlinearity according to the HAMMING metric and the LEE metric. In the particular case of quaternary Bent functions we show that the maximal nonlinearity of these functions is bounded for the HAMMING metric and we give the exact value of the maximal nonlinearity of these functions for the LEE metric. A general construction, based on Galois ring, is related in detail and applied to obtain a class of balanced and high nonlinearity quaternary cryptographic functions. We use Gray map to derive these constructed quaternary functions to obtain balanced Boolean functions having high nonlinearity.

1. INTRODUCTION

Boolean ($\{0, 1\}$-valued) functions of length n used in pseudo-random generators of stream and block ciphers play an important role in their security ([7, 1]). These functions are usually studied over finite field of two elements $\mathbb{F}_2$. Finding Boolean functions with optimal cryptographic properties as balancedness and high nonlinearity is still an open problem. The purpose of this paper is to present new results on quaternary ($\{0, 1, 2, 3\}$-valued) cryptographic functions. This work is motivated by the interest in studying quaternary objects and structures (see [8, 12]). The usual metric used in $\mathbb{Z}_4$ is the LEE metric which allows to have an isometry from ($\mathbb{Z}_4^m$, LEE distance) to ($\mathbb{F}_2^{2m}$, HAMMING distance) with the Gray map. We begin by defining and characterizing exactly quaternary cryptographic functions of length m. Then, we formally describe balancedness and nonlinearity over $\mathbb{Z}_4$ according to the HAMMING metric and the LEE metric. Quaternary Bent functions [19] (or more generaly q-ary Bent functions [3, 9, 10, 11]) are defined by Walsh transform. For m-variables quaternary Bent functions we prove that the maximal nonlinearity is bounded between $3 \cdot 4^{m-1} - 2^{m-1}$ and $3 \cdot 4^{m-1} - 2^{m-2}$ under the HAMMING metric and we give conditions to reach the upper bound. We show that the exact value of the maximal nonlinearity of these functions under the LEE metric is $4^{m-1} - 2^{m+1}$. A general construction of quaternary cryptographic functions is detailed, using cyclotomic classes of the multiplicative group of a Galois ring R. We point out the fact that the balancedness and the nonlinearity of the obtained

Keywords. Quaternary functions, Boolean functions, cryptographic functions, nonlinearity, balancedness, quaternary algebra, Gray map, Galois ring.

The work was supported by the project A-Math-Net – Applied Mathematics Knowledge Transfer Network (CZ.1.07/2.4.00/17.0100).

functions depend on the b-polynomial used to construct R and on the distribution of these classes over R. We naturally apply this construction to a particular configuration in order to obtain a class of m-variables quaternary cryptographic functions which are balanced and have nonlinearity bounded between $3\cdot 4^{m-1}-2^m$ and $3\cdot 4^{m-1}-2^{m-1}$ for the HAMMING metric and bounded between 4^m-2^{m+1} and 4^m-2^m for the LEE metric. Using the Gray map with these obtained quaternary functions we present $2m-$variables balanced Boolean functions with high nonlinearity. To avoid any confusion, an n-variables Boolean function is denoted by f while an m-variables quaternary function is denoted by F .

2. Boolean Functions Basics

Let n be a natural integer and $\mathbb{F}_2^n$ the set of all n-tuples of elements in the finite field $\mathbb{F}_2=\{0,1\}$ with its sum denoted by $\oplus$. An n-variables Boolean function f is a function 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 by $supp(f)=\{u\in\mathbb{F}_2^n \mid f(u)\neq 0\}$ and the Hamming weight $w_H(f)$ of f by the size of its support. The Hamming distance between two n-variables Boolean functions f and g is $d_H(f,g)=w_H(f\oplus g)$ where $\oplus$ denotes the addition in $\mathbb{F}_2$. The Walsh transform of an n-variables Boolean function f is the complex mapping from $\mathbb{F}_2^n$ to $\mathbb{C}$ defined by $W_f(u)=\sum_{v\in\mathbb{F}_2^n}(-1)^{u\cdot v+f(v)}$ where $u\cdot v$ denotes the usual inner product in $\mathbb{F}_2^n$. An n-variables Boolean function f is balanced if its truth table contains an equal number of 1's and 0's which means that $w_H(f)=2^{n-1}$ or in spectral term $W_f(0)=0$. The nonlinearity of a n-variables Boolean function f is the minimum distance to all affine functions $nl_2(f)=\min\limits_{g\ affine} d_H(f,g)$. Using the Walsh transform, the nonlinearity of f can be expressed by $nl_2(f)=2^{n-1}-\frac{1}{2}\max\limits_{a\in\mathbb{F}_2^n}|W_f(a)|$. Readers can read [5, 6, 16] for more detailed explanations of Boolean functions cryptographic criteria. For every n-variables Boolean function f, we have $nl_2(f)\leq 2^{n-1}-2^{\frac{n}{2}-1}$. This bound is reached for Bent functions [17, 14] which are characterised by $\forall u\in\mathbb{F}_2^n,\quad |W_f(u)|=2^{\frac{n}{2}}$ for n even. A Bent function could not be balanced. Finding maximal nonlinearity Boolean functions (see [13, 15, 18]) is an open problem.

3. Quaternary Cryptographic Functions

3.1. Quaternary Tools

Throughout this section, i will denote the complex number such that $i^2=-1$. 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 $x\rightarrow i^x$. $\mathbb{Z}_4^m$ will represent the set of all $m-$tuples of elements in $\mathbb{Z}_4$ where m is a natural integer. The addition on $\mathbb{Z}_4$ (addition $\pmod 4$) will be denoted by $+$. The LEE weights w_L of $0,1,2,3$ in $\mathbb{Z}_4$ are $0,1,2,1$ respectively and the LEE weight $w_L(u)$ of an element u of $\mathbb{Z}_4^m$ is the rational sum of the LEE weight of its components. The LEE distance $d_L(u,v)$ between two elements u and v in $\mathbb{Z}_4^m$ is $w_L(u+v)$.

Definition 3.1. An m-variables quaternary function F is a function 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 us define $\mathcal{F}(\mathbb{Z}_4^m,\mathbb{Z}_4)$ as the set of all m-variables quaternary functions.

Example 3.2. F: $\begin{array}{lll} \mathbb{Z}_4^2 & \to & \mathbb{Z}_4 \\ (x_1,x_2) & \mapsto & x_1+x_2 \mod 4 \end{array}$

The truth table is
$[F(0,0),F(0,1),F(0,2),F(0,3),F(1,0),F(2,0),F(3,0),F(1,1),F(1,2),F(1,3),$
$F(2,1),F(3,1),F(2,2),F(2,3),F(3,2),F(3,3)]$ i.e
$[0,1,2,3,1,2,3,2,3,0,3,0,0,1,1,2]$.

The support of F is defined by $supp(F)=\{u\in\mathbb{Z}_4^m \mid F(u)\neq 0\}$. We define the relative support of F by $supp_j(F)=\{u\in\mathbb{Z}_4^m \mid F(u)=j\}$ for all j in $\mathbb{Z}_4$ and $\eta_j(F)$ its size. The HAMMING weight $w_H(F)$ of F is the size of its support and the HAMMING distance between two m-variables quaternary functions F and G is $d_H(F,G)=w_H(F-G)$. The LEE weight $w_L(F)$ of F is $\eta_1(F)+\eta_3(F)+2\eta_2(F)$ and the LEE distance between two m-variables quaternary functions F and G is $d_L(F,G)=w_L(F-G)$. The Walsh transform of an m-variables quaternary function F is the complex mapping from $\mathbb{Z}_4^m$ to $\mathbb{C}$ defined by $W_F(u)=\sum_{v\in\mathbb{Z}_4^m} i^{u\cdot v+F(v)}$ where $u\cdot v$ denotes the usual inner product in $\mathbb{Z}_4^m$ (mod 4) . We define $W_F^2(u)=\sum_{v\in\mathbb{Z}_4^m} i^{u\cdot v}\,(-1)^{F(v)}$ and $W_F^3(u)=\sum_{v\in\mathbb{Z}_4^m} i^{u\cdot v}\,(-i)^{F(v)}$

3.2. Quaternary Balancedness and Nonlinearity

Definition 3.3 (Balancedness)**.** Let $F\in\mathcal{F}(\mathbb{Z}_4^m,\mathbb{Z}_4)$.

$$F \text{ is balanced } \iff \forall j\in\mathbb{Z}_4,\ \eta_j(F)=4^{m-1}.$$

Let us give a balancedness characterisation of quaternary function.

Proposition 3.4. *Let $F\in\mathcal{F}(\mathbb{Z}_4^m,\mathbb{Z}_4)$.*

$$F \textit{ is balanced } \iff W_F(0)=W_F^2(0)=0.$$

Proof. By definition we have $W_F(0)=\sum\limits_{v\in\mathbb{Z}_4^m} i^{F(v)}$ and $W_F^2(0)=\sum\limits_{v\in\mathbb{Z}_4^m}(-1)^{F(v)}$, then $W_F(0)=\eta_0(F)-\eta_2(F)+i(\eta_1(F)-\eta_3(f))$ and $W_F^2(0)=\eta_0(F)-\eta_1(F)+\eta_2(F)-\eta_3(F)$. These two equalities give us 3 equations on η_j $(0\leq j\leq 3)$ by extracting real and imaginary parts. Since $\sum\limits_{j\in\mathbb{Z}_4}\eta_j(F)=4^m$ we then obtain a system of 4 simultaneous equations in 4 unknowns that we solve. This finishes the proof. □

Similary to the binary case, we define the nonlinearity of quaternary function.

Definition 3.5 (Nonlinearity)**.** Let $F\in\mathcal{F}(\mathbb{Z}_4^m,\mathbb{Z}_4)$. The nonlinearity of F is defined by the minimum distance to all affine functions with
$nl_4^H(F)=\min\limits_{G\ affine} d_H(F,G)$ under the HAMMING metric
and with $nl_4^L(F)=\min\limits_{G\ affine} d_L(F,G)$ under the LEE metric.

Go on with a nonlinearity characterisation of quaternary function.

Proposition 3.6. *Let $F \in \mathcal{F}(\mathbb{Z}_4^m, \mathbb{Z}_4)$. The nonlinearity of F under the* HAMMING *metric is completely characterised by*

$$\begin{aligned} nl_4^H(F) &= 3\cdot 4^{m-1} - \frac{1}{4}\max_{a\in\mathbb{Z}_4^m, b\in\mathbb{Z}_4}\left\{2Re(i^b\, W_F(a)) + (-1)^b\, W_F^2(2a)\right\} \\ &= 3\cdot 4^{m-1} - \frac{1}{4}\max_{a\in\mathbb{Z}_4^m}\left\{2 \mid Re(W_F(a)) \mid + W_F^2(2a), 2 \mid Im(W_F(a)) \mid - W_F^2(2a)\right\} \end{aligned}$$

where $Re(z)$ and $Im(z)$ denote respectively the real and imaginary part of the complex number z.

Proof. By Definition 3.5, we have

$$nl_4^L(F) = \min_{G\ affine} d_H(F,G) = \min_{G\ affine} w_H(F-G)$$

Let S be the function in $\mathcal{F}(\mathbb{Z}_4^m, \mathbb{Z}_4)$ such that $S(u) = F(u) + a\cdot u + b$ with a in $\mathbb{Z}_4^m$ and b in $\mathbb{Z}_4$.

$$\begin{aligned} nl_4^H(F) &= \min_{a\in\mathbb{Z}_4^m, b\in\mathbb{Z}_4}\{\eta_1(S) + \eta_2(S) + \eta_3(S)\} \\ &= 4^m - \max_{a\in\mathbb{Z}_4^m, b\in\mathbb{Z}_4}\eta_0(S). \end{aligned}$$

Using the decomposition of $W_S(0)$, $W_S^2(0)$, $W_S^3(0)$ and the fact that $\eta_0(S)+\eta_1(S)+\eta_2(S)+\eta_3(S) = 4^m$ we obtain

$$\begin{aligned} \eta_0(S) &= \frac{1}{4}\left[4^m + W_S(0) + W_S^2(0) + W_S^3(0)\right] \\ &= \frac{1}{4}\left[4^m + \sum_{u\in\mathbb{Z}_4^m}\left(i^{F(u)+a\cdot u+b} + (-1)^{F(u)+a\cdot u+b} + (-i)^{F(u)+a\cdot u+b}\right)\right] \\ &= \frac{1}{4}\left[4^m + i^b\, W_F(a) + (-1)^b\, W_F^2(2a) + \overline{i^b\, W_F(a)}\right] \\ &= \frac{1}{4}\left[4^m + 2Re(i^b\, W_F(a)) + (-1)^b\, W_F^2(2a)\right]. \end{aligned}$$

The proof is completed, the second expression of $nl_4^H(F)$ is obvious using properties of complex numbers. □

Proposition 3.7. *Let $F \in \mathcal{F}(\mathbb{Z}_4^m, \mathbb{Z}_4)$. The nonlinearity of F under the* LEE *metric is completely characterised by*

$$\begin{aligned} nl_4^L(F) &= 4^m - \max_{a\in\mathbb{Z}_4^m, b\in\mathbb{Z}_4}\left\{Re(i^b\, W_F(a))\right\} \\ &= 4^m - \max_{a\in\mathbb{Z}_4^m}\{\mid Re(W_F(a)) \mid, \mid Im(W_F(a)) \mid\}. \end{aligned}$$

Proof. By Definition 3.5, we have

$$nl_4^L(F) = \min_{G\ affine} d_L(F,G) = \min_{G\ affine} w_L(F-G).$$

Let S be the function in $\mathcal{F}(\mathbb{Z}_4^m, \mathbb{Z}_4)$ such that $S(u) = F(u) + a \cdot u + b$ with a in $\mathbb{Z}_4^m$ and b in $\mathbb{Z}_4$.

$$nl_4^L(F) = \min_{a \in \mathbb{Z}_4^m, b \in \mathbb{Z}_4} \{\eta_1(S) + 2\eta_2(S) + \eta_3(S)\}.$$

Using the decomposition of $W_S(0)$ and $W_S^3(0)$ we have

$$W_S(0) + W_S^3(0) = 2(\eta_0(S) - \eta_2(S)).$$

Moreover

$$W_S(0) + W_S^3(0) = 2Re(i^b\, W_F(a)).$$

As $\sum\limits_{j \in \mathbb{Z}_4} \eta_j(S) = 4^m$, we obtain

$$\eta_1(S) + 2\eta_2(S) + \eta_3(S) = 4^m + \eta_2(S) - \eta_0(S).$$

That is

$$\begin{aligned} nl_4^L(F) &= \min_{a \in \mathbb{Z}_4^m, b \in \mathbb{Z}_4} \{4^m + \eta_2(S) - \eta_0(S)\} \\ &= 4^m - \max_{a \in \mathbb{Z}_4^m, b \in \mathbb{Z}_4} \left\{Re(i^b\, W_F(a))\right\} \end{aligned}$$

which ends the proof of the first expression. The second expression of $nl_4^L(F)$ is obvious by properties of complex numbers. □

3.3. Quaternary Bent Functions Properties

Definition 3.8 (Quaternary Bent functions)**.** Let F be an m-variables quaternary function. F is Bent if and only if $|\, W_F(a)| = 2^m$, for any $a \in \mathbb{Z}_4^m$.

Remark 3.9. If F is Bent, we have $W_F(a) = \pm 2^m$ or $W_F(a) = \pm i 2^m$.

Proof. $\widehat{\chi_F}(a) = \mu + i\nu$ with (μ, ν) in $\mathbb{Z} \times \mathbb{Z}$ and $|\widehat{\chi_F}(a)| = 2^m$.
Then $(2^m)^2 = \mu^2 + \nu^2$ and the only possible values for μ and ν are $(\mu, \nu) = (\pm 2^m, 0)$ or $(\mu, \nu) = (0, \pm 2^m)$: proved by recurrence on m for (μ, ν) in $\mathbb{N} \times \mathbb{N}$. □

Let us now focus on the maximal nonlinearity of an m-variables quaternary Bent function F according to the Hamming metric and the Lee metric respectively as shown in Fig.1.

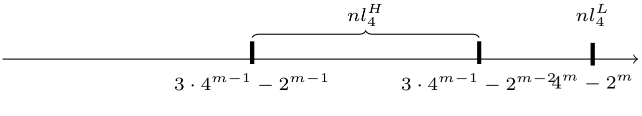

Figure 1. Nonlinearity of Quaternary Bent function .

Theorem 3.10. *Let F be a m-variables Bent function.*

(1) $3 \cdot 4^{m-1} - 2^{m-1} \leq nl_4^H(F) \leq 3 \cdot 4^{m-1} - 2^{m-2}$.

(2) $nl_4^H(F) = 3 \cdot 4^{m-1} - 2^{m-2}$ *if and only if* $W_F^2(2a) = \pm 2^m$.

Proof. (1): Proposition 3.6 gives $nl_4^H(F)$ equal to

$3 \cdot 4^{m-1} - \frac{1}{4} \sup_{a\in\mathbb{Z}_4^m} \{2 \mid Re(W_F(a)) \mid + W_F^2(2a), 2 \mid Im(W_F(a)) \mid - W_F^2(2a)\}$.

Let us write $nl_4^H(F) = 3 \cdot 4^{m-1} - \frac{1}{4}y$

where $y = \sup_{a\in\mathbb{Z}_4^m} \{2 \mid Re(W_F(a)) \mid + W_F^2(2a), 2 \mid Im(W_F(a)) \mid - W_F^2(2a)\}$

and $x = W_F^2(2a) = \sum_{u\in\mathbb{Z}_4^m} (i)^{2a.u}(-1)^{F(u)} = \sum_{u\in\mathbb{Z}_4^m} (-1)^{a.u}(-1)^{F(u)}$.

As F is Bent, we use Remark 3.9 to distinguish two main cases in order to evaluate y (let c=2^{m+1}):

- $W_F(a) = \pm 2^m : y = Max\{c + x, -x\}$
- $W_F(a) = \pm i2^m : y = Max\{x, c - x\}$

The geometric representation of y in terms of x (Fig.2) shows that y ranges between 2^m and 2^{m+1} which completes the proof.

(2): Let $nl_4^H(F) = 3 \cdot 4^{m-1} - 2^{m-2}$. If F is Bent and $W_F(a)$ real then $2^m = \sup_{a\in\mathbb{Z}_4^m} \{2^{m+1} + W_F^2(2a), -W_F^2(2a)\}$. In this case $W_F^2(2a) < 0$ and $W_F^2(2a)$ is equal to -2^m or $2^{m+1} + W_F^2(2a) = 2^m$ that is $W_F^2(2a) = 2^m - 2^{m+1} = -2^m$. The case $W_F(a)$ is imaginary is similar.

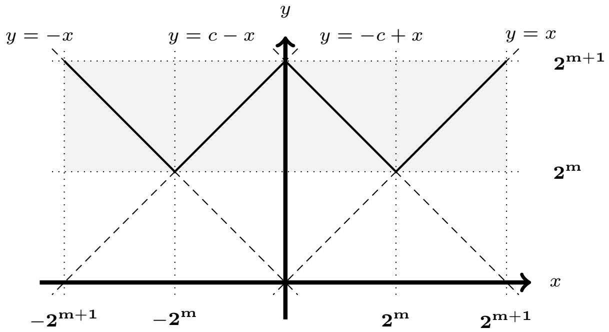

Figure 2. y in terms of x.

□

Theorem 3.11. *Let F be an m-variables Bent function.*

$$nl_4^L(F) = 4^m - 2^m.$$

Proof. Proposition 3.7 gives $nl_4^L(F) = 4^m - \max_{a\in\mathbb{Z}_4^m, b\in\mathbb{Z}_4} \{Re(i^b W_F(a))\}$.

Using remark 3.9 we have $Re(i^b W_F(a)) = \pm 2^m$ which finishes the proof. □

4. Galois Rings and Cyclotomic Classes

In this section we give definitions and properties of the Galois ring $GR(4, m)$ without proofs. We refer the reader to [20] and [8] for further informations about Galois rings.

4.1. Galois Rings

As usual, $\mathbb{Z}_4 = \mathbb{Z}/4\mathbb{Z} = \{0,1,2,3\}$ is the ring of integers modulo 4 and $\mathbb{F}_2$ the finite field with two elements. Let $\mu : \mathbb{Z}_4 \to \mathbb{F}_2$ be the mod-2 reduction map. We extend μ to $\mathbb{Z}_4[x] \to \mathbb{F}_2[x]$ in the natural way. A monic polynomial $h(x)$ in $\mathbb{Z}_4[x]$ of degree m is said to be basic irreducible if $h_2(x) = \mu(h(x))$ is a monic irreducible primitive divisor of $x^{2^m-1} - 1$ in $\mathbb{F}_2[x]$ (Hensel lift). The Galois ring $R = GR(4,m)$ of 4^m elements is a Galois extension of order m of $\mathbb{Z}_4$ and is isomorphic to the factor ring $\mathbb{Z}_4[x]/(h(x))$ where $h(x)$ is a monic basic irreducible polynomial of degree m (b-polynomial). Let β be a root of $h(x)$ of order $2^m - 1$ ($\beta^{2^m-1} - 1 = 0$). Then R is the polynomial ring $\mathbb{Z}_4[\beta]$ where $\{1, \beta, \cdots, \beta^{m-1}\}$ is a basis of R over $\mathbb{Z}_4$. 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. The Teichmüller system $\mathcal{T} = \{0, 1, \beta, \cdots, \beta^{2^m-2}\}$ is the set of roots of $x^{2^m} - x$ in R and can be viewed as the set of representatives of K as $D = 2R = 2\mathcal{T}$. Let $\theta = \bar{\beta}$ be a primitive root of $h_2(x)$ in $\mathbb{F}_2[x]$, we can identify K with $\mathbb{F}_{2^m} = \overline{\mathcal{T}} = \{0, 1, \theta, \cdots, \theta^{2^m-2}\}$. The multiplicative group $R^\star = R \setminus D$ of R is a group of order $(2^m-1)2^m$ which is the direct product $\mathcal{H} \times \mathcal{U}$ where $\mathcal{H}$ is the cyclic group of order $(2^m - 1)$ generated by β and $\mathcal{U}$ is the Abelian group of principal units of R of order 2^m that is elements of the form $1 + 2z_0$ with z_0 in $\mathcal{T}$. There are two canonical ways to represent the 4^m elements of R, a multiplicative one and an additive one. In the multiplicative representation, every element z of R has a unique expansion $z = z_1 + 2z_2$ with z_1 and z_2 in $\mathcal{T}$.

4.2. Cyclotomic Classes

Let $R = GR(4,m)$ be the Galois ring of 4^m elements, $D = \{0, 2, 2\beta, \cdots, 2\beta^{2^m-2}\}$ the set of zero divisors with $\mid D \mid= 2^m$ and $R^\star = \{z_1(1+2z_0),\ z_0 \in \mathcal{T}, z_1 \in \mathcal{T}\setminus\{0\}\}$ the multiplicative group of R with $\mid R^\star \mid= 2^m(2^m - 1)$.

Definition 4.1. Let m be a natural integer and $R = GR(4,m)$ be the Galois ring of 4^m elements and $R^\star$ its multiplicative group. The 2^m cyclotomic classes of order $2^m - 1$ of $R^\star$ are:
$C_k = \{\beta^j + 2\beta^k,\ 0 \le j \le 2^m - 2\}$ for any k such that $0 \le k \le 2^m - 2$ and $C_{2^m-1} = \{\beta^j,\ 0 \le j \le 2^m - 2\}$.

5. Construction

Let $R = GR(4,m)$ be the Galois ring of 4^m elements and D the set of zero divisors of R. Let us consider the 2^m cyclotomic classes C_k of order $2^m - 1$ of $R^\star$ (see Definition 4.1).
We construct the quaternary function F such that the function F takes the same value for each element of C_k.

We now compute formally the expressions of W_F and W_F^2 for this constructed function F. We have

$$\begin{cases} C_k & = & \{\beta^j + 2\beta^k,\ 0 \leq j \leq 2^m - 2\},\ 0 \leq k \leq 2^m - 2 \\ C_{2^m-1} & = & \{\beta^j,\ 0 \leq j \leq 2^m - 2\} \end{cases}$$

with $\mid C_{k,\ 0 \leq k \leq 2^m-1} \mid = 2^m - 1$. And $D = \{0\} \cup \{2\beta^j,\ 0 \leq j \leq 2^m - 2\}$.
Let a in $\mathbb{Z}_4^m$.

$$W_F(a) = \underbrace{\sum_{v \in D} i^{a \cdot v + F(v)}}_{S_D(a)} + \sum_{0 \leq k \leq 2^m-2} \underbrace{\left(\sum_{v \in C_k} i^{a \cdot v + F(v)} \right)}_{S_{C_k}(a)} + \underbrace{\sum_{v \in C_{2^m-1}} i^{a \cdot v + F(v)}}_{S_{C_{2^m-1}}(a)}$$

$$W_F(a) = S_D(a) + \sum_{0 \leq k \leq 2^m-2} S_{C_k}(a) + S_{C_{2^m-1}}(a) \tag{5.1}$$

As $D = \{0, 2, 2\beta, \cdots, 2\beta^{2^m-2}\}$ we have

$$S_D(a) = i^{F(0)} + \sum_{0 \leq k \leq 2^m-2} (-1)^{a \cdot \beta^k} i^{F(2\beta^k)} \tag{5.2}$$

If $v \in C_k$ for $0 \leq k \leq 2^m - 2$ then $v = \beta^j + 2\beta^k$ with $0 \leq j \leq 2^m - 2$ and

$$S_{C_k}(a) = (-1)^{a \cdot \beta^k} \sum_{0 \leq j \leq 2^m-2} i^{a \cdot \beta^j} i^{F(\beta^j + 2\beta^k)} \tag{5.3}$$

If $v \in C_{2^m-1}$ then $v = \beta^j$ for $0 \leq j \leq 2^m - 2$ and

$$S_{C_{2^m-1}}(a) = \sum_{0 \leq j \leq 2^m-2} i^{a \cdot \beta^j} i^{F(\beta^j)} \tag{5.4}$$

In equations (5.2), (5.3) and (5.4), terms of the form $(-1)^{a \cdot \beta^k}$ and $i^{a \cdot \beta^j}$ show that $W_F(a)$ depends on the b-polynomial used to construct the Galois ring and terms of the form $i^{F(2\beta^k)}$, $i^{F(\beta^j + 2\beta^k)}$ and $i^{F(\beta^j)}$ show that $W_F(a)$ depends on the way that F takes value on the different cosets $C_{k,\ 0 \leq k \leq 2^m-1}$ and D.
As the construction states that for a given class C_k, the function F takes the same value, if $v = \beta^j + 2\beta^k \in C_k$ then let us define $F_k = F(v) = F(\beta^j + 2\beta^k)$ which does not depend on j.

$$\begin{aligned} W_F(a) &= S_D(a) + \sum_{0 \leq k \leq 2^m-2} \left((-1)^{a \cdot \beta^k} i^{F_k} \sum_{0 \leq j \leq 2^m-2} i^{a \cdot \beta^j} \right) + i^{F_{2^m-1}} \sum_{0 \leq j \leq 2^m-2} i^{a \cdot \beta^j} \\ &= S_D(a) + \left(\sum_{0 \leq j \leq 2^m-2} i^{a \cdot \beta^j} \right) \left(\sum_{0 \leq k \leq 2^m-2} (-1)^{a \cdot \beta^k} i^{F_k} + i^{F_{2^m-1}} \right) \end{aligned}$$

We have now to distinguish the case $a \in D$ from the case $a \notin D$.
$\underline{a \in D}$
Let $a = 2\beta^l$ with $0 \leq l \leq 2^m - 2$ or $a = 0$.

$$W_F(0) = \sum_{v \in D} i^{F(v)} + (2^m - 1) \sum_{0 \leq k \leq 2^m-1} i^{F_k} \tag{5.5}$$

$$W_F(a) = \sum_{v\in D} i^{F(v)} + \left(\sum_{0\leq j\leq 2^m-2} (-1)^{\beta^l\cdot\beta^j} \right) \left(\sum_{0\leq k\leq 2^m-1} i^{F_k} \right) \tag{5.6}$$

$\underline{a \notin D}$

Let $a = \beta^s + 2\beta^l$ in C_l for $0 \leq l \leq 2^m - 2$ and for $l = 2^m - 1$ we have $a = \beta^s$ with $0 \leq s \leq 2^m - 2$.

Furthermore : $(-1)^{a\cdot\beta^k} = (-1)^{\beta^s\cdot\beta^k}$ and $i^{a\cdot\beta^j} = \begin{cases} i^{\beta^s\cdot\beta^j}(-1)^{\beta^l\cdot\beta^j} \\ i^{\beta^s\cdot\beta^j} \end{cases}$

That is

$$W_F(a) = S_D(s) + A(s,l)\left(B(s) + i^{F_{2^m-1}}\right) \tag{5.7}$$

where

$$S_D(s) = i^{F(0)} + \sum_{0\leq k\leq 2^m-2} (-1)^{\beta^s\cdot\beta^k} i^{F(2\beta^k)} \tag{5.8}$$

$$A(s,l) = \sum_{0\leq j\leq 2^m-2} (-1)^{\beta^l\cdot\beta^j} i^{\beta^s\cdot\beta^j} \tag{5.9}$$

$$B(s) = \sum_{0\leq k\leq 2^m-2} (-1)^{\beta^s\cdot\beta^k} i^{F_k} \tag{5.10}$$

$$A(s) = \sum_{0\leq j\leq 2^m-2} i^{\beta^s\cdot\beta^j} \tag{5.11}$$

We have that $S_D(s)$ and $B(s)$ do not depend on the class of a but only on values of F and A depends only on a but not on values of F. Moreover, we have

$$W_F^2(2a) = \sum_{v\in\mathbb{Z}_4^m} (-1)^{a.v}(-1)^{F(v)} = \sum_{v\in D}(-1)^{F(v)} + \sum_{0\leq k\leq 2^m-1} \left(\sum_{v\in C_k} (-1)^{a\cdot v+F(v)} \right)$$

As for the calculation of $W_F(a)$, we find that

$$W_F^2(2a) = \sum_{v\in D}(-1)^{F(v)} + \sum_{0\leq k\leq 2^m-1} (-1)^{F_k} \sum_{0\leq j\leq 2^m-2} (-1)^{a.\beta^j} \tag{5.12}$$

Equations (5.6) and (5.7) give the exact value of $W_F(a)$ and (5.12) the exact value of $W_F^2(2a)$ according to the detailed calculation done by equations (5.1)–(5.5) and (5.8)–(5.11).

Remark 5.1 (Balancedness of F)**.** The balancedness of F depends on the way that F takes value on the different cosets C_k and D.

Remark 5.2 (Nonlinearity of F)**.** The nonlinearity of F under the Hamming and Lee metric depends on the choice of the b-polynomial and the way that F takes value according to u belongs to C_k or D.

We now apply these results to a particular configuration in order to obtain a balanced quaternary function with high nonlinearity under the Hamming metric and Lee metric as shown in Fig.3 and Fig.4 respectively.

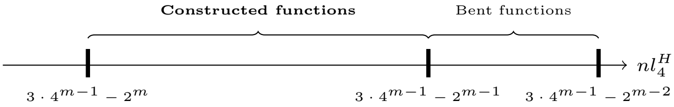

Figure 3. Constructed Quaternary function nonlinearity nl_4^H.

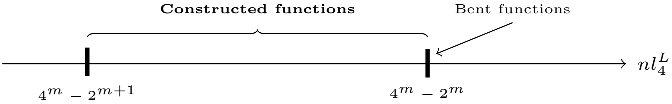

Figure 4. Constructed Quaternary function nonlinearity nl_4^L.

Proposition 5.3. *For k, $0 \leq k \leq 2^m - 2$ and for $\gamma \in \{0,1,2,3\}$, we define $\delta_k = \gamma$ if $k \equiv \gamma \pmod 4$. With a suitable b-polynomial, we construct an m-variables quaternary function F as follows: $F(\beta^j + 2\beta^k) = F(2\beta^k) = \delta_k$ and $F(0) = 3$, for j, $0 \leq j \leq 2^m - 2$. This quaternary function is balanced and its nonlinearity under the* Hamming *metric satisfies $3 \cdot 4^{m-1} - 2^m \leq nl_4^H(F) \leq 3 \cdot 4^{m-1} - 2^{m-1}$ and its nonlinearity under the* Lee *metric satisfies $4^m - 2^{m+1} \leq nl_4^L(F) \leq 4^m - 2^m$.*

Numerical Results

Nonlinearity under the Hamming metric $nl_4^H(F)$ and the Lee metric $nl_4^L(F)$ (using Propositions 3.6 and 3.7) of constructed balanced quaternary m-variables functions F with Nbp the number of possible b-polynomials, Nbs the number of suitable b-polynomials and $B_1^H = 3 \cdot 4^{m-1} - 2^m, B_2^H = 3 \cdot 4^{m-1} - 2^{m-1}, B_1^L = 4^m - 2^{m+1}$ and $B_2^L = 4^m - 2^m$.

m	Nbp	Nbs	*suitable bpolynomial*	B_1^H	$\mathbf{nl_4^H(F)}$	B_2^H	B_1^L	$\mathbf{nl_4^L(F)}$	B_2^L
3	2	2	$x^3 + 2x^2 + x + 3$	40	**44**	44	48	**56**	56
4	2	2	$x^4 + 2x^2 + 3x + 1$	176	**180**	184	224	**232**	240
5	6	6	$x^5 + 3x^2 + 2x + 3$	736	**744**	752	960	**976**	992
6	6	2	$x^6 + x^5 + x^4 + 2x^2 + 3x + 1$	3008	**3032**	3040	3968	**4016**	4032
7	18	14	$x^7 + 2x^4 + x + 3$	12160	**12208**	12224	16128	**16224**	16256
8	16	2	$x^8 + 3x^5 + x^3 + 2x^2 + 3x + 1$	48896	**49008**	49024	65024	**65248**	65280
9	48	10	$x^9 + 2x^6 + 2x^5 + 3x^4 + x^3 + 3$	196096	**196288**	196352	261120	**261504**	261632

6. Derived Boolean Functions

Let $R = GR(4,m)$ be the Galois ring of 4^m elements and D the set of zero divisors of R. Let us consider the m-variables quaternary function F obtained by the construction which uses the 2^m cyclotomic classes of order $2^m - 1$ of $R^\star$. By taking the binary images of F under the Gray map, we obtain $n = 2m$-variables Boolean functions which are balanced and having high nonlinearity.

Definition 6.1. The Gray map ϕ is defined from $\mathbb{Z}_4$ to $\mathbb{F}_2 \times \mathbb{F}_2$ with $\phi(2q + r) = (q, q \oplus r)$. We also define Q from $\mathbb{Z}_4$ to $\mathbb{F}_2$ with $Q(2q + r) = q$.

The Gray map is clearly a bijection from $\mathbb{Z}_4$ to $\mathbb{F}_2^2$ and its inverse is defined by $\phi^{-1}(q,s) = 2q + (q \oplus s)$. Identifying $\mathbb{F}_2^m \times \mathbb{F}_2^m$ to $\mathbb{F}_2^{2m}$, we extend naturally ϕ

to $\mathbb{Z}_4^m$ componentwise by $\phi_m(2q_0 + r_0, \cdots, 2q_{m-1} + r_{m-1}) = (q_0, \cdots, q_{n-1}, q_0 \oplus r_0, \cdots, q_{m-1} \oplus r_{m-1})$ and ϕ_m^{-1} to $\mathbb{F}_2^{2m}$ by $\phi_m^{-1}(q_0, \cdots, q_{n-1}, s_0, \cdots, s_{m-1}) = (2q_0 + q_0 \oplus s_0, \cdots, 2q_{m-1} + q_{m-1} \oplus s_{m-1})$.

Definition 6.2. The $2m$-variables Boolean function f derived by the Gray map is

$$\begin{array}{cccc} f: & \mathbb{F}_2^{2m} & \to & \mathbb{F}_2 \\ & y & \mapsto & Q(F(\phi_m^{-1}(y))) \end{array}$$

Numerical Results :

Nonlinearity $nl_2(f) = 2^{n-1} - \frac{1}{2} \max\limits_{a \in \mathbb{F}_2^n} |\boldsymbol{W}_f(a)|$ of obtained balanced n-variables Boolean functions f with $n = 2m$ derived from the previous constructed balanced quaternary m-variables functions F compared with known values.

n	bnl^1	bnl^2	nl^1	nl^2	$\mathbf{nl_2(f)}$
6	12	10	22	24	**24**
8	58	70	94	112	**112**
10	260	366	390	478	**464**
12	1124	1700	1600		**1952**
14	4760	7382	6524		**8000**

bnl^1: Lobanov's lower bound
bnl^2: Carlet - Feng's ([4]) lower bound

nl^1: Best balanced exact Nonlinearity before
nl^2: Carlet-Feng's ([4]) exact Nonlinearity with optimal algebraic immunity

7. Numerical Example for $m = 3$ and $n = 6$

Let consider the Galois ring $R = GR(4,3)$ of 64 elements built with the b-polynomial $h(x) = x^3 + 2x^2 + x + 3$.

The 8 cyclotomic classes of order 7 of $R^\star$ (Def.4.1) are :

$$\begin{array}{lcl}
C_0 & : & \{3, \beta+2, \beta^2+2, \beta^3+2, \beta^4+2, \beta^5+2, \beta^6+2\} \\
C_1 & : & \{1+2\beta, 3\beta, \beta^2+2\beta, \beta^3+2\beta, \beta^4+2\beta, \beta^5+2\beta, \beta^6+2\beta\} \\
C_2 & : & \{1+2\beta^2, \beta+2\beta^2, \beta^2+2\beta^2, \beta^3+2\beta^2, \beta^4+2\beta^2, \beta^5+2\beta^2, \beta^6+2\beta^2\} \\
C_3 & : & \{1+2\beta^3, \beta+2\beta^3, \beta^2+2\beta^3, \beta^3+2\beta^3, \beta^4+2\beta^3, \beta^5+2\beta^3, \beta^6+2\beta^3\} \\
C_4 & : & \{1+2\beta^4, \beta+2\beta^4, \beta^2+2\beta^4, \beta^3+2\beta^4, \beta^4+2\beta^4, \beta^5+2\beta^4, \beta^6+2\beta^4\} \\
C_5 & : & \{1+2\beta^5, \beta+2\beta^5, \beta^2+2\beta^5, \beta^3+2\beta^5, \beta^4+2\beta^5, \beta^5+2\beta^5, \beta^6+2\beta^5\} \\
C_6 & : & \{1+2\beta^6, \beta+2\beta^6, \beta^2+2\beta^6, \beta^3+2\beta^6, \beta^4+2\beta^6, \beta^5+2\beta^6, \beta^6+2\beta^6\} \\
C_7 & : & \{1, \beta, \beta^2, \beta^3, \beta^4, \beta^5, \beta^6\}
\end{array}$$

The obtained partitions applying the construction are (Prop. 5.3) :
Let $E_j = \{u \in \mathbb{Z}_4^3, F(u) = j\}$, $j = 0, 1, 2, 3$.

$$\begin{array}{lcl}
E_0 & = & C_0 \cup C_4 \cup \{2, 2\beta^4\} \\
E_1 & = & C_1 \cup C_5 \cup \{2\beta, 2\beta^5\} \\
E_2 & = & C_2 \cup C_6 \cup 2\{\beta^2, 2\beta^6\} \\
E_3 & = & C_3 \cup C_7 \cup \{2\beta^3, 0\}
\end{array}.$$

The balanced constructed 3-variables quaternary function F is :
$F = 3322312311001200312003111302203200220021331132130321113030122302$
with $nl_4^H(F) = 44$ and $nl_4^L(F) = 56$.

The balanced derived 6-variables Boolean function f is :
$f = 1111101100000100101001000101101100110010110011010110001010011101$
with $nl_2(f) = 24$.

8. Conclusion

This paper presents new results on quaternary cryptographic functions, bringing out a new approach of functions used in the security of pseudo-random generators of stream and block ciphers. The main goal of this work, similarly motivated by the $\mathbb{Z}_4$ linearity paper [8], is to present an alternative to the open problem of finding optimal Boolean functions. After defining quaternary functions and describing their $\mathbb{Z}_4$ balancedness and nonlinearity, under the Hamming metric and the Lee metric, we give results on the maximal nonlinearity of quaternary Bent functions. Using the algebraic structure of a Galois ring, we present a general construction of quaternary functions, pointing out necessary trade offs in order to obtain optimal cryptographic properties. In a natural way, we apply this construction with a particular configuration to get balanced and high nonlinearity quaternary functions. Faithful to our main objective, we take the image of our quaternary constructed functions under the Gray map to obtain balanced and high nonlinearity Boolean functions. $\mathbb{Z}_4$ codes, Galois Rings and Difference Sets over $\mathbb{Z}_4$ seems to offer great investment opportunities and reinforce our motivation to go on with this new kind of approach.

References

[1] A. Canteau, M. Trabbia: *Improved fast correlation attacks using parity-check equations of weight 4 and 5*, Advances in Cryptology, EUROCRYPT 2000, LNCS, **1807** (2000), 573–588.

[2] C. Carlet: *On Bent and highly nonlinear balanced/resilient functions and their algebraic immunities*, AAECC - LNCS, **3857** (2006), 1–28.

[3] C. Carlet, S. Dubuc: *On generalized Bent and q-ary perfect nonlinear functions*, Finite Fields and Applications **1999**, (2001), 81–94.

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

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

[6] N. Courtois, J. Pieprzyk: *Cryptanalysis of block ciphers with over-defined systems of equations*, Advances in Cryptology, ASIACRYPT 2002, LNCS, **2501** (2002), 267–287.

[7] C. Ding, G. Xiao, W. Shan: *The Stability Theory of Stream Ciphers*, LNCS, Springer, Berlin, 1991.

[8] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J .A. Sloane, P. Solé: *The $\mathbb{Z}_4$ linearity of Kerdock, Preparata, Goethals and related codes*, IEEE Transactions on Information Theory **40** (2) (1994), 301–319.

[9] X. D. Hou: *p-ary and q-ary versions of certain results about Bent functions and resilient functions*, Finite Fields and Applications **10** (2004), 566–582.

[10] X. D. Hou: *q-ary Bent functions constructed from chain rings*, Finite Fields and Applications **4** (1998), 55–61.

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

[12] P. V. Kumar, T. Hellesth , A. R. Calderbank, A. R. Hammons: *Large Families of Quaternary Sequences with Low Correlation*, IEEE Transactions on Information Theory **42** (2) (1996), 579–592.

[13] S. Kavut, S. Maitra, S. Sarkar, M. D. Yücel: *Enumeration of* 9*-variables rotation symetric Boolean functions having non-linearity* $>$ 240, Advances in Cryptology, INDOCRYPT 2006, LNCS, **4329** (2006), 266–279.

[14] P. V. Kumar, R. A. Scholtz, L. R. Welch: *Generalized Bent Functions and Their Properties*, Journal of Combinatorial Theory, Ser. A, **1** (40) (1985), 90–107.

[15] N. Li, W. F. Qi: *Construction and analysis of Boolean functions of* $2t+1$ *variables with maximum algebraic immunity*, Advances in Cryptology, ASIACRYPT 2006, LNCS, **4284** (2006), 84–98.

[16] W. Meier, E. Pasalic, C. Carlet: *Algebraic attacks and decomposition of Boolean functions*, Advances in Cryptology, EUROCRYPT 2004, LNCS, **3027** (2004), 474–491.

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

[18] Z. Saber, M. F. Uddin and A. Youssef: *On the existence of* $(9,3,5,240)$ *resilient functions*, IEEE Transactions on Information Theory **52** (5) (2006), 2269–2270.

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

[20] B. R. McDonald: *Finite Rings with Identity*, Marcel Dekker Inc., 1974.

Zoubida Jadda, CREC, UR - MACCLIA, Ecoles Militaires Saint-Cyr Coëtquidan, France,
e-mail: zoubida.jadda@st-cyr.terre-net.defense.gouv.fr

Patrice Parraud, CREC, UR - MACCLIA, Ecoles Militaires Saint-Cyr Coëtquidan, France,
e-mail: patrice.parraud@st-cyr.terre-net.defense.gouv.fr