Quaternary Cryptographic Bent Functions and their Binary projection

JADDA Zoubida[1] QARBOUA Soukayna[2] PARRAUD Patrice[1]

[1] Ecoles Militaires de Saint-Cyr Coëtquidan, FRANCE
CREC, UR - MACCLIA
zoubida.jadda@st-cyr.terre-net.defense.gouv.fr
patrice.parraud@st-cyr.terre-net.defense.gouv.fr

[2] LMIA, Faculty of Sciences, University of Mohamed V Agdal, Rabat, Morocco
soukayna.qarboua@gmail.com

JOURNÉES C2, OCTOBER 2012 / DINARD

The aim of this work

m-variables quaternary functions(F, m)
$F : GR(4, m) \to \mathbb{Z}_4 \qquad \mathbb{Z}_4 = \{0, 1, 2, 3\}$

$n-$ variables boolean functions(f, n)
$f : \mathbb{F}_2^n \to \mathbb{F}_2 \qquad (\mathbb{F}_2 = \{0, 1\})$

The quaternary approach (CONSTRUCTION):

- GALOIS rings $R = GR(4, m)$.
- CRYPTOGRAPHIC properties .
- Characterization of a family of quaternary CRYPTOGRAPHIC functions.

From $\mathbb{Z}_4$ to $\mathbb{F}_2$ (APPLICATION):

- The binary projection.
- Drived boolean cryptographic functions.

The aim of this work

m-variables quaternary functions(F, m)
$F : GR(4, m) \to \mathbb{Z}_4 \qquad \mathbb{Z}_4 = \{0, 1, 2, 3\}$

$n-$ variables boolean functions(f, n)
$f : \mathbb{F}_2^n \to \mathbb{F}_2 \qquad (\mathbb{F}_2 = \{0, 1\})$

The quaternary approach (CONSTRUCTION):

- GALOIS rings $R = GR(4, m)$.
- CRYPTOGRAPHIC properties .
- Characterization of a family of quaternary CRYPTOGRAPHIC functions.

From $\mathbb{Z}_4$ to $\mathbb{F}_2$ (APPLICATION):

- The binary projection.
- Drived boolean cryptographic functions.

The aim of this work

m-variables quaternary functions(F, m)
$F : GR(4, m) \rightarrow \mathbb{Z}_4 \quad \mathbb{Z}_4 = \{0, 1, 2, 3\}$

$n -$ variables boolean functions(f, n)
$f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2 \quad (\mathbb{F}_2 = \{0, 1\})$

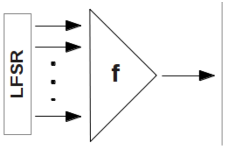
The quaternary approach (CONSTRUCTION):

- GALOIS rings $R = GR(4, m)$.
- CRYPTOGRAPHIC properties .
- Characterization of a family of quaternary CRYPTOGRAPHIC functions.

From $\mathbb{Z}_4$ to $\mathbb{F}_2$ (APPLICATION):

- The binary projection.
- Drived boolean cryptographic functions.

CONTEXT:



The aim of this work

m-variables quaternary functions(F, m)
$F : GR(4, m) \rightarrow \mathbb{Z}_4 \quad \mathbb{Z}_4 = \{0, 1, 2, 3\}$

$n -$ variables boolean functions(f, n)
$f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2 \quad (\mathbb{F}_2 = \{0, 1\})$

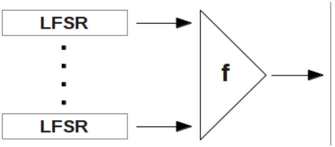
The quaternary approach (CONSTRUCTION):

- GALOIS rings $R = GR(4, m)$.
- CRYPTOGRAPHIC properties .
- Characterization of a family of quaternary CRYPTOGRAPHIC functions.

From $\mathbb{Z}_4$ to $\mathbb{F}_2$ (APPLICATION):

- The binary projection.
- Drived boolean cryptographic functions.

CONTEXT:



Outline

Outline

Outline

Outline

Outline

outline

Boolean functions

Let $f : \mathbb{F}_2^n \longmapsto \mathbb{F}_2$

- Truth table : $[f(0, \cdots, 0), \cdots, f(1, \cdots, 1)]_{2^n}$
- Support : $supp(f) = \{u \in \mathbb{F}_2^n \mid f(u) \neq 0\}$
- Weight : $w_H(f) = \mid supp(f) \mid$
- HAMMING metric : $d_H(f, g) = w_H(f \oplus g)_{(\oplus = + mod(2))}$

Boolean functions

Let $f : \mathbb{F}_2^n \longmapsto \mathbb{F}_2$

- Truth table : $[f(0,\cdots,0),\cdots,f(1,\cdots,1)]_{2^n}$
- Support : $supp(f) = \{u \in \mathbb{F}_2^n \mid f(u) \neq 0\}$
- Weight : $w_H(f) = \mid supp(f) \mid$
- HAMMING metric : $d_H(f,g) = w_H(f \oplus g)_{(\oplus = +mod(2))}$

CRYPTOGRAPHIC PROPERTIES.

Walsh transform : $W_f(u) = \sum_{v \in \mathbb{F}_2^n} (-1)^{u.v}(-1)^{f(v)},\ u \in \mathbb{F}_2^n$

Balancedness : $w_H(f) = 2^{n-1} \iff W_f(0) = 0$

Nonlinearity : $nl_2(f) = \min_{g\ affine} d_H(f,g) \iff nl_2(f) = 2^{n-1} - \frac{1}{2}\max_{u \in \mathbb{F}_2^n} |W_f(u)|$

Boolean functions

Let $f : \mathbb{F}_2^n \longmapsto \mathbb{F}_2$

- Truth table : $[f(0,\cdots,0),\cdots,f(1,\cdots,1)]_{2^n}$
- Support : $supp(f) = \{u \in \mathbb{F}_2^n \mid f(u) \neq 0\}$
- Weight : $w_H(f) = \mid supp(f) \mid$
- HAMMING metric : $d_H(f,g) = w_H(f \oplus g)_{(\oplus = + mod(2))}$

CRYPTOGRAPHIC PROPERTIES.

Walsh transform : $W_f(u) = \sum_{v \in \mathbb{F}_2^n} (-1)^{u.v}(-1)^{f(v)}, \; u \in \mathbb{F}_2^n$

Balancedness : $w_H(f) = 2^{n-1} \iff W_f(0) = 0$

Nonlinearity : $nl_2(f) = \min_{g \text{ affine}} d_H(f,g) \iff nl_2(f) = 2^{n-1} - \frac{1}{2}\max_{u \in \mathbb{F}_2^n} |W_f(u)|$

f is bent $\iff \forall u \in \mathbb{F}_2^n, \quad |W_f(u)| = 2^{\frac{n}{2}}$.

Maximal nonlinearity $(2^{n-1} - 2^{\frac{n}{2}-1})$ for n even but (not balanced).

Quaternary functions

Let $F, G \in \mathcal{F}(\mathbb{Z}_4^m, \mathbb{Z}_4) : \mathbb{Z}_4^m \longmapsto \mathbb{Z}_4$

The ring of integers modulus 4 — The group of 4^{th} root of unity in $\mathbb{C}$

$$\mathbb{Z}_4 = \mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\} \overset{group}{\sim} \mathbb{U}_4 = \{\pm 1, \pm i\} \quad i^2 = -1$$

Quaternary functions

Let $F, G \in \mathcal{F}(\mathbb{Z}_4^m, \mathbb{Z}_4) : \mathbb{Z}_4^m \longmapsto \mathbb{Z}_4$

The ring of integers modulus 4 — The group of 4^{th} root of unity in $\mathbb{C}$

$$\mathbb{Z}_4 = \mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\} \overset{group}{\sim} \mathbb{U}_4 = \{\pm 1, \pm i\} \quad i^2 = -1$$

- Truth table : $[F(0, \cdots, 0), \cdots, F(1, \cdots, 1)]_{4^m}$
- Relative support : $supp_j(F) = \{u \in \mathbb{Z}_4^m \mid F(u) = j\}_{0 \le j \le 3}$
- Relative cardinal : $\eta_j(F) =\mid supp_j(F) \mid$

LEE METRIC

$z \in \mathbb{Z}_4$	0	1	**2**	3
$w_L(z)$	0	1	**2**	1

- LEE Weight : $w_L(F) = \eta_1(F) + \mathbf{2}\eta_2(F) + \eta_3(F)$
- LEE Distance : $d_L(F, G) = w_L(F - G)_{[\text{"}-\text{"}\ mod(4)]}$

Quaternary functions

Let $F, G \in \mathcal{F}(\mathbb{Z}_4^m, \mathbb{Z}_4) : \mathbb{Z}_4^m \longmapsto \mathbb{Z}_4$

The ring of integers modulus 4 | The group of 4^{th} root of unity in $\mathbb{C}$

$$\mathbb{Z}_4 = \mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\} \overset{group}{\sim} \mathbb{U}_4 = \{\pm 1, \pm i\} \quad i^2 = -1$$

- Truth table : $[F(0, \cdots, 0), \cdots, F(1, \cdots, 1)]_{4^m}$
- Relative support : $supp_j(F) = \{u \in \mathbb{Z}_4^m \mid F(u) = j\}_{0 \leq j \leq 3}$
- Relative cardinal : $\eta_j(F) = \mid supp_j(F) \mid$

LEE METRIC

$z \in \mathbb{Z}_4$	0	1	**2**	3
$w_L(z)$	0	1	**2**	1

- LEE Weight : $w_L(F) = \eta_1(F) + \mathbf{2}\eta_2(F) + \eta_3(F)$
- LEE Distance : $d_L(F, G) = w_L(F - G)_{[" -" \ mod(4)]}$

WALSH TRANSFORM.

$$W_F(u) = \sum_{v \in \mathbb{Z}_4^n} i^{u.v} i^{F(v)}, \quad u \in \mathbb{Z}_4^n$$

$$W_F^2(u) = \sum_{v \in \mathbb{Z}_4^m} i^{u.v} (-1)^{F(v)}, \quad u \in \mathbb{Z}_4^n$$

Cryptographic properties.

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

The function F is **balanced** $\iff \eta_j(F) = 4^{m-1} \quad \forall j \in \{0,1,2,3\}$

$\iff W_F(0) = W_F^2(0) = 0$

The **nonlinearity** of F :

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

$$= 4^m - \max_{a \in \mathbb{Z}_4^m, b \in \mathbb{Z}_4} \left\{ Re(i^b W_F(a)) \right\}$$

CRYPTOGRAPHIC PROPERTIES.

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

The function F is **balanced** $\iff \eta_j(F) = 4^{m-1} \quad \forall j \in \{0,1,2,3\}$
$\iff W_F(0) = W_F^2(0) = 0$

The **nonlinearity** of F :

$$nl_4^L(F) = \min_{G \text{ affine}} d_L(F,G) = 4^m - \max_{a\in\mathbb{Z}_4^m, b\in\mathbb{Z}_4} \left\{ Re(i^b W_F(a)) \right\}$$

$$\boxed{F \text{ is bent} \iff \forall x \in \mathbb{Z}_4^m,\ |W_F(x)| = 2^m}$$

The nonlinearity of a **bent** function F is $nl_4^L(F) = 4^m - 2^m$.

outline

GALOIS Rings

THE MULTIPLICATIVE REPRESENTATION AND CYCLOTOMIC CLASSES

$$R \simeq \mathbb{Z}_4[x]/(g(x)) \ _{(b\_poly \text{ of deg } m)} \simeq \mathbb{Z}_4[\beta] \ _{(2^m-1^{th}\text{root of unity })} \simeq \mathbb{Z}_4^m$$

GALOIS Rings
THE MULTIPLICATIVE REPRESENTATION AND CYCLOTOMIC CLASSES

$$R \simeq \mathbb{Z}_4[x]/(g(x))\ _{(b\_poly \text{ of deg } m)} \simeq \mathbb{Z}_4[\beta]\ _{(2^m-1^{th}\text{root of unity })} \simeq \mathbb{Z}_4^m$$

$$GR(4,m) = R^*/\mathcal{T} \cup D \cup \mathcal{T}$$

$$\forall z \in R, \qquad z = \begin{cases} \beta^j & \text{if} \quad z \in \mathcal{T}^* \\ 2\beta^j & \text{if} \quad z \in D^* \\ \beta^i + 2\beta^j & \text{if} \quad z \in R^*/T \\ 0 & \text{if} \quad z = 0 \end{cases}$$

(Multiplicative representation)

$0 \leq j, i \leq 2^m - 2$

GALOIS Rings
THE MULTIPLICATIVE REPRESENTATION AND CYCLOTOMIC CLASSES

$$R \simeq \mathbb{Z}_4[x]/(g(x))_{\ (b\_poly \text{ of deg } m)} \simeq \mathbb{Z}_4[\beta]_{\ (2^m-1^{th} \text{root of unity })} \simeq \mathbb{Z}_4^m$$

$$GR(4,m) = R^*/\mathcal{T} \cup D \cup \mathcal{T}$$

$$\forall z \in R, \qquad z = \begin{cases} \beta^j & \text{if} \quad z \in \mathcal{T}^* \\ 2\beta^j & \text{if} \quad z \in D^* \\ \beta^i + 2\beta^j & \text{if} \quad z \in R^*/T \\ 0 & \text{if} \quad z = 0 \end{cases}$$

(Multiplicative representation)

$0 \leq j, i \leq 2^m - 2$

GALOIS Rings
THE MULTIPLICATIVE REPRESENTATION AND CYCLOTOMIC CLASSES

$$R \simeq \mathbb{Z}_4[x]/(g(x))_{\ (b\_poly \text{ of deg } m)} \simeq \mathbb{Z}_4[\beta]_{\ (2^m-1^{th} \text{root of unity})} \simeq \mathbb{Z}_4^m$$

$$GR(4,m) = R^*/\mathcal{T} \cup D \cup \mathcal{T}$$

$$\forall z \in R, \qquad z = \begin{cases} \beta^j & \text{if} \quad z \in \mathcal{T}^* \\ 2\beta^j & \text{if} \quad z \in D^* \\ \beta^i + 2\beta^j & \text{if} \quad z \in R^*/T \\ 0 & \text{if} \quad z = 0 \end{cases}$$

(Multiplicative representation)
$0 \leq j, i \leq 2^m - 2$

The 2^m-CYCLOTOMIC CLASSES $(C_j)_{0 \leq j \leq 2^m-1}$ of order $2^m - 1$ of R^* are defined by :

$$\begin{cases} C_j = \{\beta^l(1 + 2\beta^j),\ 0 \leq l \leq 2^m - 2\} \\ C_{2^m-1} = \{\beta^l,\ 0 \leq l \leq 2^m - 2\} \end{cases}$$

$$R = \cup_{j=0}^{2^m-1} C_j \cup D$$

Return

outline

The *m*-variables quaternary function

DEFINITION OF F_k :

$\forall k \in \{0, 1, .., 2^m - 2\}$

We define the *m*-variables quaternary function F_k as follow :

$$\begin{array}{cccl} F_k & : & R & \rightarrow & \mathbb{Z}_4 \\ & & a+2b & \rightarrow & F_k(a+2b) = h_k(\beta^k(1+2ba^{2^m-2})) \end{array}$$

where, $h_k : \mathfrak{C}_k \rightarrow \mathbb{Z}_4$ and $\mathfrak{C}_k = \{\beta^k\} \cup \{\beta^k(1+2\beta^j) \ , \ \ 0 \leq j \leq 2^m - 2\}$

The *m*-variables quaternary function

DEFINITION OF F_k :

$\forall k \in \{0, 1, .., 2^m - 2\}$

We define the *m*-variables quaternary function F_k as follow :

$$\begin{array}{rccl} F_k & : & R & \rightarrow & \mathbb{Z}_4 \\ & & a+2b & \rightarrow & F_k(a+2b) = h_k(\beta^k(1+2ba^{2^m-2})) \end{array}$$

where, $h_k : \mathfrak{C}_k \rightarrow \mathbb{Z}_4$ and $\mathfrak{C}_k = \{\beta^k\} \cup \{\beta^k(1+2\beta^j) \ , \ 0 \leq j \leq 2^m - 2\}$

CARACTERISATION OF F_k :

$$F_k(x) = \begin{cases} h_k(\beta^k(1+2\beta^j)) & \textit{if} \quad x \in C_j, \ 0 \leq j \leq 2^m - 2. \\ h_k(\beta^k) & \textit{if} \quad x \in C_{2^m-1} \cup D. \end{cases}$$

Go to

Conditions on the intern function h_k

Relation between bentness of F_k and his intern function h_k

$\forall k \in \{0, 1, .., 2^m - 2\}$

The q-ary function F_k is bent if

$$\forall x \in \mathcal{T} \begin{cases} \sum_{v \in \mathfrak{C}_k} i^{h_k(v)} = 0 & (1) \\ \left| \sum_{v \in \mathcal{T}} i^{h_k(\beta^k(1+2v)) + 3Tr(v \oplus x)} \right| = 2^{\frac{m}{2}} & (2) \end{cases}$$

with,

$$\forall a, b \in \mathcal{T}, \quad a \oplus b = a + b + 2(ab)^{2^{m-1}} \in \mathcal{T}$$

$$\forall z \in R, \quad Tr(z) = \sum_{l=0}^{m-1} \sigma^l(z) \quad \in \mathbb{Z}_4$$

Algebraic duality

Let note E^* the dual of $\mathcal{T}$, and $L(x,y) : \mathcal{T} \times \mathcal{T} \rightarrow 2\mathbb{F}_2$ a bilinear, symetric and nondegenerate function.

$$\text{if, } \forall x \in \mathcal{T} \begin{cases} l_1(x) = L(b_1, x) \\ l_2(x) = L(b_2, x) \\ l_3(x) = L(b_3, x) \end{cases}$$

are three balanced functions where $b_1 \neq b_2 \neq 0$ and, $b_3 = b_1 \oplus b_2$

Algebraic duality

Let note E^* the dual of $\mathcal{T}$, and $L(x,y) : \mathcal{T} \times \mathcal{T} \rightarrow 2\mathbb{F}_2$ a bilinear, symetric and nondegenerate function.

$$\text{if, } \forall x \in \mathcal{T} \begin{cases} l_1(x) = L(b_1, x) \\ l_2(x) = L(b_2, x) \\ l_3(x) = L(b_3, x) \end{cases}$$

are three balanced functions where $b_1 \neq b_2 \neq 0$ and, $b_3 = b_1 \oplus b_2$

Then the orthogonal of B=$\{0, b_1, b_2, b_3\}$ is :

$$\boxed{B^\perp = \{x \in \mathcal{T} \mid \forall l \in B^* : l(x) = 0\}, \; B^* = \{l_1, l_2\}}$$

And, if $\forall\, i \in \{1,2,3\} \quad b_i \notin B^\perp \Longrightarrow |B^\perp| = 2^{m-2}$

Algebraic duality

Let note E^* the dual of $\mathcal{T}$, and $L(x,y) : \mathcal{T} \times \mathcal{T} \to 2\mathbb{F}_2$ a bilinear, symetric and nondegenerate function.

$$\text{if, } \forall x \in \mathcal{T} \begin{cases} l_1(x) = L(b_1, x) \\ l_2(x) = L(b_2, x) \\ l_3(x) = L(b_3, x) \end{cases}$$

are three balanced functions where $b_1 \neq b_2 \neq 0$ and, $b_3 = b_1 \oplus b_2$

Then the orthogonal of B=$\{0, b_1, b_2, b_3\}$ is :

$$\boxed{B^\perp = \{x \in \mathcal{T} \mid \forall l \in B^* : l(x) = 0\}, \; B^* = \{l_1, l_2\}}$$

And, if $\forall\, i \in \{1,2,3\} \quad b_i \notin B^\perp \Longrightarrow |B^\perp| = 2^{m-2}$

Example of splitting:

Let $L(x,y) = 2Tr(xy)$ and $b_1 \neq b_2 \in \mathcal{T}^*$ with $Tr(b_1)$ is even and $Tr(b_1 b_2)$ is odd Then :

Algebraic duality

Let note E^* the dual of $\mathcal{T}$, and $L(x,y) : \mathcal{T} \times \mathcal{T} \to 2\mathbb{F}_2$ a bilinear, symetric and nondegenerate function.

if, $\forall x \in \mathcal{T} \begin{cases} l_1(x) = L(b_1, x) \\ l_2(x) = L(b_2, x) \\ l_3(x) = L(b_3, x) \end{cases}$ are three balanced functions where $b_1 \neq b_2 \neq 0$ and, $b_3 = b_1 \oplus b_2$

Then the orthogonal of B=$\{0, b_1, b_2, b_3\}$ is :

$$B^{\perp} = \{x \in \mathcal{T} \mid \forall l \in B^* : l(x) = 0\}, \; B^* = \{l_1, l_2\}$$

And, if $\forall\, i \in \{1,2,3\} \quad b_i \notin B^{\perp} \Longrightarrow |B^{\perp}| = 2^{m-2}$

Example of splitting:

Let $L(x,y) = 2Tr(xy)$ and $b_1 \neq b_2 \in \mathcal{T}^*$ with $Tr(b_1)$ is even and $Tr(b_1 b_2)$ is odd Then :

$$\mathcal{T} = B^{\perp} \oplus B = \cup_{i=0}^{3} b_i \oplus B^{\perp}$$

CONSTRUCTION OF h_k

Let $\alpha = (\alpha_0, \alpha_1, \alpha_2, \alpha_3) \in \mathbb{Z}_4^4$ such that:

$$(S_1) \quad \left\{ \begin{array}{lcl} | \, i^{\alpha_0} + i^{\alpha_1} + i^{\alpha_2} + i^{\alpha_3} \, | & = & 2 \\ | \, i^{\alpha_0} + i^{\alpha_1} - i^{\alpha_2} - i^{\alpha_3} \, | & = & 2 \\ | \, i^{\alpha_0} - i^{\alpha_1} + i^{\alpha_2} - i^{\alpha_3} \, | & = & 2 \\ | \, i^{\alpha_0} - i^{\alpha_1} - i^{\alpha_2} + i^{\alpha_3} \, | & = & 2 \end{array} \right.$$

and $b_1, b_2 \in \mathcal{T}^*$ defined in the splitting example.

CONSTRUCTION OF h_k

Let $\alpha = (\alpha_0, \alpha_1, \alpha_2, \alpha_3) \in \mathbb{Z}_4^4$ such that:

$$(S_1) \quad \begin{cases} \mid i^{\alpha_0} + i^{\alpha_1} + i^{\alpha_2} + i^{\alpha_3} \mid & = & 2 \\ \mid i^{\alpha_0} + i^{\alpha_1} - i^{\alpha_2} - i^{\alpha_3} \mid & = & 2 \\ \mid i^{\alpha_0} - i^{\alpha_1} + i^{\alpha_2} - i^{\alpha_3} \mid & = & 2 \\ \mid i^{\alpha_0} - i^{\alpha_1} - i^{\alpha_2} + i^{\alpha_3} \mid & = & 2 \end{cases}$$

and $b_1, b_2 \in \mathcal{T}^*$ defined in the splitting example.

$$\forall\, 0 \leq j \neq i \leq 3, \quad \alpha_i + Tr(b_i) \neq \alpha_j + Tr(b_j) \qquad (S_2)$$

CONSTRUCTION OF h_k

Let $\alpha = (\alpha_0, \alpha_1, \alpha_2, \alpha_3) \in \mathbb{Z}_4^4$ such that:

$$(S_1) \quad \left\{ \begin{array}{lcl} | \, i^{\alpha_0} + i^{\alpha_1} + i^{\alpha_2} + i^{\alpha_3} \, | & = & 2 \\ | \, i^{\alpha_0} + i^{\alpha_1} - i^{\alpha_2} - i^{\alpha_3} \, | & = & 2 \\ | \, i^{\alpha_0} - i^{\alpha_1} + i^{\alpha_2} - i^{\alpha_3} \, | & = & 2 \\ | \, i^{\alpha_0} - i^{\alpha_1} - i^{\alpha_2} + i^{\alpha_3} \, | & = & 2 \end{array} \right.$$

and $b_1, b_2 \in \mathcal{T}^*$ defined in the splitting example.

$$\forall\, 0 \leq j \neq i \leq 3, \quad \alpha_i + Tr(b_i) \neq \alpha_j + Tr(b_j) \qquad (S_2)$$

Then the intern function h_k defined by :

$$\forall j,\ 0 \leq j \leq 3,\ \forall x \in B^{\perp} \oplus b_j,\ h_k(\beta^k(1 + 2x)) = \alpha_j + Tr(b_j)$$

verifies the conditions (1) and (2) .

Construction of h_k

Let $\alpha = (\alpha_0, \alpha_1, \alpha_2, \alpha_3) \in \mathbb{Z}_4^4$ such that:

$$(S_1) \quad \left\{ \begin{array}{lcl} | \, i^{\alpha_0} + i^{\alpha_1} + i^{\alpha_2} + i^{\alpha_3} \, | & = & 2 \\ | \, i^{\alpha_0} + i^{\alpha_1} - i^{\alpha_2} - i^{\alpha_3} \, | & = & 2 \\ | \, i^{\alpha_0} - i^{\alpha_1} + i^{\alpha_2} - i^{\alpha_3} \, | & = & 2 \\ | \, i^{\alpha_0} - i^{\alpha_1} - i^{\alpha_2} + i^{\alpha_3} \, | & = & 2 \end{array} \right.$$

and $b_1, b_2 \in \mathcal{T}^*$ defined in the splitting example.

$$\forall\, 0 \leq j \neq i \leq 3, \quad \alpha_i + Tr(b_i) \neq \alpha_j + Tr(b_j) \qquad (S_2)$$

Then the intern function h_k defined by :

$$\forall j,\ 0 \leq j \leq 3,\ \forall x \in B^{\perp} \oplus b_j,\ h_k(\beta^k(1+2x)) = \alpha_j + Tr(b_j)$$

verifies the conditions (1) and (2) .

Let α a solution of (S_2) then $\alpha + i \mod 4$ and $\sigma^{13}(\alpha)$ are also solutions.

Solutions and models

We note a model a the vector (a_0, a_1, a_2, a_3) defined by:

$$\forall\, 0 \leq i \neq j \leq 3, \qquad a_j = \alpha_j + Tr(b_j) \quad \text{and} \quad a_i \neq a_j.$$

Solutions and models

We note a model a the vector (a_0, a_1, a_2, a_3) defined by:

$$\forall\, 0 \leq i \neq j \leq 3, \qquad a_j = \alpha_j + Tr(b_j) \quad \text{and} \quad a_i \neq a_j.$$

If a is a model $\Rightarrow \begin{cases} a + l \mod 4 & 0 \leq l \leq 3 \\ & \text{are} \\ \sigma^l(a) = (a_l, a_{l+1}, a_{l+2}, a_{l+3}) & \text{also models} \end{cases}$

Solutions and models

We note a model a the vector (a_0, a_1, a_2, a_3) defined by:

$$\forall\, 0 \leq i \neq j \leq 3, \qquad a_j = \alpha_j + Tr(b_j) \quad \text{and} \quad a_i \neq a_j.$$

If a is a model $\Rightarrow \begin{cases} a + l \mod 4 \\ \sigma^l(a) = (a_l, a_{l+1}, a_{l+2}, a_{l+3}) \end{cases}$ $0 \leq l \leq 3$ are also models

Forall balanced function h_k defined by :

$$h(\beta^k(1+2x)) = a_j \text{ if } x \in b_j \oplus B^{\perp} \ , \ \exists\, \alpha \text{ satisfying } (S_2)$$

Solutions and models

We note a model a the vector (a_0, a_1, a_2, a_3) defined by:

$$\forall\, 0 \leq i \neq j \leq 3, \qquad a_j = \alpha_j + Tr(b_j) \quad \text{and} \quad a_i \neq a_j.$$

If a is a model $\Rightarrow \begin{cases} a + l \mod 4 & 0 \leq l \leq 3 \\ & \text{are} \\ \sigma^l(a) = (a_l, a_{l+1}, a_{l+2}, a_{l+3}) & \text{also models} \end{cases}$

Forall balanced function h_k defined by :

$$h(\beta^k(1+2x) = a_j \text{ if } x \in b_j \oplus B^{\perp} \;,\; \exists\, \alpha \text{ satisfying } (S_2)$$

The quaternary Bent function, $F_k \;:\; R = \cup_{j=0}^{2^m-1} C_j \cup D \;\to\; \mathbb{Z}_4$

$$\begin{cases} F_k(C_j) & = & a_j \quad \text{if } \beta^j \in B^{\perp} \oplus b_j \\ F_k(D \cup \mathcal{T}^*) & = & a_0 \end{cases}$$

outline

The vector representation of elements of R

$$R = GR(4, m) = \mathcal{T}^* \cup D \cup (\cup_{j=0}^{2^m-2} C_j)$$

The vector representation of elements of R

$$R = GR(4,m) = \mathcal{T}^* \cup D \cup (\cup_{j=0}^{2^m-2} C_j) \overset{d}{\simeq} \mathbb{Z}_4[\beta] = E^* \cup W \cup (\cup_{j=0}^{2^m-2} V_j)$$

$\forall z \in R: \quad z = \sum_{j=0}^{m-1} z_j \beta^j$ $\quad \overset{z_j \in Z_4}{\text{(Additive representation)}}$

with, β a root of the *b_polynomial*

$$z \in \mathbb{Z}_4^m \begin{cases} E = & d(\mathcal{T}) & = & \{0\} \cup \{v_i,\ 0 \le i \le 2^m - 2\} \\ W = & d(D) & = & \{0\} \cup \{2v_i,\ 0 \le i \le 2^m - 2\}_{(v_i \times v_j = v_{i+j[2^m-1]})} \\ V_j = & d(C_j) & = & \{v_l(1+2v_j),\ 0 \le l \le 2^m - 2\} \end{cases}$$

The vector representation of elements of R

$$R = GR(4,m) = \mathcal{T}^* \cup D \cup (\cup_{j=0}^{2^m-2} C_j) \overset{d}{\simeq} \mathbb{Z}_4[\beta] = E^* \cup W \cup (\cup_{j=0}^{2^m-2} V_j)$$

$\forall z \in R: \quad z = \sum_{j=0}^{m-1} z_j \beta^j \quad \overset{z_j \in Z_4}{\text{(Additive representation)}}$

with, β a root of the b_polynomial

$$z \in \mathbb{Z}_4^m \begin{cases} E = & d(\mathcal{T}) & = & \{0\} \cup \{v_i,\ 0 \le i \le 2^m - 2\} \\ W = & d(D) & = & \{0\} \cup \{2v_i,\ 0 \le i \le 2^m - 2\}_{(v_i \times v_j = v_{i+j[2^m-1]})} \\ V_j = & d(C_j) & = & \{v_l(1 + 2v_j),\ 0 \le l \le 2^m - 2\} \end{cases}$$

The vector representation of elements of R

$$R = GR(4,m) = \mathcal{T}^* \cup D \cup (\cup_{j=0}^{2^m-2} C_j) \overset{d}{\simeq} \mathbb{Z}_4[\beta] = E^* \cup W \cup (\cup_{j=0}^{2^m-2} V_j)$$

$\forall z \in R: \quad z = \sum_{j=0}^{m-1} z_j \beta^j \qquad \overset{z_j \in Z_4}{\text{(Additive representation)}}$

with, β a root of the b_polynomial

$$z \in \mathbb{Z}_4^m \begin{cases} E = & d(\mathcal{T}) & = & \{0\} \cup \{v_i,\ 0 \leq i \leq 2^m - 2\} \\ W = & d(D) & = & \{0\} \cup \{2v_i,\ 0 \leq i \leq 2^m - 2\}_{(v_i \times v_j = v_{i+j[2^m-1]})} \\ V_j = & d(C_j) & = & \{v_l(1 + 2v_j),\ 0 \leq l \leq 2^m - 2\} \end{cases}$$

REDEFINITION OF F_k ($k \in \{0, 1, .., 2^m - 2\}$):

$$\begin{array}{lllll} \bar{F}_k & : & E^* \cup W \cup (\cup_{j=0}^{2^m-2} V_j) & \rightarrow & \mathbb{Z}_4 \\ & & u + 2v & \rightarrow & \bar{F}_k(u+2v) = F_k(d^{-1}(u+2v)) \end{array}$$

$$\bar{h}_k \quad : \quad d(\mathfrak{C}_k) \quad \rightarrow \quad \mathbb{Z}_4, \bar{h}_k(x) = h_k(d^{-1}(x))$$

The direct mapping between $\mathbb{Z}_4^m$ and $\mathbb{F}_2^{2m}$

FROM $\mathbb{Z}_4^m$ TO $F_2{}^{2m}$:

$$\begin{array}{cccc} \varphi & : & \mathbb{Z}_4^m & \rightarrow & \mathbb{F}_2^{2m} \\ & & u+2v & \rightarrow & \tilde{u} \parallel \tilde{v} \end{array}$$

is a bijection.

where ˜ is the component mod 2 reduction and $||$ is the concatenation.

The direct mapping between $\mathbb{Z}_4^m$ and $\mathbb{F}_2^{2m}$

FROM $\mathbb{Z}_4^m$ TO $F_2{}^{2m}$:

$$\begin{array}{cccc} \varphi & : & \mathbb{Z}_4^m & \rightarrow & \mathbb{F}_2^{2m} \\ & & u + 2v & \rightarrow & \tilde{u} \parallel \tilde{v} \end{array}$$

is a bijection.

where ˜ is the component mod 2 reduction and $||$ is the concatenation.

$$\mathbb{F}_2^{2m} = \varphi(\mathbb{Z}_4^m) = \cup_{j=0}^{2^m-2} \varphi(V_j) \cup \varphi(E^*) \cup \varphi(w)$$

The direct mapping between $\mathbb{Z}_4^m$ and $\mathbb{F}_2^{2m}$

FROM $\mathbb{Z}_4^m$ TO F_2^{2m}:

$$\varphi \; : \; \begin{array}{ccc} \mathbb{Z}_4^m & \rightarrow & \mathbb{F}_2^{2m} \\ u+2v & \rightarrow & \tilde{u} \parallel \tilde{v} \end{array}$$

is a bijection.

where ˜ is the component mod 2 reduction and $||$ is the concatenation.

$$\mathbb{F}_2^{2m} = \varphi(\mathbb{Z}_4^m) = \cup_{j=0}^{2^m-2} \varphi(V_j) \cup \varphi(E^*) \cup \varphi(w)$$

Let $\psi_{i \in \mathbb{N}}$ any mapping from $\mathbb{Z}_4$ to $\mathbb{F}_2$ such that :

$$\sum_{x \in \mathbb{Z}_4} (-1)^{\psi_i(x)} = 0$$

Example: $\psi_i(2q+r) = q$ or $\psi_i(2q+r) = q+r \pmod 2$.

The $2m$-variables Derived boolean functions

DEFINITION OF f :

The $2m$-variables boolean function f derived from the quaternary constructed function F_k and defined as :

$$\begin{array}{cccc} f & : & \mathbb{F}_2^{2m} & \rightarrow & \mathbb{F}_2 \\ & & x & \mapsto & \psi_i(\bar{F}_k(\varphi^{-1}(x))) \end{array}$$ is bent.

The $2m$-variables Derived boolean functions

Definition of f :

The $2m$-variables boolean function f derived from the quaternary constructed function F_k and defined as :

$$\begin{array}{cccc} f & : & \mathbb{F}_2^{2m} & \rightarrow & \mathbb{F}_2 \\ & & x & \mapsto & \psi_i(\bar{F}_k(\varphi^{-1}(x))) \end{array} \quad \text{is bent.}$$

Caracterisation of f :

$$\forall(\tilde{u}||\tilde{v}) \in \mathbb{F}_2^{2m} = \varphi(\mathbb{Z}_4^m) = \cup_{j=0}^{2^m-2}\varphi(V_j) \cup \varphi(E^*) \cup \varphi(w)$$

$$f(\tilde{u}||\tilde{v}) = \begin{cases} \psi_i(\bar{h}_k(v_k(v_0 + 2v_j)) & \textit{if} \quad \varphi^{-1}(\tilde{u}||\tilde{v}) \in V_{j_{0\leq j\leq 2^m-2}} \\ \psi_i(\bar{h}_k(v_k)) & \textit{if} \quad \varphi^{-1}(\tilde{u}||\tilde{v}) \in E^* \cup W \end{cases}$$

The $2m+1$-variables derived boolean functions

DEFINITION OF f :

The derived boolean function f defined as :

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

has maximal nonlinearity equal to $4^m - 2^{m+1}$.

The $2m+1$-variables derived boolean functions

DEFINITION OF f :

The derived boolean function f defined as :

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

has maximal nonlinearity equal to $4^m - 2^{m+1}$.

CARACTERISATION OF f :

$$\forall(\tilde{u}||\tilde{v}||\varepsilon) \in \mathbb{F}_2^{2m+1} = \varphi(\mathbb{Z}_4^m)||\varepsilon = \cup_{j=0}^{2^m-2}\varphi(V_j)||\varepsilon \cup \varphi(E^*)||\varepsilon \cup \varphi(w)||\varepsilon$$

$$f(\tilde{u}||\tilde{v}||\varepsilon) = \begin{cases} \psi_\varepsilon(\bar{h}_k(v_k(v_0+2v_j))) & \textit{if} \quad \tilde{u}||\tilde{v}||\varepsilon \in \varphi(V_j)||\varepsilon, \ 0 \leq j \leq 2^m-2 \\ \psi_\varepsilon(\bar{h}_k(\varphi^{-1}(v_k))) & \textit{if} \quad \tilde{u}||\tilde{v}||\varepsilon \in \varphi(E^*)||\varepsilon \cup \varphi(W)||\varepsilon \end{cases}$$

outline

Example of construction (GALOIS Ring)

$$(a_0, a_1, a_2 a_3) = (0, 2, 1, 3)$$

Example of construction (GALOIS Ring)

$$(a_0, a_1, a_2 a_3) = (0, 2, 1, 3)$$

$$R = GR(4,3) \overset{d}{\simeq} \mathbb{Z}_{\mathbf{4}}[\beta],$$

$g(x) = x^3 + 2x^2 + x + 3$, with β be a root of $g(x)$ of order 7 .

Example of construction (Galois Ring)

$$(a_0, a_1, a_2 a_3) = (0, 2, 1, 3)$$

$$R = GR(4,3) \overset{d}{\simeq} \mathbb{Z}_{\mathbf{4}}[\beta],$$

$g(x) = x^3 + 2x^2 + x + 3$, with β be a root of $g(x)$ of order 7 .

$\mathcal{T}^*$ E*	1 { 1, 0, 0 }	β { 0, 1, 0 }	β^2 { 0, 0, 1 }	β^3 { 1, 3, 2 }	β^4 { 2, 3, 3 }	β^5 { 3, 3, 1 }	β^6 { 1, 2, 1 }
D^* W*	2 { 2, 0, 0 }	2β { 0, 2, 0 }	$2\beta^2$ { 0, 0, 2 }	$2\beta^3$ { 2, 2, 0 }	$2\beta^4$ { 0, 2, 2 }	$2\beta^5$ { 2, 2, 2 }	$2\beta^6$ { 2, 0, 2 }
C_0	3	3β	$3\beta^2$	$3\beta^3$	$3\beta^4$	$3\beta^5$	$3\beta^6$
C_1	$1+2\beta$	$\beta+2\beta^2$	$\beta^2+2\beta^3$	$\beta^3+2\beta^4$	$\beta^4+2\beta^5$	$\beta^5+2\beta^6$	β^6+2
C_2	$1+2\beta^2$	$\beta+2\beta^3$	$\beta^2+2\beta^4$	$\beta^3+2\beta^5$	$\beta^4+2\beta^6$	β^5+2	$\beta^6+2\beta$
C_3	$1+2\beta^3$	$\beta+2\beta^4$	$\beta^2+2\beta^5$	$\beta^3+2\beta^6$	β^4+2	$\beta^5+2\beta$	$\beta^6+2\beta^2$
C_4	$1+2\beta^4$	$\beta+2\beta^5$	$\beta^2+2\beta^6$	β^3+2	$\beta^4+2\beta$	$\beta^5+2\beta^2$	$\beta^6+2\beta^3$
C_5	$1+2\beta^5$	$\beta+2\beta^6$	β^2+2	$\beta^3+2\beta$	$\beta^4+2\beta^2$	$\beta^5+2\beta^3$	$\beta^6+2\beta^4$
C_6	$1+2\beta^6$	$\beta+2$	$\beta^2+2\beta$	$\beta^3+2\beta^2$	$\beta^4+2\beta^3$	$\beta^5+2\beta^4$	$\beta^6+2\beta^5$

Example of construction (GALOIS Ring)

$$(a_0, a_1, a_2 a_3) = (0, 2, 1, 3)$$

$$R = GR(4,3) \overset{d}{\simeq} \mathbb{Z}_4[\beta],$$

$g(x) = x^3 + 2x^2 + x + 3$, with β be a root of $g(x)$ of order 7 .

$\mathcal{T}^*$	1	β	β^2	β^3	β^4	β^5	β^6
E*	**{ 1, 0, 0 }**	**{ 0, 1, 0 }**	**{ 0, 0, 1 }**	**{ 1, 3, 2 }**	**{ 2, 3, 3 }**	**{ 3, 3, 1 }**	**{ 1, 2, 1 }**
D^*	2	2β	$2\beta^2$	$2\beta^3$	$2\beta^4$	$2\beta^5$	$2\beta^6$
W*	**{ 2, 0, 0 }**	**{ 0, 2, 0 }**	**{ 0, 0, 2 }**	**{ 2, 2, 0 }**	**{ 0, 2, 2 }**	**{ 2, 2, 2 }**	**{ 2, 0, 2 }**
C_0	3	3β	$3\beta^2$	$3\beta^3$	$3\beta^4$	$3\beta^5$	$3\beta^6$
$\mathbf{V}_0$	$\{3,0,0\}$	$\{0,3,0\}$	$\{0,0,3\}$	$\{3,1,2\}$	$\{2,1,1\}$	$\{1,1,3\}$	$\{3,2,3\}$
C_1	$1+2\beta$	$\beta+2\beta^2$	$\beta^2+2\beta^3$	$\beta^3+2\beta^4$	$\beta^4+2\beta^5$	$\beta^5+2\beta^6$	β^6+2
$\mathbf{V}_1$	$\{1,2,0\}$	$\{0,1,2\}$	$\{2,2,1\}$	$\{1,1,0\}$	$\{0,1,1\}$	$\{1,3,3\}$	$\{3,2,1\}$
C_2	$1+2\beta^2$	$\beta+2\beta^3$	$\beta^2+2\beta^4$	$\beta^3+2\beta^5$	$\beta^4+2\beta^6$	β^5+2	$\beta^6+2\beta$
$\mathbf{V}_2$	$\{1,0,2\}$	$\{2,3,0\}$	$\{0,2,3\}$	$\{3,1,0\}$	$\{0,3,1\}$	$\{1,3,1\}$	$\{1,0,1\}$
C_3	$1+2\beta^3$	$\beta+2\beta^4$	$\beta^2+2\beta^5$	$\beta^3+2\beta^6$	β^4+2	$\beta^5+2\beta$	$\beta^6+2\beta^2$
$\mathbf{V}_3$	$\{3,2,0\}$	$\{0,3,2\}$	$\{2,2,3\}$	$\{3,3,0\}$	$\{0,3,3\}$	$\{3,1,1\}$	$\{1,2,3\}$
C_4	$1+2\beta^4$	$\beta+2\beta^5$	$\beta^2+2\beta^6$	β^3+2	$\beta^4+2\beta$	$\beta^5+2\beta^2$	$\beta^6+2\beta^3$
$\mathbf{V}_4$	$\{1,2,2\}$	$\{2,3,2\}$	$\{2,0,3\}$	$\{3,3,2\}$	$\{2,1,3\}$	$\{3,3,3\}$	$\{3,0,1\}$
C_5	$1+2\beta^5$	$\beta+2\beta^6$	β^2+2	$\beta^3+2\beta$	$\beta^4+2\beta^2$	$\beta^5+2\beta^3$	$\beta^6+2\beta^4$
$\mathbf{V}_5$	$\{3,2,2\}$	$\{2,1,2\}$	$\{2,0,1\}$	$\{1,1,2\}$	$\{2,3,1\}$	$\{1,1,1\}$	$\{1,0,3\}$
C_6	$1+2\beta^6$	$\beta+2$	$\beta^2+2\beta$	$\beta^3+2\beta^2$	$\beta^4+2\beta^3$	$\beta^5+2\beta^4$	$\beta^6+2\beta^5$
$\mathbf{V}_6$	$\{3,0,2\}$	$\{2,1,0\}$	$\{0,2,1\}$	$\{1,3,0\}$	$\{0,1,3\}$	$\{3,1,3\}$	$\{3,0,3\}$

Choice of b_1 and b_2

$b_i \in \mathcal{T}$	1	β	β^2	β^3	β^4	β^5	β^6	0
$Tr(b_i)$	3	2	2	1	2	1	1	0

Choice of b_1 and b_2

$b_i \in \mathcal{T}$	1	β	β^2	β^3	β^4	β^5	β^6	0
$Tr(b_i)$	3	2	2	1	2	1	1	0

We can choose $b_1 = ?$ and $b_2 = ?$ and $b_3 = b_1 \oplus b_2 = ?$

Choice of b_1 and b_2

$b_i \in \mathcal{T}$	1	β	β^2	β^3	β^4	β^5	β^6	0
$Tr(b_i)$	3	2	2	1	2	1	1	0

We can choose $b_1 = ?$ and $b_2 = ?$ and $b_3 = b_1 \oplus b_2 = ?$

$\oplus$	b_1	1	β	β^2	β^3	β^4	β^5	β^6	0
b_2									
1		0	β^3	β^6	β	β^5	β^4	β^2	1
β		β^3	0	β^4	1	β^2	β^6	β^5	β
β^2		β^6	β^4	0	β^5	β	β^3	1	β^2
β^3		β	1	β^5	0	β^6	β^2	β^4	β^3
β^4		β^5	β^2	β	β^6	0	1	β^3	β^4
β^5		β^4	β^6	β^3	β^2	1	0	β	β^5
β^6		β^2	β^5	1	β^4	β^3	β	0	β^6
0		1	β	β^2	β^3	β^4	β^5	β^6	0

Choice of b_1 and b_2

$b_i \in \mathcal{T}$	1	β	β^2	β^3	β^4	β^5	β^6	0
$Tr(b_i)$	3	2	2	1	2	1	1	0

We can choose $b_1 = \beta^2$ and $b_2 = \beta^3$ and $b_3 = b_1 \oplus b_2 = \beta^5$

$\oplus$	b_1	1	β	β^2	β^3	β^4	β^5	β^6	0
b_2									
1		0	β^3	β^6	β	β^5	β^4	β^2	1
β		β^3	0	β^4	1	β^2	β^6	β^5	β
β^2		β^6	β^4	0	β^5	β	β^3	1	β^2
β^3		β	1	β^5	0	β^6	β^2	β^4	β^3
β^4		β^5	β^2	β	β^6	0	1	β^3	β^4
β^5		β^4	β^6	β^3	β^2	1	0	β	β^5
β^6		β^2	β^5	1	β^4	β^3	β	0	β^6
0		1	β	β^2	β^3	β^4	β^5	β^6	0

Choice of b_1 and b_2

$b_i \in \mathcal{T}$	1	β	β^2	β^3	β^4	β^5	β^6	0
$Tr(b_i)$	3	2	2	1	2	1	1	0

We can choose $b_1 = \beta^2$ and $b_2 = \beta^3$ and $b_3 = b_1 \oplus b_2 = \beta^5$

$\oplus$	b_1	1	β	β^2	β^3	β^4	β^5	β^6	0
b_2									
1		0	β^3	β^6	β	β^5	β^4	β^2	1
β		β^3	0	β^4	1	β^2	β^6	β^5	β
β^2		β^6	β^4	0	β^5	β	β^3	1	β^2
β^3		β	1	β^5	0	β^6	β^2	β^4	β^3
β^4		β^5	β^2	β	β^6	0	1	β^3	β^4
β^5		β^4	β^6	β^3	β^2	1	0	β	β^5
β^6		β^2	β^5	1	β^4	β^3	β	0	β^6
0		1	β	β^2	β^3	β^4	β^5	β^6	0

We have $\mathcal{T} = \cup_{i=0}^{3} B^\perp \oplus b_i$ and $B^\perp = \{x \in \mathcal{T}\,,\; 2Tr(xb_1) = 2Tr(xb_2) = 0\}$

$$\begin{aligned} B^\perp \oplus b_0 &= \{0, \beta^6\} \\ B^\perp \oplus b_1 &= \{\beta^2, 1\} \\ B^\perp \oplus b_2 &= \{\beta^3, \beta^4\} \\ B^\perp \oplus b_3 &= \{\beta^5, \beta\} \end{aligned}$$

Then we can definie explicitly our quaternary function like that:

$$\forall x \in R,\ F_k(x) = \begin{cases} 0 & \textit{if } x \in \cup C_6 \cup D \cup \mathcal{T}^* \\ 2 & \textit{if } x \in \cup C_2 \cup C_0 \\ 1 & \textit{if } x \in \cup C_3 \cup C_4 \\ 3 & \textit{if } x \in \cup C_5 \cup C_1 \end{cases}$$

Then we can definie explicitly our quaternary function like that:

$$\forall x \in R,\ F_k(x) = \begin{cases} 0 & \textit{if } x \in \cup C_6 \cup D \cup \mathcal{T}^* \\ 2 & \textit{if } x \in \cup C_2 \cup C_0 \\ 1 & \textit{if } x \in \cup C_3 \cup C_4 \\ 3 & \textit{if } x \in \cup C_5 \cup C_1 \end{cases}$$

Then $\bar{F}$ is defined such that:

$$\forall x \in \mathbb{Z}_4^m,\ \bar{F}_k(x) = \begin{cases} 0 & \textit{if } x \in \cup V_6 \cup W \cup E^* \\ 2 & \textit{if } x \in \cup V_2 \cup V_0 \\ 1 & \textit{if } x \in \cup V_3 \cup V_4 \\ 3 & \textit{if } x \in \cup V_5 \cup V_1 \end{cases}$$

Let $\psi : \mathbb{Z}_4 \to \mathbb{F}_2$,$\psi(2q + r) = q$ then :

Let $\psi : \mathbb{Z}_4 \rightarrow \mathbb{F}_2$,$\psi(2q + r) = q$ then :
The $2m$-Derived boolean function it's constructed like that:

$$\forall x \in \mathbb{Z}_4^m,\ f(\varphi(x)) = \begin{cases} 0 & if\ \varphi(x) \in \cup\varphi(V_6) \cup \varphi(W) \cup \varphi(E^*) \\ 1 & if\ \varphi(x) \in \cup\varphi(V_2) \cup \varphi(V_0) \\ 0 & if\ \varphi(x) \in \cup\varphi(V_3) \cup \varphi(V_4) \\ 1 & if\ \varphi(x) \in \cup\varphi(V_5) \cup \varphi(V_1) \end{cases}$$

Let $\psi : \mathbb{Z}_4 \to \mathbb{F}_2$,$\psi(2q+r) = q$ then :
The $2m$-Derived boolean function it's constructed like that:

$$\forall x \in \mathbb{Z}_4^m,\ f(\varphi(x)) = \begin{cases} 0 & \text{if } \varphi(x) \in \cup\varphi(V_6) \cup \varphi(W) \cup \varphi(E^*) \\ 1 & \text{if } \varphi(x) \in \cup\varphi(V_2) \cup \varphi(V_0) \\ 0 & \text{if } \varphi(x) \in \cup\varphi(V_3) \cup \varphi(V_4) \\ 1 & \text{if } \varphi(x) \in \cup\varphi(V_5) \cup \varphi(V_1) \end{cases}$$

Let $\psi_{\varepsilon\in\{0,1\}} : \mathbb{Z}_4 \to \mathbb{F}_2$, $\psi_\varepsilon(2q+r) = q * \varepsilon + \bar{\varepsilon} * r$ then:
The $2m+1$-Derived boolean function it's defined like that:

Let $\psi : \mathbb{Z}_4 \rightarrow \mathbb{F}_2$,$\psi(2q + r) = q$ then :
The $2m$-Derived boolean function it's constructed like that:

$$\forall x \in \mathbb{Z}_4^m,\ f(\varphi(x)) = \begin{cases} 0 & \text{if } \varphi(x) \in \cup\varphi(V_6) \cup \varphi(W) \cup \varphi(E^*) \\ 1 & \text{if } \varphi(x) \in \cup\varphi(V_2) \cup \varphi(V_0) \\ 0 & \text{if } \varphi(x) \in \cup\varphi(V_3) \cup \varphi(V_4) \\ 1 & \text{if } \varphi(x) \in \cup\varphi(V_5) \cup \varphi(V_1) \end{cases}$$

Let $\psi_{\varepsilon\in\{0,1\}} : \mathbb{Z}_4 \rightarrow \mathbb{F}_2$, $\psi_\varepsilon(2q + r) = q * \varepsilon + \bar{\varepsilon} * r$ then:
The $2m + 1$-Derived boolean function it's defined like that:

$$\forall x \in \mathbb{Z}_4^m,\ f(\varphi(x)||\varepsilon) = \begin{cases} 0 & \text{if } \varphi(x)||\varepsilon \in \cup\varphi(V_6)_\varepsilon \cup \varphi(W)_\varepsilon \cup \varphi(E^*)_\varepsilon \\ \varepsilon & \text{if } \varphi(x)||\varepsilon \in \cup\varphi(V_2)_\varepsilon \cup \varphi(V_0)_\varepsilon \\ \bar{\varepsilon} & \text{if } \varphi(x)||\varepsilon \in \cup\varphi(V_3)_\varepsilon \cup \varphi(V_4)_\varepsilon \\ \varepsilon + \bar{\varepsilon} & \text{if } \varphi(x)||\varepsilon \in \cup\varphi(V_5)_\varepsilon \cup \varphi(V_1)_\varepsilon \end{cases}$$

Conclusion

- THE QUATERNARY FUNCTION:

$$\begin{array}{rcll} F_k & : & R = GR(4,m) & \to \mathbb{Z}_4 \\ & & a + 2b & \to F_k(a+2b) = h_k(\beta^k(1+2ba^{2^m-2})) \end{array}$$

with $\forall k,\ 0 \leq k \leq 2^m - 2,\ h_k : \mathfrak{C}_k \to \mathbb{Z}_4$

Conclusion

- THE QUATERNARY FUNCTION:

$$\begin{array}{rcccl} F_k & : & R = GR(4,m) & \rightarrow & \mathbb{Z}_4 \\ & & a + 2b & \rightarrow & F_k(a+2b) = h_k(\beta^k(1+2ba^{2^m-2})) \end{array}$$

with $\forall k,\ 0 \leq k \leq 2^m - 2,\ h_k : \mathfrak{C}_k \rightarrow \mathbb{Z}_4$

- THE BINARY PROJECTIONS:

$$\begin{array}{rcl} f : \mathbb{F}_2^{2m} & \rightarrow & \mathbb{F}_2 \\ x & \rightarrow & \psi_i(F_k(d^{-1}(\varphi^{-1}(x)))) \end{array}$$

$$\begin{array}{rcl} f : \mathbb{F}_2^{2m+1} & \rightarrow & \mathbb{F}_2 \\ x||\varepsilon & \rightarrow & \psi_\varepsilon(F_k(d^{-1}(\varphi^{-1}(x)))) \end{array}$$

with $R \xrightarrow{d} \mathbb{Z}_4^m \xrightarrow{\varphi} \mathbb{F}_2^{2m}$ and $\psi, \psi_\varepsilon : \mathbb{Z}_4 \xrightarrow{balanced} \mathbb{F}_2$