Objets combinatoires en cryptographie et en théorie des codes

Sihem Mesnager

Université Paris VIII et XIII, Département de Mathématiques
LAGA (Laboratoire Analyse, Géométrie et Applications),
Équipe MTII (Mathématiques pour le Traitement de l'Information et de l'Image)

Séminaire LIPN Université Paris XIII
13 Mai 2014, Villetaneuse, France

Recherche en combinatoire

1. Étude d'objets combinatoires en cryptographie et codes correcteurs
2. Étude de problèmes issus de la théorie de l'information en utilisant des outils combinatoires et des idées venant de la combinatoire
3. Étude de problèmes combinatoires en codes et cryptographie

Outline

☞ Study of combinatorial objects in cryptography and coding theory

1. Background on Boolean functions
   - Some background on Boolean functions
   - Boolean functions for error correcting codes and symmetric cryptography

2. Bent functions over finite fields
   - Presentation of some contributions concerning combinatorial objects in symmetric cryptography
   - Presentation of some contributions concerning combinatorial objects in coding theory

Background on Boolean functions

$f : \mathbb{F}_2^n \to \mathbb{F}_2$ an n-variable Boolean function.

The truth-table :

x_1	x_2	x_3	$f(x)$
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	1

$f : \mathbb{F}_2^n \to \mathbb{F}_2$ an n-variable Boolean function

Definition (Algebraic Normal Form (A.N.F), unique)

Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ a Boolean function. Then f can be expressed as :

$$f(x_1, \ldots, x_n) = \bigoplus_{I \subset \{1,\ldots,n\}} a_I \left(\prod_{i \in I} x_i \right) = \bigoplus_{u \in \mathbb{F}_2^n} a_u x^u, a_I \in \mathbb{F}_2$$

where $I = \mathrm{supp}(u) = \{i = 1, \ldots, n \mid u_i = 1\}$ and $x^u = \prod_{i=1}^{n} x_i^{u_i}$.

The A.N.F exists and is unique.

Definition (The algebraic degree)

The algebraic degree $\deg(f)$ of f is the maximum weight of u such that $a_u \neq 0$.

Affine functions f $(\deg(f) \leq 1)$: $f(x) = a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus \cdots \oplus a_n x_n,\ a_i \in \mathbb{F}_2$

☞ We identify the vectorspace $\mathbb{F}_2^n$ with the Galois field $\mathbb{F}_{2^n}$

Any function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ admits a unique representation :
$f(x) = \sum_{j=0}^{2^n-1} a_j x^j \; ; a_j, x \in \mathbb{F}_{2^n}$

- f is Boolean iff

$a_0, a_{2^n-1} \in \mathbb{F}_2$ and $a_{2j \bmod 2^n-1} = (a_{j \bmod 2^n-1})^2; 0 < j < 2^n - 1$

- $[1, 2^n - 2] = \cup_{r=1}^{c} \Gamma_r$; where

$\Gamma_r = \{j_r \bmod 2^n - 1, 2j_r \bmod 2^n - 1, \cdots, 2^{o(j_r)-1} j_r \bmod 2^n - 1\}$

$$f(x) = a_0 + a_{2^n-1}x^{2^n-1} + \sum_{r=1}^{c} \sum_{s=0}^{o(j_r)-1} a_{2^s j_r \bmod 2^n-1} x^{2^s j_r}$$

$$= a_0 + a_{2^n-1}x^{2^n-1} + \sum_{r=1}^{c} \sum_{s=0}^{o(j_r)-1} (a_{j_r \bmod 2^n-1} x^{j_r})^{2^s}$$

$$= a_0 + a_{2^n-1}x^{2^n-1} + \sum_{r=1}^{c} Tr_1^{o(j_r)}(a_{j_r \bmod 2^n-1} x^{j_r})$$

where $a_0, a_{2^n-1} \in \mathbb{F}_2, a_{j_r \bmod 2^n-1} \in \mathbb{F}_{2^{o(j_r)}}$

Background on Boolean functions : representation

☞ We identify the vectorspace $\mathbb{F}_2^n$ with the Galois field $\mathbb{F}_{2^n}$

Definition (The polynomial form (unique))

Let n be a positive integer. Every Boolean function f defined on $\mathbb{F}_{2^n}$ has a (unique) trace expansion called its **polynomial form :**

$$\forall x \in \mathbb{F}_{2^n}, \quad f(x) = \sum_{j \in \Gamma_n} Tr_1^{o(j)}(a_j x^j) + \epsilon(1 + x^{2^n-1}), \quad a_j \in \mathbb{F}_{2^{o(j)}}$$

- Γ_n is the set of representatives of each cyclotomic class of 2 modulo $2^n - 1$,
- $o(j)$ is the size of the cyclotomic coset containing j,
- $\epsilon = wt(f)$ modulo 2 (recall $wt(f) := \#supp(f) := \#\{x \in \mathbb{F}_{2^n} \mid f(x) = 1\}$).

Recall :

Definition (Absolute trace of $x \in \mathbb{F}_{2^k}$ over $\mathbb{F}_2$)

$Tr_1^k(x) := \sum_{i=0}^{k-1} x^{2^i} = x + x^2 + x^{2^2} + \cdots + x^{2^{k-1}} \in \mathbb{F}_2$

Example : Let $n = 4$. $f : \mathbb{F}_{2^4} \to \mathbb{F}_2$,
$f(x) = \sum_{j \in \Gamma_4} Tr_1^{o(j)}(a_j x^j) + \epsilon(1 + x^{15}), \quad a_j \in \mathbb{F}_{2^{o(j)}}$.
Γ_4 is the set obtained by choosing one element in each cyclotomic class of 2 modulo $2^n - 1 = 2^4 - 1 = 15$. $C(j)$ the cyclotomic coset of 2 modulo 15 containing j.
$C(j) = \{j, j2, j2^2, j2^3, \cdots, j2^{o(j)-1}\}$ where $o(j)$ is the smallest positive integer such that $j2^{o(j)} \equiv j \pmod{2^n - 1}$.
The cyclotomic cosets modulo 15 are :
$C(0) = \{0\}$
$C(1) = \{1, 2, 4, 8\}$
$C(3) = \{3, 6, 12, 9\}$
$C(5) = \{5, 10\}$
$C(7) = \{7, 14, 11, 13\}$
We find $\Gamma_4 = \{0, 1, 3, 5, 7\}$
$f(x) = Tr_1^{o(1)}(a_1 x^1) + Tr_1^{o(3)}(a_3 x^3) + Tr_1^{o(5)}(a_5 x^5) + Tr_1^{o(7)}(a_7 x^7) + a_0 + \epsilon(1 + x^{15})$;
$f(x) = Tr_1^4(a_1 x) + Tr_1^4(a_3 x^3) + Tr_1^2(a_5 x^5) + Tr_1^4(a_7 x^7) + a_0 + \epsilon(1 + x^{15})$
where $a_1, a_3, a_7 \in \mathbb{F}_{2^4}$, $a_5 \in \mathbb{F}_{2^2}$ and $a_0, \epsilon \in \mathbb{F}_2$;
$Tr_1^4 : \mathbb{F}_{2^4} \to \mathbb{F}_2$; $x \mapsto x + x^2 + x^{2^2} + x^{2^3}$;
$Tr_1^2 : \mathbb{F}_{2^2} \to \mathbb{F}_2$; $x \mapsto x + x^2$.

Algebraic degree of the polynomial form

Definition

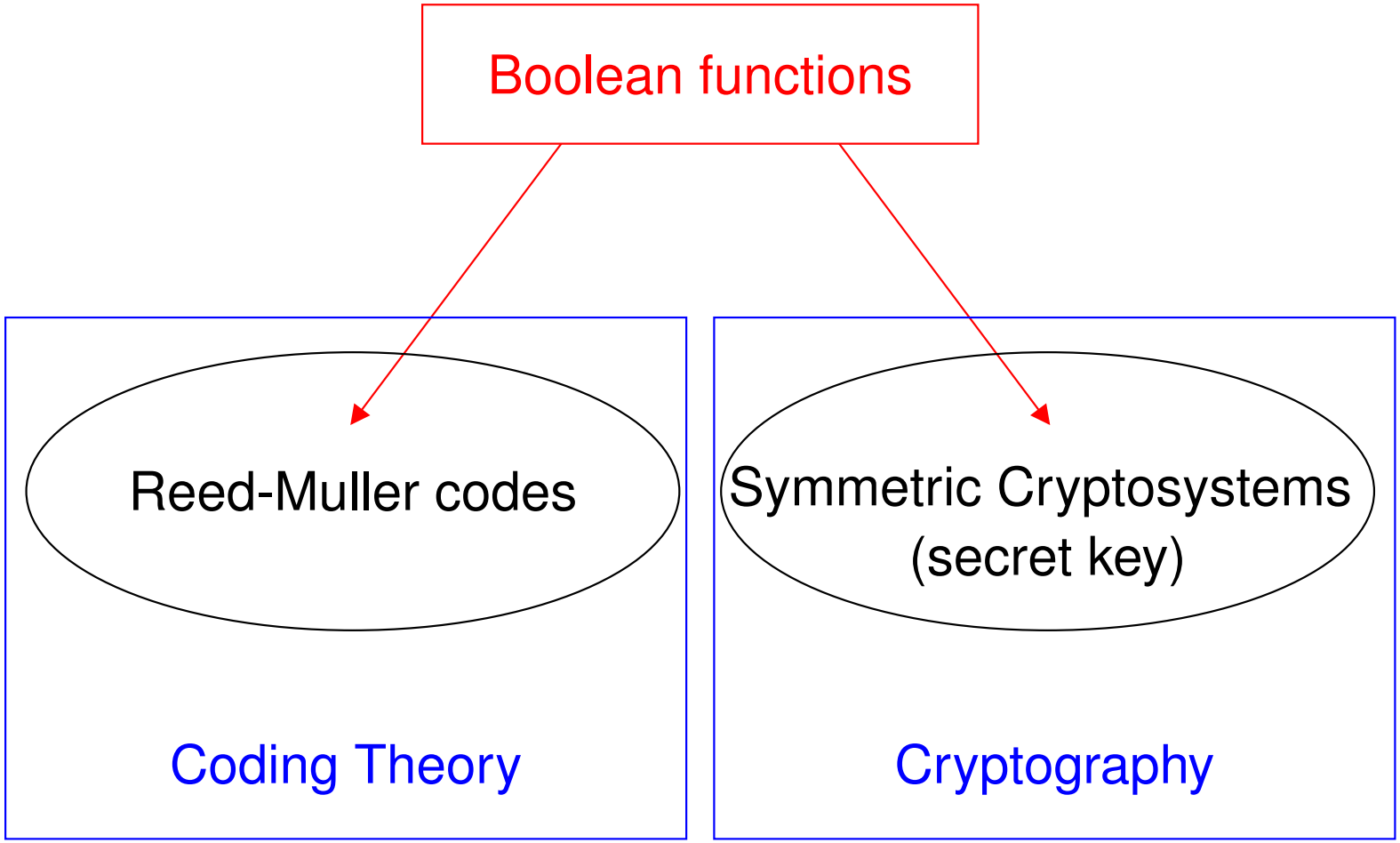
Let n be a positive integer. Every Boolean function f defined on $\mathbb{F}_{2^n}$ has a (unique) trace expansion called its **polynomial form** :

$$\forall x \in \mathbb{F}_{2^n}, \quad f(x) = \sum_{j \in \Gamma_n} Tr_1^{o(j)}(a_j x^j) + \epsilon(1 + x^{2^n-1}), \quad a_j \in \mathbb{F}_{2^{o(j)}}$$

- ☞ **The algebraic degree** of f denoted by $\deg(f)$, is the maximum Hamming weight of the binary expansion of an exponent j for which $a_j \neq 0$ if $\epsilon = 0$ and to n if $\epsilon = 1$.

- Affine functions : $Tr_1^n(ax) + \lambda$, $a \in \mathbb{F}_{2^n}$, $\lambda \in \mathbb{F}_2$.

☞ In both **Error correcting coding** and **Symmetric cryptography**, Boolean functions are important objects !



Error Correcting Coding

$$\texttt{Source} \longrightarrow (u_1, \ldots, u_k) \rightarrow \texttt{Encoding} \rightarrow (x_1, \ldots, x_n)$$

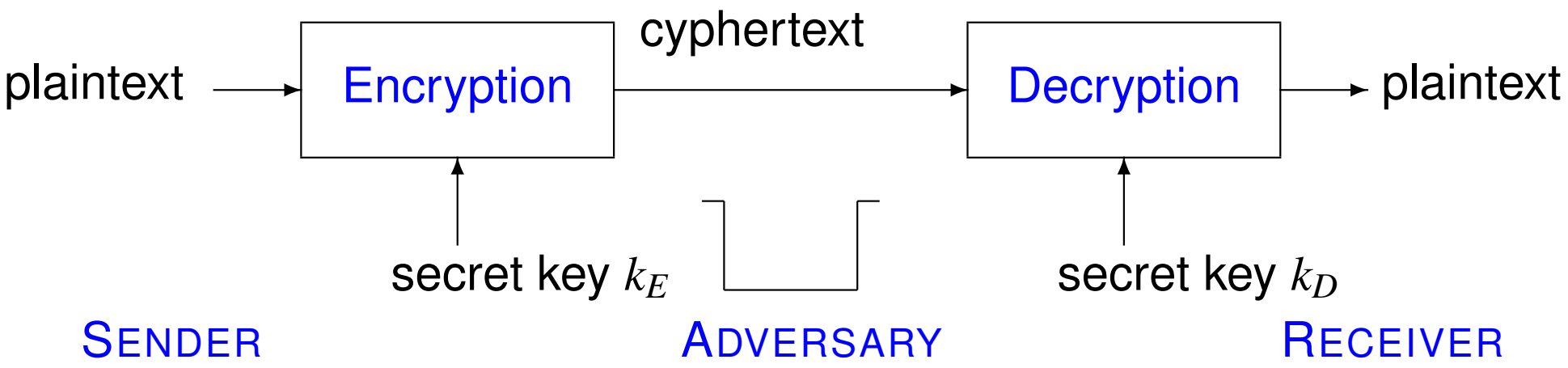
$$\rightarrow \texttt{noisy channel} \rightarrow$$

$$(y_1, \ldots, y_n) \rightarrow \texttt{Decoding} \rightarrow (v_1, \ldots, v_k)$$

$\mathcal{B}_n = \{f : \mathbb{F}_2^n \to \mathbb{F}_2\}$

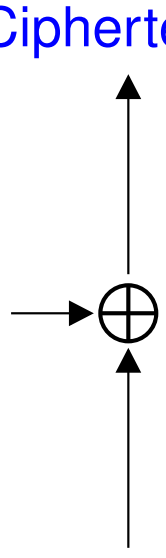
- The Reed-Muller code $\mathcal{RM}(r,n)$ can be defined in terms of **Boolean functions** : $\mathcal{RM}(r,n)$ is the set of all n-variable Boolean functions $\mathcal{B}_n$ of algebraic degrees at most r. More precisely, it is the linear code of all binary words of length 2^n corresponding to the truth-tables of these functions.
- For every $0 \leq r \leq n$, the Reed-Muller code $\mathcal{RM}(r,n)$ of order r, is a linear code :

$$\left[\underbrace{2^n}_{length}, \underbrace{\sum_{i=0}^{r} \binom{n}{i}}_{dimension}, \underbrace{\quad}_{minimum}\ \underbrace{2^{n-r}}_{distance} \right]$$

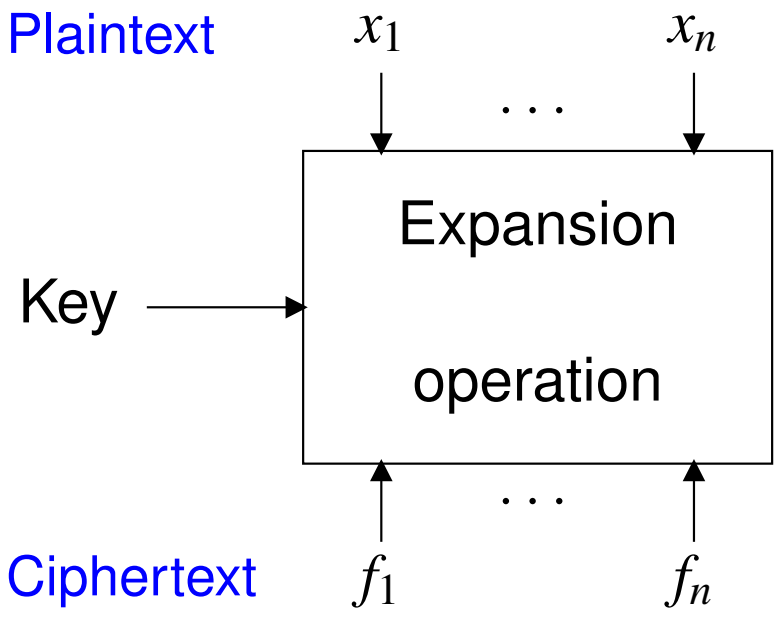

plaintext
Encryption
cyphertext
Decryption
plaintext
secret key k_E
secret key k_D
SENDER
ADVERSARY
RECEIVER

Stream ciphers

Pseudo-random generator with a Boolean function



Bloc ciphers (AES,DES, etc)



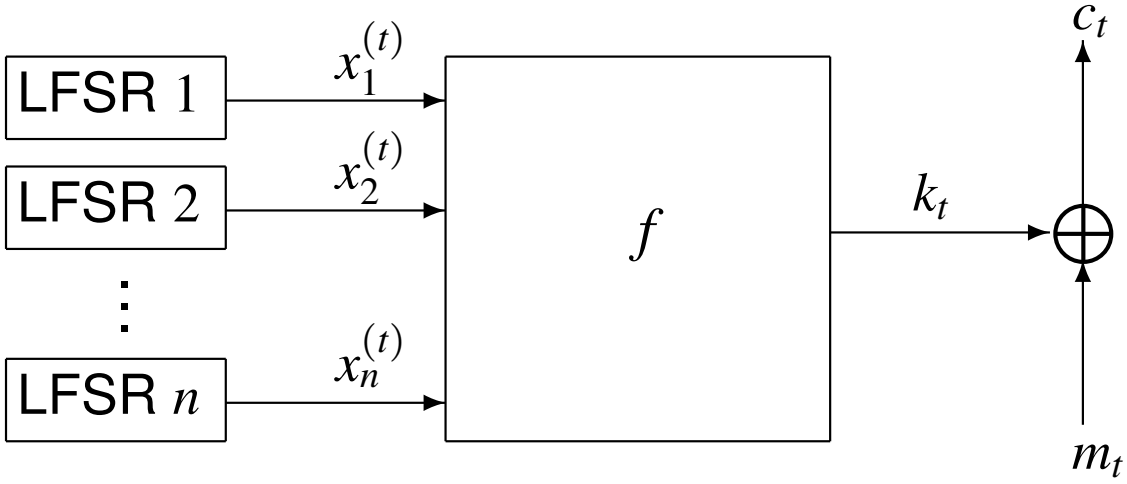
f_i : functions of substitution (S-box)

f_i : Boolean function

The two models of pseudo-random generators with a Boolean function :

COMBINER MODEL :

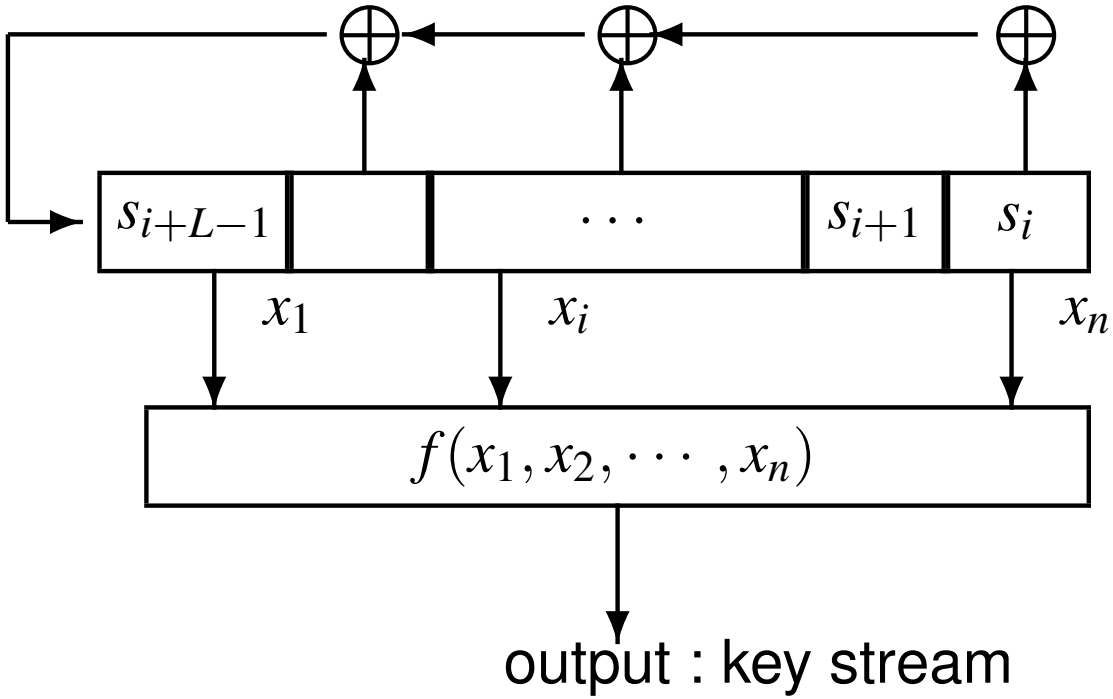
m_t : plain text
c_t : cipher text
k_t : key stream



LFSR : Linear Feedback Shift Register

- A Boolean function combines the outputs of several LFSR to produce the key stream : **a combining (Boolean) function** f.
- The initial state of the LFSR's depends on a secret key.

FILTER MODEL :



- A Boolean function takes as inputs several bits of a single LFSR to produce the key stream : **a filtering (Boolean) function** f

☞ To make the cryptanalysis very difficult to implement, we have to pay attention when choosing the Boolean function, that has to follow several recommendations : **cryptographic criteria** !

Some main cryptographic criteria for Boolean functions

• CRITERION 1 : To protect the system against distinguishing attacks, the cryptographic function must be balanced, that is, its Hamming weight is 2^{n-1}.

• CRITERION 2 : The cryptographic function must have an high algebraic degree to protect against the Berlekamp-Massey attack.

• The Hamming distance $d_H(f,g) := \#\{x \in \mathbb{F}_{2^n} \mid f(x) \neq g(x)\}$.
CRITERION 3 : To protect the system against linear attacks and correlation attacks, the Hamming distance from the cryptographic function to all affine functions must be large.
• CRITERION 4 : To be resistant to correlation attacks on combining registers, a combining function f must be m-resilient where m is as large as possible.
• Algebraic immunity of f : $\mathrm{AI}(f)$ is the lowest degree of any nonzero function g such that $f \cdot g = 0$ or $(1+f) \cdot g = 0$.
CRITERION 5 : To be resistant to algebraic attacks, f must be of high algebraic immunity that is, close to the maximum $\lceil \frac{n}{2} \rceil$. But this condition is not sufficient because of Fast Algebraic Attacks (FFA) : cryptographic functions should be resistant to FFA !
Some of these criteria are antagonistic ! Tradeoffs between all these criteria must be found.

Boolean functions meet the main cryptographic criteria provided that some combinatorial conjectures are correct.

CONJECTURE (TU–DENG CONJECTURE)

For all $k \geq 2$ and all $t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$,
$\#\{(a,b) \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^2 | a+b=t \text{ and } w_2(a)+w_2(b) \leq k-1\} \leq 2^{k-1}$.

where $w_2(a)$ denotes 2-weight of a.

- Many works : [Flori-Randriambololona-Cohen-SM 2010], [Flori-Randriambololona 2011-2012], [Flori-Cohen 2012], ect.
- Serval conjectures have been derived...

Definition (The discrete Fourier (Walsh) Transform)

$$\widehat{\chi_f}(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+a\cdot x}, \quad a \in \mathbb{F}_2^n$$

where "$\cdot$" is the canonical scalar product in $\mathbb{F}_2^n$ defined by $x \cdot y = \sum_{i=1}^{n} x_i y_i, \forall x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n, \quad \forall y = (y_1, \ldots, y_n) \in \mathbb{F}_2^n$.

or

Definition (The discrete Fourier (Walsh) Transform)

$$\widehat{\chi_f}(a) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+Tr_1^n(ax)}, \quad a \in \mathbb{F}_{2^n}$$

where "Tr_1^n" is the absolute trace function on $\mathbb{F}_{2^n}$.

A cryptographic parameter for Boolean functions : nonlinearity

Definition (The Hamming distance between two Boolean functions)

$$d_H(f,g) = wt(f \oplus g) = \#\{x \in \mathbb{F}_2^n \mid f(x) \neq g(x)\}$$

A cryptographic criterion : The distance of a cryptographic function to all affine functions must be high to protect the system against linear attacks and correlation attacks.

- ☞ The nonlinearity of f is the minimum Hamming distance to affine functions :

Definition (Nonlinearity)

$f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ a Boolean function. The nonlinearity denoted by $\mathrm{nl}(f)$ of f is

$$\mathrm{nl}(f) := \min_{l \in A_n} d_H(f,l)$$

where A_n : is the set of affine functions over $\mathbb{F}_{2^n}$.

General upper bound on the nonlinearity of Boolean functions

The Nonlinearity of f is equals :

$$\mathrm{nl}(f) = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n} |\widehat{\chi_f}(a)|$$

➔Thanks to Parseval's relation : $\sum_{a \in \mathbb{F}_2^n} \widehat{\chi_f}^2(a) = 2^{2n}$

we have : $\max_{a \in \mathbb{F}_2^n} \left(\widehat{\chi_f}(a)\right)^2 \geq 2^n$

Hence : for every n-variable Boolean function f, the nonlinearity is always upper bounded by $2^{n-1} - 2^{\frac{n}{2}-1}$

➔It can reach this value if and only if n is even.

➔ The functions used as combining or filtering functions must have nonlinearity close to this maximum.

- **General upper bound on the nonlinearity of any n-variable Boolean function :** $\mathrm{nl}(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$

DEFINITION (BENT FUNCTION [ROTHAUS, 76])

$f : \mathbb{F}_2^n \to \mathbb{F}_2$ (n even) is said to be a bent function if $nl(f) = 2^{n-1} - 2^{\frac{n}{2}-1}$

Bent functions have been studied for 35 years (initiators : Dillon 1974 ; Rothaus 1976).

- **A main characterization of "bentness" :**

$$(f \text{ is bent }) \iff \widehat{\chi_f}(\omega) = \pm 2^{\frac{n}{2}}, \quad \forall \omega \in \mathbb{F}_2^n$$

Bent functions are combinatorial objects :

Definition

- Let G be a finite (abelian) group of order μ. A subset D of G of cardinality k is called (μ, k, λ)-difference set in G if every element $g \in G$, different from the identity, can be written as $d_1 - d_2$, $d_1, d_2 \in D$, in exactly λ different ways.
- Hadamard difference set in elementary abelian 2-group : $(\mu, k, \lambda) = (2^n, 2^{n-1} \pm 2^{\frac{n}{2}-1}, 2^{n-2} \pm 2^{\frac{n}{2}-1})$.

Theorem

A Boolean function f over $\mathbb{F}_2^n$ is bent if and only if $supp(f) := \{x \in \mathbb{F}_2^n \mid f(x) = 1\}$ is a Hadamard difference set in $\mathbb{F}_2^n$.

Example : Let f a Boolean function defined on $\mathbb{F}_2^4$ $(n = 4)$ by $f(x_1, x_2, x_3, x_4) = x_1x_4 + x_2x_3$ The support of f is $Supp(f) = \{(1,0,0,1), (1,0,1,1), (1,1,0,1), (0,1,1,0), (0,1,1,1), (1,1,1,0)\}$ is a Hadamard $(16, 6, 2)$-difference set of $\mathbb{F}_2^4$.

d_1	d_2	$d_1 + d_2$
1001	1011	0010
1001	1101	0100
1001	0110	1111
1001	0111	1110
1001	1110	0111
1011	1101	0110
1011	0110	1101
1011	0111	1100
1011	1110	0101
1101	0110	1011
1101	0111	1010
1101	1110	0011
0110	0111	0001
0110	1110	1000
0111	1110	1001

The covering radius of $\mathcal{RM}(1,n)$ and bent functions

- ☞ The Covering radius $\rho(1,n)$ of the Reed-Muller code $\mathcal{RM}(1,n)$ coincides with the maximum nonlinearity $nl(f)$.
- ☞ General upper bound on the nonlinearity : $\mathrm{nl}(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$

  - When n is odd, $\rho(1,n) < 2^{n-1} - 2^{\frac{n}{2}-1}$
  - When n is even, $\rho(1,n) = 2^{n-1} - 2^{\frac{n}{2}-1}$ and the associated n-variable Boolean functions are the bent functions.

Covering radius of the Reed-Muller code $\mathcal{RM}(r,n)$

- The maximal nonlinearity of order r of n-variable Boolean functions coincides with the covering radius of $\mathcal{RM}(r,n)$.

Definition (Covering radius of the Reed-Muller code $\mathcal{RM}(r,n)$)

Covering radius of the Reed-Muller code $\mathcal{RM}(r,n)$ of order r and length 2^n :

$$\bullet \rho(r,n) := \max_{f \in \mathcal{B}_n} \min_{g \in \mathcal{RM}(r,n)} d_H(f,g) = \max_{f \in \mathcal{B}_n} nl_r(f)$$

where $\mathcal{B}_n := \{f : \mathbb{F}_2^n \to \mathbb{F}_2\}$. Or :

$$\bullet \rho(r,n) := \min\{d \in \mathbb{N} \mid \cup_{x \in \mathcal{RM}(r,n)} B(x,d) = \mathbb{F}_2^n\}$$

where $B(x,d) := \{y \in \mathbb{F}_2^n \mid d_H(x,y) \leq d\}$(Hamming ball)

- The covering radius plays an important role in error correcting codes : measures the maximum errors to be corrected in the context of maximum-likelihood decoding.

THEOREM ([CARLET-SM 2007])

Let $r > 1$. The covering radius of the Reed-Muller code of order r satisfies asymptotically :$\rho(r,n) \leq 2^{n-1} - \frac{\sqrt{15}}{2} \cdot (1+\sqrt{2})^{r-2} \cdot 2^{n/2} + O(n^{r-2})$

Our results have improved the best known upper bounds dating from 15 years ago. Up to now, our bounds are the best bounds known in the literature.

Our results are obtained by induction on r thanks to improved upper bounds on the covering radius $\rho(2,n)$:

THEOREM ([CARLET-SM 2007])

For every positive integer $n \geq 17$, the covering radius $\rho(2,n)$ of the second-order Reed-Muller code $\mathcal{RM}(2,n)$ is upper bounded by

$$\left\lfloor 2^{n-1} - \frac{\sqrt{15}}{2} \cdot 2^{\frac{n}{2}} \cdot \left(1 - \frac{122929}{21 \cdot 2^n} - \frac{155582504573}{4410 \cdot 2^{2n}}\right) \right\rfloor \quad (1)$$

Brief outline of the proof

$B_n := \{f : \mathbb{F}_2^n \to \mathbb{F}_2\}$.
We prove an asymptotic upper bound on the covering radius $\rho(2,n)$ of the Reed-Muller code of order 2 :

$$\rho(2,n) \leq 2^{n-1} - \sqrt{15}\, 2^{\frac{n}{2}-1} + O(1).$$

Indeed, we have :

$$\boxed{\forall k \in \mathbb{N}, \quad \rho(2,n) \leq 2^{n-1} - \frac{1}{2} \min_{f \in \mathcal{B}_n} \sqrt{\frac{\mathcal{S}_{k+1}(f)}{\mathcal{S}_k(f)}}}$$

where

$$\mathcal{S}_k(f) = \sum_{g \in \mathcal{RM}(2,n)} \left(\sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+g(x)} \right)^{2k}, f \in \mathcal{B}_n,\ k \in \mathbb{N}$$

Brief outline of the proof

$$\forall k \in \mathbb{N}, \quad \rho(2,n) \leq 2^{n-1} - \frac{1}{2} \min_{f \in \mathcal{B}_n} \sqrt{\frac{\mathcal{S}_{k+1}(f)}{\mathcal{S}_k(f)}}$$

1. Decomposition of $\mathcal{S}_k(f)$ into sums of characters : $S_k(f) = \sum_{w=0}^{k} N_k^{(2w)} M_f^{(2w)}$ where $M_f^{(2w)} = \sum_{\substack{g \in \mathcal{RM}(n-3,n) \\ wt(g)=2w}} (-1)^{\langle f,g \rangle}$ and $N_k^{(2w)}$ is an integer independent of f
2. Lower bound of the sums of characters $M_f^{(2w)}$ thanks to the characterization of the words of Reed-Muller codes given by Kasami, Tokura and Azumi : $\forall f \in \mathcal{B}_n$, $M_f^{(2w)} \geq M_{min}^{(2w)}$.
3. Lower bound of $\frac{\mathcal{S}_{k+1}(f)}{\mathcal{S}_k(f)}$, $\forall f$, leading to an upper bound $\rho(2,n) \leq 2^{n-1} - \frac{1}{2}\sqrt{\frac{\mathcal{S}_{k+1}^{min}}{\mathcal{S}_k^{min}}}$ for $k \leq \mathrm{k}_n$ where k_n varies according to the value of n and $\mathcal{S}_k^{min} = \sum_{w=0}^{k} N_k^{(2w)} M_{min}^{(2w)}$.

Brief outline of the proof

$$\forall k \in \mathbb{N}, \quad \rho(2,n) \leq 2^{n-1} - \frac{1}{2} \min_{f \in \mathcal{B}_n} \sqrt{\frac{\mathcal{S}_{k+1}(f)}{\mathcal{S}_k(f)}}$$

1. Decomposition of $\mathcal{S}_k(f)$ into sums of characters : $S_k(f) = \sum_{w=0}^{k} N_k^{(2w)} M_f^{(2w)}$ where $M_f^{(2w)} = \sum_{\substack{g \in \mathcal{RM}(n-3,n) \\ wt(g)=2w}} (-1)^{\langle f,g \rangle}$ and $N_k^{(2w)}$ is an integer independent of f
2. Lower bound of the sums of characters $M_f^{(2w)}$ thanks to the characterization of the words of Reed-Muller codes given by Kasami, Tokura and Azumi : $\forall f \in \mathcal{B}_n$, $M_f^{(2w)} \geq M_{min}^{(2w)}$.
3. Lower bound of $\frac{\mathcal{S}_{k+1}(f)}{\mathcal{S}_k(f)}$, $\forall f$, leading to an upper bound $\rho(2,n) \leq 2^{n-1} - \frac{1}{2}\sqrt{\frac{\mathcal{S}_{k+1}^{min}}{\mathcal{S}_k^{min}}}$ for $k \leq \mathrm{k}_n$ where k_n varies according to the value of n and $\mathcal{S}_k^{min} = \sum_{w=0}^{k} N_k^{(2w)} M_{min}^{(2w)}$.

Brief outline of the proof

$$\forall k \in \mathbb{N}, \quad \rho(2,n) \leq 2^{n-1} - \frac{1}{2} \min_{f \in \mathcal{B}_n} \sqrt{\frac{\mathcal{S}_{k+1}(f)}{\mathcal{S}_k(f)}}$$

1. Decomposition of $\mathcal{S}_k(f)$ into sums of characters : $S_k(f) = \sum_{w=0}^{k} N_k^{(2w)} M_f^{(2w)}$ where $M_f^{(2w)} = \sum_{\substack{g \in \mathcal{RM}(n-3,n) \\ wt(g)=2w}} (-1)^{\langle f,g \rangle}$ and $N_k^{(2w)}$ is an integer independent of f
2. Lower bound of the sums of characters $M_f^{(2w)}$ thanks to the characterization of the words of Reed-Muller codes given by Kasami, Tokura and Azumi : $\forall f \in \mathcal{B}_n$, $M_f^{(2w)} \geq M_{min}^{(2w)}$.
3. Lower bound of $\frac{\mathcal{S}_{k+1}(f)}{\mathcal{S}_k(f)}$, $\forall f$, leading to an upper bound $\rho(2,n) \leq 2^{n-1} - \frac{1}{2}\sqrt{\frac{\mathcal{S}_{k+1}^{min}}{\mathcal{S}_k^{min}}}$ for $k \leq \mathrm{k}_n$ where k_n varies according to the value of n and $\mathcal{S}_k^{min} = \sum_{w=0}^{k} N_k^{(2w)} M_{min}^{(2w)}$.

Final remarks :

- $\rho(2,n) \leq 2^{n-1} - \frac{1}{2}\sqrt{\frac{\mathcal{S}_{k+1}^{min}}{\mathcal{S}_{k}^{min}}}$ for $k \leq \mathrm{k}_n$ where k_n varies according to the value of n :

n	$3-8$	$9-11$	$12-13$	≥ 14
k_n	4	5	6	7

- The greater we take the value of k, the better the upper bound obtained. Moreover, using Cauchy-Schwartz's inequality in the Euclidean space $\mathbb{R}^{\mathcal{RM}(r,n)}$ and tends k to infinity show that the exact value of $\rho(2,n)$ is reached. Unfortunately, we are brought to restrict the choice of k and we get only a bound.
- Our method could be applied directly to $\rho(r,n)$ but the best result is obtained with our method to $\rho(2,n)$. Indeed, we are able to improve the upper bound thanks the knowledge of the codewords in the dual code $\mathcal{RM}(n-3,n)$. For $r > 2$ the knowledge of the codewords of $\mathcal{RM}(n-r-1,n)$ is not enough to improve the upper bounds.
- We can further improve $\rho(2,n)$ thanks to a good estimation of $M_f^{(2w)}$: combinatorial idea are needed !

Some properties are known.

Properties of bent functions :

- The bentness is an affine invariant.
  If f is bent and ℓ is affine, then $f+\ell$ is bent.
  The *automorphism group* of the set of bent functions

  $$\{\sigma \text{ permutation s.t.} f\circ\sigma \text{ bent}, \forall f \text{ bent } \}$$

  is the general affine group.
  A class of bent functions is called *complete* if it is globally invariant under the action of the general affine group and under the addition of affine functions.
  Two functions f and $f\circ\sigma+$ affine are called EA-equivalent.
- If f is bent then $\deg f \leq \frac{n}{2}$.
- if f is bent then $wt(f) = 2^{n-1} \pm 2^{\frac{n}{2}-1}$.
- If f is bent then $\widehat{\chi_f}(\omega) = 2^{\frac{n}{2}}(-1)^{\tilde{f}(\omega)}$, for all $\omega \in \mathbb{F}_2^n$, defines the dual function $\tilde{f}$ of f. The dual is bent too.

Classification and enumeration :

☞ The classification of bent functions for $n \geq 10$ and even counting them are still wide open problems.

- The number of bent functions is known for $n \leq 8$. For n = 8, it equals approximately $2^{106.3}$ [Langevin-Leander-Rabizzoni-Veron-Zanotti 08].
- Only bounds on their number are known (cf. [Carlet-Klapper 02]).
- The problem of determining an efficient lower bound on the number of n-variable bent functions is open.
- Few constructions are known.

☞ From now, $n = 2m$ be an (even) integer.

The bivariate representation (unique) : $n = 2m$

$$\mathbb{F}_{2^n} \approx \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$$

$$f(x,y) = \sum_{0 \le i,j \le 2^m - 1} a_{i,j} x^i y^j;\ a_{i,j} \in \mathbb{F}_{2^m}$$

.

- Then the algebraic degree of f equals $\max_{(i,j)\,|\,a_{i,j} \neq 0}(w_2(i) + w_2(j))$.
- And f being Boolean, its bivariate representation can be written in the form $f(x,y) = Tr_1^m(P(x,y))$ where $P(x,y)$ is some polynomial over $\mathbb{F}_{2^m}$.

General Primary constructions of bent functions

- **Maiorana-Mc Farland's class $\mathcal{M}$** : the best known construction of bent functions defined in bivariate form (explicit construction). $f_{\pi,g}(x,y) = x \cdot \pi(y) + g(y)$, with $\pi : \mathbb{F}_2^m \to \mathbb{F}_2^m$ be a permutation and $g : \mathbb{F}_2^m \to \mathbb{F}_2$ any mapping.
- **Dillon's Partial Spreads class $\mathcal{PS}^-$** : well known construction of bent functions functions whose bentness is achieved under a condition based on a decomposition of its supports (not explicit construction) : $supp(f) = \bigcup_{i=1}^{2^{m-1}} E_i^\star$ where $\{E_i, 1 \leq i \leq 2^{m-1}\}$ are m-dimensional subspaces with $E_i \cap E_j = \{0\}$.
- **Dillon's Partial Spreads class $\mathcal{PS}_{ap}$** : a subclass of $\mathcal{PS}^-$'s class. Functions in $\mathcal{PS}_{ap}$ are defined explicitly in bivariate form : $f(x,y) = g(xy^{2^m-2})$ with g is a balanced Boolean function on $\mathbb{F}_{2^m}$ which vanishes at 0.
- **Dillon's class H** : a nice original construction of bent functions in bivariate representation but less known because Dillon could only exhibit functions which already belonged to the well known Maiorana-Mc Farland class. The bentness is achieved under some non-obvious conditions.

Spread

Definition (Spread)

A m-spread of $\mathbb{F}_{2^n}$ is a set of pairwise supplementary m-dimensional subspaces of $\mathbb{F}_{2^n}$ whose union equals $\mathbb{F}_{2^n}$

Example (A classical example of m-Spread)

- in $\mathbb{F}_{2^n}$: $\{u\mathbb{F}_{2^m}, u \in U\}$ where $U := \{u \in \mathbb{F}_{2^n} \mid u^{2^m+1} = 1\}$
- in $\mathbb{F}_{2^n} \approx \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$: $\{E_a, a \in \mathbb{F}_{2^m}\} \cup \{E_\infty\}$ where $E_a := \{(x, ax)\,;\, x \in \mathbb{F}_{2^m}\}$ and $E_\infty := \{(0, y)\,;\, y \in \mathbb{F}_{2^m}\} = \{0\} \times \mathbb{F}_{2^m}$.

☞ We were interested in bent functions g defined on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$, whose restrictions to elements of the m-spread $\{E_a, E_\infty\}$ are linear.

Class $\mathcal{H}$

Functions g defined on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ whose restrictions to elements of the m-spread $\{E_a, E_\infty\}$ are linear, are of the form (2)

$$g(x,y) = \begin{cases} Tr_1^m\left(x\psi\left(\frac{y}{x}\right)\right) \text{ if } x \neq 0 \\ Tr_1^m(\mu y) \text{ if } x = 0 \end{cases} \tag{2}$$

where $\psi : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ and $\mu \in \mathbb{F}_{2^m}$.

Proposition ([Carlet-SM 2012])

Let g be a function defined on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ by (2) : Then g is bent iff

$$G(z) := \psi(z) + \mu z \text{ is a permutation on } \mathbb{F}_{2^m} \tag{3}$$

$$\forall \beta \in \mathbb{F}_{2^m}^\star, \text{the function } z \mapsto G(z) + \beta z \text{ is 2-to-1 on } \mathbb{F}_{2^m}. \tag{4}$$

Definition (Class $\mathcal{H}$ [Carlet-SM 2012])

We call $\mathcal{H}$ the class of functions of the form (2) satisfying (3) and (4).

- The class H of Dillon is a subclass of $\mathcal{H}$.

A first contribution thanks to the introduction of the class $\mathcal{H}$:

If we identify $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ with $\mathbb{F}_{2^n}$, then the vector spaces $\{(x, ax)\,;\, x \in \mathbb{F}_{2^m}\}$ and $\{(0, y)\,;\, y \in \mathbb{F}_{2^m}\}$ become the $2^m + 1$ vector spaces $u\mathbb{F}_{2^m}$.

Nonlinear Boolean functions whose restrictions to any vector space $u\mathbb{F}_{2^m}$ (where $u \in U$) are linear are sums of Niho power functions, that is of functions of the form :

$$Tr_1^{o((2^m-1)s+1)}\left(a_s x^{(2^m-1)s+1}\right) \text{ with } 2 \leq s \leq 2^m$$

d is said to be an exponent of type Niho if $d \equiv 2^i \pmod{2^m - 1}$

☞ Functions of class $\mathcal{H}$ in univariate form are the known Niho bent functions $\rightarrow$ new framework to study the Niho bent functions.

Known Niho bent functions :

- $f(x) = Tr_1^m\left(ax^{2^m+1}\right)$, $a \in \mathbb{F}_{2^m}^\star$ [Kasami]
- Three families of binomial functions [Dobbertin-Leander-Canteaut-Carlet-Felke-Gaborit 2006] : $f(x) = Tr_1^m(at^{2^m+1}) + Tr_1^n(bx^{d_2})$ where $a = b^{2^m+1} \in \mathbb{F}_{2^m}^\star$
  1. $d_2 = (2^m-1)\,3\, + 1$ (if $m \equiv 2$ [mod 4], then b must be the fifth power of an element in $\mathbb{F}_{2^n}$; otherwise, b can be any nonzero element), (degree m) ;
  2. $d_2 = (2^m-1)\frac{1}{4} + 1$ (m odd), (degree 3) ;
  3. $d_2 = (2^m-1)\frac{1}{6} + 1$ (m even), (degree m).
- The second Dobbertin et al.'s class has been extended [Leander-Kholosha 2006] into the functions : $Tr_1^n\left(\alpha x^{2^m+1} + \sum_{i=1}^{2^{r-1}-1} x^{s_i}\right)$, $r > 1$ such that
  - $gcd(r,m) = 1$,
  - $\alpha \in \mathbb{F}_{2^n}$ such that $\alpha + \alpha^{2^m} = 1$,
  - $s_i = (2^m-1)\frac{i}{2^r} \mod (2^m+1) + 1$, $i \in \{1, \cdots, 2^{r-1}-1\}$.

Class $\mathcal{H}$ and *Niho* bent functions

Thanks to the correspondence between the bent functions (bivariate forms) of class $\mathcal{H}$ and the Niho bent functions (univariate forms) we give answers to many questions left open in the literature :

1. The duals of the known cubic binomial Niho functions are calculated. Moreover, they are not of Niho type. [Carlet-SM 2012].
2. The duals of the multi-monomial Niho bent functions are calculated. Moreover, they are not of Niho type [Carlet-Helleseth-Kholosha-SM 2011], [Budaghyan-Carlet-Helleseth-Kholosha-SM 2012].
3. The family of the cubic binomial Niho functions is in the completed $\mathcal{M}$ class [Carlet-SM 2012].
4. The multi-monomial Niho bent functions is in the completed $\mathcal{M}$ class [Carlet-Helleseth-Kholosha-SM 2011], [Budaghyan-Carlet-Helleseth-Kholosha-SM 2012].
5. The class H of Dillon is not contained in the completed $\mathcal{M}$ class [Budaghyan-Carlet-Helleseth-Kholosha-SM 2012].

A second contribution thanks to the introduction of the class $\mathcal{H}$:

Recall : A function g in the class $\mathcal{H}$ is bent if and only if

$$G(z) := \psi(z) + \mu z \text{ is a permutation on } \mathbb{F}_{2^m} \tag{5}$$

$$\forall \beta \in \mathbb{F}_{2^m}^{\star}, \text{ function } z \mapsto G(z) + \beta z \text{ is 2-to-1 on } \mathbb{F}_{2^m}. \tag{6}$$

We have :

PROPOSITION ([CARLET-SM 2012])

- The condition (6) implies the condition (5).
- Any function G from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^m}$ satisfies (6) if and only if,for every $\gamma \in \mathbb{F}_{2^m}$, the function $H_\gamma : z \in \mathbb{F}_{2^m} \mapsto \begin{cases} \frac{G(z+\gamma)+G(\gamma)}{z} \text{ if } z \neq 0 \\ 0 \text{ if } z = 0 \end{cases}$ is a permutation on $\mathbb{F}_{2^m}$.

Definition

Let m be any positive integer. A permutation polynomial G over $\mathbb{F}_{2^m}$ is called an o-polynomial if, for every $\gamma \in \mathbb{F}_{2^m}$, the function H_γ :

$z \in \mathbb{F}_{2^m} \mapsto \begin{cases} \frac{G(z+\gamma)+G(\gamma)}{z} \text{ if } z \neq 0 \\ 0 \text{ if } z = 0 \end{cases}$ is a permutation on $\mathbb{F}_{2^m}$.

The notion of o-polynomial comes from Finite Projective Geometry :

- ☞ There is a close connection between "o-polynomials" and "hyperovals" from Finite Projective Geometry !

Definition (A hyperoval of $PG_2(2^n)$)

Denote by $PG_2(2^n)$ the projective plane over $\mathbb{F}_{2^n}$.
A hyperoval of $PG_2(2^n)$ is a set of $2^n + 2$ points no three collinear.

A hyperoval of $PG_2(2^n)$ can then be represented by
$D(f) = \{(1, t, f(t)), t \in \mathbb{F}_{2^n}\} \cup \{(0,1,0), (0,0,1)\}$ or
$D(f) = \{(f(t), t, 1), t \in \mathbb{F}_{2^n}\} \cup \{(0,1,0), (1,0,0)\}$ where f is an o-polynomial.

The list, up to equivalence, of the known o-polynomials on $\mathbb{F}_{2^m}$

1. $G(z) = z^6$ where m is odd ;
2. $G(z) = z^{3\cdot 2^k+4}$, where $m = 2k-1$;
3. $G(z) = z^{2^k+2^{2k}}$, where $m = 4k-1$;
4. $G(z) = z^{2^{2k+1}+2^{3k+1}}$, where $m = 4k+1$;
5. $G(z) = z^{2^k} + z^{2^k+2} + z^{3\cdot 2^k+4}$, where $m = 2k-1$;
6. $G(z) = z^{\frac{1}{6}} + z^{\frac{3}{6}} + z^{\frac{5}{6}}$ where m is odd ;
7. $G(z) = \frac{\delta^2(z^4+z)+\delta^2(1+\delta+\delta^2)(z^3+z^2)}{z^4+\delta^2z^2+1} + z^{1/2}$, where $Tr_1^m(1/\delta) = 1$ and, if $m \equiv 2$ [mod 4], then $\delta \notin \mathbb{F}_4$;
8. $G(z) = z^{1/2} + \frac{1}{Tr_m^n(b)}\left(Tr_m^n(b^r)(z+1)+ Tr_m^n((bz+b^{2^m})^r)(z+Tr_m^n(b)z^{1/2}+1)^{1-r}\right)$,

where m is even, $r = \pm\frac{2^m-1}{3}$, $b \in \mathbb{F}_{2^{2m}}$, $b^{2^m+1} = 1$ and $b \neq 1$, where $Tr_m^n(x) = x + x^{2^m}$ is the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$.

Class $\mathcal{H}$ and o-polynomes

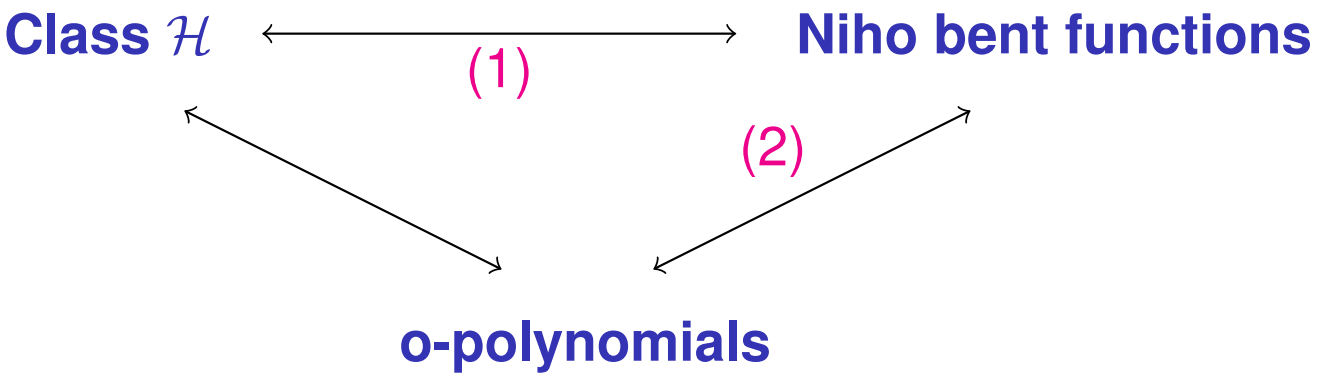
Thanks to the connection between bent functions in the class $\mathcal{H}$ with the o-polynomes we construct 16 potentially new families of bent functions in $\mathcal{H}$ and thus new bent functions of type Niho :

- In the literature, 8 classes of o-polynomials discovered by the geometers in 40 years.
- Each o-polynomial G leads to two potentially new families of bent functions in $\mathcal{H}$ (G^{-1} is an o-polynomial too) and thus in the set of Niho bent functions [Carlet-SM 2012].
- We have proved that some of those families of bent functions are affinely inequivalent [Carlet-SM 2012]

Moreover,
• We have identified the associate o-polynomials of all the known Niho bent functions [Carlet-SM 2012], [Helleseth-Kholosha-SM 2011], [Helleseth-Kholosha 2012].
• We have found new bent functions in a known class of binomial Niho bent. Moreover, relations between a known class of binomial Niho bent and o-polynomials give rise to the Subiaco and Adelaide classes of hyperovals [Helleseth-Kholosha-SM 2011].

Class $\mathcal{H}$, Niho bent functions and o-polynomial

Class $\mathcal{H}$ (bent functions in bivariate forms ; contains a class H introduced by Dillon in 1974).



1. The correspondence (1), offers a new framework to study Niho bent functions. We have used a such framework to answer many questions left open in the literature.
2. Thanks to the connection (2) and thanks to the results of the geometers (obtained in 40 years), we construct several potentially new families of bent functions in $\mathcal{H}$ and thus new bent functions of type Niho.

Bent functions with Dillon-like exponents

Bent functions whose restrictions to the multiplicative cosets $u\mathbb{F}_{2^m}^\star$ $(u \in U)$ are constant :

PROPOSITION (SM 2014)

Let $n = 2m$. Let f a Boolean function defined on $\mathbb{F}_{2^n}$ such that $f(0) = 0$. The two assertions are equivalent :

1. $f(x) = \sum_i Tr_1^{o(d_i)}(a_i x^{d_i})$ with $\forall i, d_i \equiv 0 \pmod{2^m - 1}$;
2. $\forall u \in U$, the restriction of f to $u\mathbb{F}_{2^m}^\star$ is constant (that is, $f(uy) = f(u), \forall y \in \mathbb{F}_{2^m}^\star$) ;

NOTATION

We denote by $\mathcal{D}_n$ the set of bent functions f defined on $\mathbb{F}_{2^n}$ by $f(0) = 0$ and $f(x) = \sum_i Tr_1^{o(d_i)}(a_i x^{d_i})$ with $\forall i, d_i \equiv 0 \pmod{2^m - 1}$.

Note that $\mathcal{D}_n$ is the set of bent functions whose polynomial form is the sum of multiple trace terms via Dillon-like exponents.

☞ We have proved that the elements of $\mathcal{D}_n$ are in a known subclass of bent functions : the so-called hyper-bent functions !

Hyper-bent Boolean functions

DEFINITION (HYPER-BENT BOOLEAN FUNCTION [YOUSSEF-GONG 01])

$f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ (n even) is said to be a hyper-bent if the function $x \mapsto f(x^i)$ is bent, for every integer i co-prime to $2^n - 1$.

Characterization : f is hyper-bent on $\mathbb{F}_{2^n}$ if and only if its extended Hadamard transform takes only the values $\pm 2^{\frac{n}{2}}$.

DEFINITION (THE EXTENDED DISCRETE FOURIER (WALSH) TRANSFORM)

$$\forall \omega \in \mathbb{F}_{2^n}, \quad \widehat{\chi_f}(\omega, k) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+Tr_1^n(\omega x^k)}, \text{ with } \gcd(k, 2^n - 1) = 1.$$

- Hyper-bent functions have properties stronger than bent functions ; they are rarer than bent functions.

☞ Hyper-bent functions are used in S-boxes (DES).

Notation

We denote by $\mathcal{H}_n$ the set of hyper-bent functions f defined on $\mathbb{F}_{2^n}$

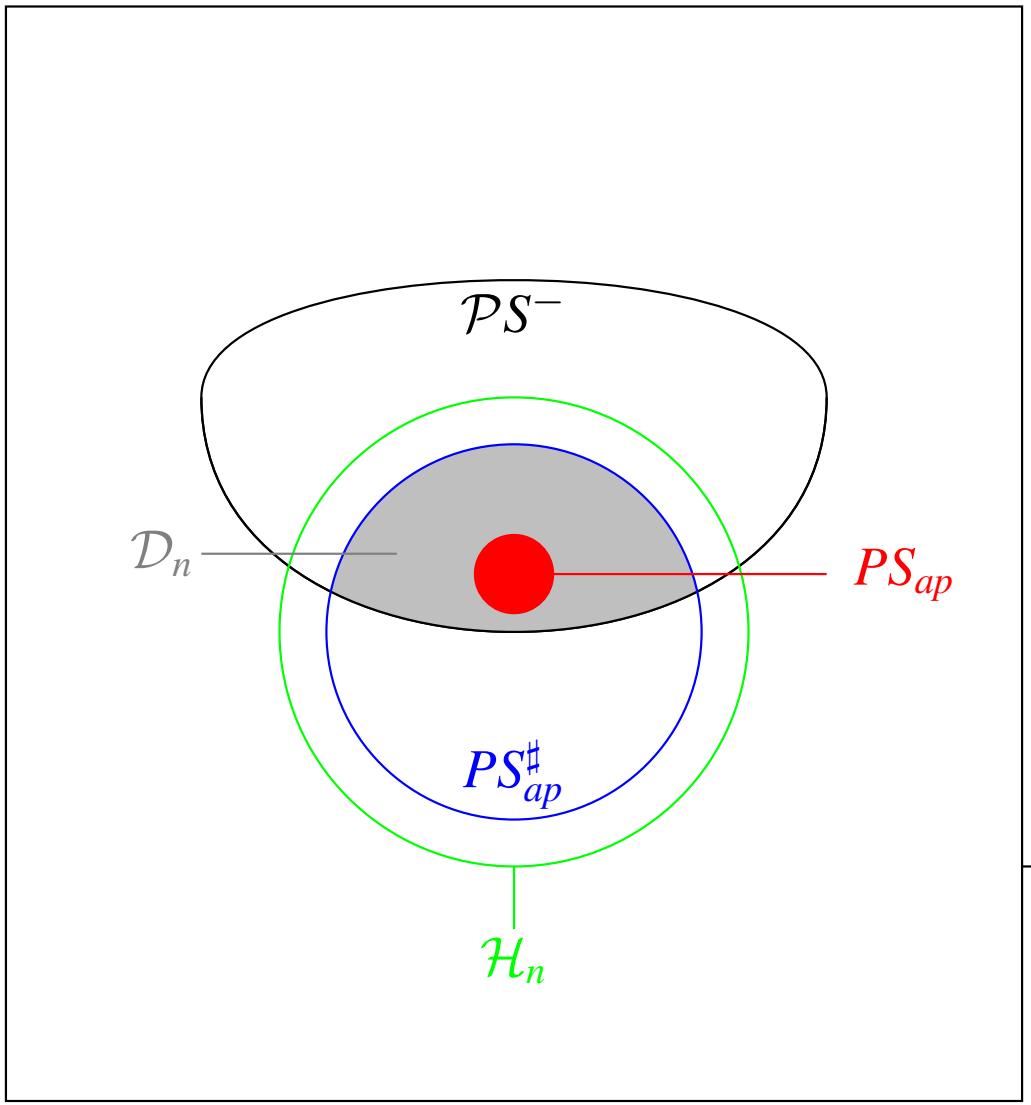
We have the following result : (alternative proof of : $\mathcal{PS}_{ap} \subset \mathcal{H}_n$ ([Carlet-Gaborit 2006])

Theorem (SM 2014)

1. Functions in $\mathcal{D}_n$ are the functions of the form $g(x) = f(\delta x)$ with $f \in \mathcal{PS}_{ap}$ and $\delta \in \mathbb{F}_{2^n}^{\star}$
2. $\mathcal{PS}_{ap}^{\#} = \mathcal{D}_n \cup (1 + \mathcal{D}_n)$
3. $\mathcal{PS}_{ap} \subset \mathcal{D}_n \subset \mathcal{PS}_{ap}^{\#} \subset \mathcal{H}_n$
4. $\mathcal{PS}_{ap}^{\#} \cap \mathcal{PS}^{-} = \mathcal{D}_n$
5. $\mathcal{D}_n \subset \mathcal{H}_n \cap \mathcal{PS}^{-}$

Note that there exists $f \in \mathcal{H}_n$ such that $f \notin \mathcal{PS}_{ap}^{\#}$ (for $n = 4$ obtained by computer [Carlet-Gaborit 2006]).

Bent functions form partial spreads and hyperbent functions



For any bent/ hyper-bent Boolean function f defined over $\mathbb{F}_{2^n}$:

- Polynomial form :

$$\forall x \in \mathbb{F}_{2^n}, \quad f(x) = \sum_{j \in \Gamma_n} Tr_1^{o(j)}(a_j x^j) \quad , a_j \in \mathbb{F}_{2^{o(j)}}$$

PROBLEM (HARD)

Characterize classes of bent / hyper-bent functions in polynomial form, by giving explicitly the coefficients a_j.

All the known characterizations of hyper-bentness are obtained for functions in $\mathcal{D}_n$ (and $1+f \in \mathcal{PS}^{\#}_{ap}$) :

- Until 2009, the only know construction of hyper-bent function is the monomial bent function ($x \mapsto Tr_1^n(ax^{2^m-1})$) of [Dillon 1974] extended by [Charpin-Gong 2008]. The (hyper-)bentness has been characterized by means of Kloosterman sums !
- In 2009 : we have constructed **the first (two) classes of binomial hyper-bent functions** [SM 2009].
  - in the first class : we have characterized the hyper-bentess by means of Kloosterman sums ;
  - in the second class : we have characterized the hyper-bentess by means of Kloosterman sums and cubic sums.

Kloosterman sums with the value 0 and 4

Hyper-bentness can be characterized by means of Kloosterman sums :

- **It is known since 1974 that the zeros of Kloosterman sums give rise to (hyper)-bent functions** :
  [Dillon 1974] ($r = 1$)[Charpin-Gong 2008] (r such that $gcd(r, 2^m + 1) = 1$) :
  Let $n = 2m$. Let $a \in \mathbb{F}_{2^m}^\star$

$$\begin{array}{rccc} f_a^{(r)} & : & \mathbb{F}_{2^n} & \longrightarrow & \mathbb{F}_2 \\ & & x & \longmapsto & Tr_1^n(ax^{r(2^m-1)}) \end{array}$$

  then : $f_{a,b}^{(r)}$ is (hyper)-bent if and only if $K_m(a) = 0$.

- In 2009 **we have shown that the value 4 of Kloosterman sums leads to constructions of hyper-bent functions** :
  [SM 2009] : Let $n = 2m$ (m odd). Let $a \in \mathbb{F}_{2^m}^\star$ and $b \in \mathbb{F}_4^\star$.

$$\begin{array}{rccc} f_{a,b}^{(r)} & : & \mathbb{F}_{2^n} & \longrightarrow & \mathbb{F}_2 \\ & & x & \longmapsto & Tr_1^n\left(ax^{r(2^m-1)}\right) + Tr_1^2\left(bx^{\frac{2^n-1}{3}}\right); gcd(r, 2^m + 1) = 1 \end{array}$$

  then : $f_{a,b}^{(r)}$ is (hyper)-bent if and only if $K_m(a) = 4$.

- We have computed a such that $K_m(a) = 4$ [Flori-SM-Cohen]

Hyper-bent functions which are sum of multiple trace terms

When all the coefficients in the polynomial forms belong to $\mathbb{F}_{2^m}$, Charpin and Gong have provided a nice characterization of hyper-bentness of functions which are sum of several Dillon-like monomial functions in terms of Dickson polynomials.

- ☞ [Charpin-Gong 2008] : the link between the zero of Kloosterman sums and Dillon monomial hyper-bent functions ([Dillon 1974]) has been generalized into a link between hyper-bent functions of a sub-class of $\mathcal{D}_n$ and some exponential sums involving Dickson polynomials of degree r.
- ☞ [SM 2010] : the link between the value 4 of Kloosterman sums and binomial hyper-bent functions ([SM 2009]) has been generalized into a link between hyper-bent functions of another sub-class of $\mathcal{D}_n$ and exponential sums involving Dickson polynomials of degree r and 3.

Hyper-bent functions with multiple trace terms via Dillon-like exponents

Next, we have studied the hyper-bentness of functions of the general form in $\mathcal{D}_n$ ([SM-Flori 2012]) :

$$f_{a_r,b}(x) = \sum_{r \in R} Tr_1^n(a_r x^{r(2^m-1)}) + Tr_1^t(bx^{s(2^m-1)})$$

where

- R is a set of representatives of the cyclotomic classes modulo 2^m+1 (not necessary of maximal size as in the Charpin-Gong criterion)
- the coefficients a_r are in $\mathbb{F}_{2^m}$,
- s divides 2^m+1, i.e $s(2^m-1)$ is a Dillon-like exponent. Set $\tau = \frac{2^m+1}{s}$.
- $t = o(s(2^m-1))$, i.e t is the size of the cyclotomic coset of s modulo 2^m+1,
- the coefficient b is in $\mathbb{F}_{2^t}$.

☞ Our approach : generalization of the approach obtained previously in [SM 2009] and [SM 2013].

An application([SM-Flori 2012])

- we characterize the hyper-bentness for a potentially new family

$$f_{a_r,b}(x) = \sum_{r\in R} Tr_1^n(a_r x^{r(2^m-1)}) + Tr_1^6(bx^{\frac{2^n-1}{9}}), b \in \mathbb{F}_{64}^\star, m \equiv 3 \pmod 6$$

- we characterize the hyper-bentness for a potentially new family

$$f_{a_r,b}(x) = \sum_{r\in R} Tr_1^n(a_r x^{r(2^m-1)}) + Tr_1^{10}(bx^{\frac{2^n-1}{11}}), b \in \mathbb{F}_{2^{10}}^\star, m \equiv 5 \pmod{10}$$

- we characterize the hyper-bentness for a potentially new family

$$f_{a_r,b}(x) = \sum_{r\in R} Tr_1^n(a_r x^{r(2^m-1)}) + Tr_1^{12}(bx^{\frac{2^n-1}{13}}), b \in \mathbb{F}_{2^{12}}^\star, m \equiv 6 \pmod{12}$$

- we characterize the hyper-bentness for a potentially new family

$$f_{a_r,b}(x) = \sum_{r\in R} Tr_1^n(a_r x^{r(2^m-1)}) + Tr_1^8(bx^{\frac{2^n-1}{17}}), b \in \mathbb{F}_{2^8}^\star, m \equiv 4 \pmod 8$$

- we characterize the hyper-bentness for a potentially new family

$$f_{a_r,b}(x) = \sum_{r\in R} Tr_1^n(a_r x^{r(2^m-1)}) + Tr_1^{10}(bx^{\frac{2^n-1}{33}}), b \in \mathbb{F}_{2^{10}}^\star, m \equiv 5 \pmod{10}$$

Hyper-bent functions and hyperelliptic curves

- The characterizations for hyper-bent functions in $\mathcal{D}_n$ requires time and space which is exponential in m !
- We can use the hyperelliptic curve formalism to reduce computational complexity : polynomial time and space in m ([Lisonek 2010],[Flori-SM 2012]).

To obtain efficient characterizations of the hyper-bentness we use :

1. Two fundamental results on the link between Boolean functions, exponential sums and cardinalities of hyperelliptic curve [Flori-SM 2012]
2. The current implementation of point counting over hyperelliptic curves [Vercauteren 2004], [Hubrechts 2007].

DEFINITION

A (imaginary) hyperelliptic curve of genus g over K is a non- singular curve given by an equation of the form $H : y^2 + h(x)y = f(x)$ where $h(x)$ is of degree $\leq g$ and $f(x)$ is monic of degree $2g + 1$

Here we denote $\#H$ the number of $\mathbb{F}_{2^m}$-rational points on H.

Exponential sums and hyperelliptic curves

- A classical link between Kloosterman sums and cardinality of elliptic curves :

THEOREM ([LACHAUD-WOLFMANN 87], [KATZ-LIVNÉ 87])

Let $m \geq 3$, $a \in \mathbb{F}_{2^n}^\star$. Let $E_a : y^2 + xy = x^3 + a$
Then :

$$K_m(a) = -2^m + \#E_a.$$

- Link between exponential sums and cardinalities of hyperelliptic curve : a first fundamental result :

THEOREM ([FLORI-SM 2012])

Let $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ be a function such that $f(0) = 0$ and G_f be the (affine) curve defined over $\mathbb{F}_{2^m}$ by

$$G_f : y^2 + y = f(x)$$

Then :

$$\sum_{x \in \mathbb{F}_{2^m}^*} \chi(Tr_1^m(f)(x)) = -2^m - 1 + \#G_f.$$

Link between exponential sums and cardinalities of hyperelliptic curves : a second fundamental result :

THEOREM ([FLORI-SM 2012])

Let $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ be a function and H_f be the (affine) curve defined over $\mathbb{F}_{2^m}$ by

$$H_f : y^2 + xy = x + x^2 f(x)$$

Then :

$$\sum_{x \in \mathbb{F}_{2^m}^*} \chi(Tr_1^m(1/x) + Tr_1^m(f)(x)) = -2^m + \#H_f.$$

- We have studied the action of Dickson polynomials on subsets of finite fields of even characteristic related to the trace of the inverse of an element which generalizes results of [Charpin-Helleseth-Zonoviev 2009]. Such properties refine our results on the characterizations of hyper-bentness and are used to reduce the number of cardinalities of hyperelliptic curves.

Bent functions whose restrictions to the multiplicative cosets $u\mathbb{F}_{2^m}^\star$ ($u \in U$) are affine

Notation

$\mathcal{A}_n := \{f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ such that the restriction to $u\mathbb{F}_{2^m}^\star$ is affine for every $u \in U\}$

The bent functions in $\mathcal{A}_n$: ([Carlet-SM 2012], [SM 2013]) :

Theorem

The bent functions in $\mathcal{A}_n$ are :

1. Functions which are the sum of a function from the class $\mathcal{PS}_{ap}^{\#}$ and an affine function.
2. Niho bent functions
3. Functions which are the sum of a Niho bent function and the function $1 + \mathbf{1}_{u_0\mathbb{F}_{2^m}}$ or the sum of a Niho bent function and the function $\mathbf{1}_{u_0\mathbb{F}_{2^m}}$ where $u_0 \in U$.

Very recently, we have provided 7 new infinite families of bent functions by explicitly calculating their dual functions [SM 2014] based on a nice result of [Carlet 2004] (a secondary construction of bent functions) :

THEOREM

Let n be an even integer. Let f_1, f_2 and f_3 be three pairwise distinct bent functions over $\mathbb{F}_{2^n}$ such that $\psi = f_3 + f_2 + f_1$ is bent. Let g be a Boolean function defined by $g(x) = f_1(x)f_2(x) + f_1(x)f_3(x) + f_2(x)f_3(x)$. Then g is bent if and only if $\tilde{f}_1 + \tilde{f}_2 + \tilde{f}_3 + \tilde{\psi} = 0$.
Furthermore, if g is bent then its dual function $\tilde{g}$ is given by

$$\tilde{g}(x) = \tilde{f}_1(x)\tilde{f}_2(x) + \tilde{f}_2(x)\tilde{f}_3(x) + \tilde{f}_3(x)\tilde{f}_1(x), \forall x \in \mathbb{F}_{2^n}.$$

Racall The dual function of a bent function f denoted by $\widetilde{f}$ is defined by the equation : $(-1)^{\widetilde{f}(x)} 2^{\frac{n}{2}} = \widehat{\chi_f}(x)$.

Bent vectorial functions

Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^r}$ be an (n, r)-(vectorial) function.
The nonlinearity is defined as the minimum nonlinearity of all their component functions $v \cdot F$ (where "$\cdot$" is a scalar product in $\mathbb{F}_{2^r}$), $v \in \mathbb{F}_{2^r}^\star$ and we have :

$$nl(F) = 2^{n-1} - \frac{1}{2} \max_{v \in \mathbb{F}_{2^r}^\star;\ u \in \mathbb{F}_{2^n}} \left| \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr_1^m(vF(x)) + Tr_1^n(ux)} \right|.$$

Definition (Bent vectorial function)

Let n be an even integer and r be an integer. An (n, r)-function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^r}$ is called bent if the upper bound $2^{n-1} - 2^{n/2-1}$ on its nonlinearity $nl(F)$ is achieved with equality.

- Bent (n, r)-functions exist if and only if n is even and $r \leq \frac{n}{2}$ [Nyberg 1991].
- The bentness of vectorial functions can be characterized by the bentness of their component (Boolean) functions : an (n, r)-function F is bent if and only if all of the component functions of F are bent.

General primary constructions of bent vectorial functions

There exist 5 general constructions of bent vectorial functions :

1. A general construction from the strict Maiorana-McFarland (bent $(2m, r)$-function) : $F(x, y) = L(x\,\pi(y)) + G(y)$, where π permutation of $\mathbb{F}_{2^m}$, and G is any (m, r)-function ;
2. A general construction from the extended Maiorana-McFarland class (bent $(2m, r)$- function) : $F(x, y) = \psi(x, y) + G(y)$ where G is any (m, r)-function ; $\forall y \in \mathbb{F}_{2^m}$, $x \mapsto \psi(x, y)$ is linear ; $\forall x \in \mathbb{F}_{2^m} \setminus \{0\}$, $y \mapsto \psi(x, y)$ is balanced ;
3. A general construction from the general Maiorana-McFarland class ;
4. A general construction form PS_{ap} class (bent $(2m, r)$- function) : $F(x, y) = G\left(\frac{x}{y}\right)$; $(x, y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ where G is a balanced (m, r)-function ;
5. A general construction from Partial Spread construction (bent $(2n + 2m, r)$-function) $F(x, y) = K(\frac{x}{y}, \frac{z}{t})$, where K is a $(n + m, r)$-function st. $\forall x \in \mathbb{F}_{2^n}$, $y \in \mathbb{F}_{2^m} \mapsto K(x, y)$ is balanced and $\forall y \in \mathbb{F}_{2^m}$, $x \in \mathbb{F}_{2^n} \mapsto K(x, y)$ is balanced.

THEOREM ([SM 2014])

Let G be an o-polynomial on $\mathbb{F}_{2^m}$. Let F be a function from $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ to $\mathbb{F}_{2^m}$ such that for $(x, y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$,

$$F(x, y) = xG(yx^{2^m-2}),$$

then the vectorial function F is bent.

Linear codes from hyperovals

- Minimal linear codes are combinatorial objects : linear codes such that the support of every codeword does not contain the support of another linearly independent codeword :

DEFINITION

The *support* of a codeword $c \in \mathcal{C}$ is $supp(c) = \{i \in \{1, \ldots, n\} | c_i \neq 0\}$. A codeword c *covers* a codeword c' if $supp(c') \subset supp(c)$.

DEFINITION (MINIMAL CODEWORD)

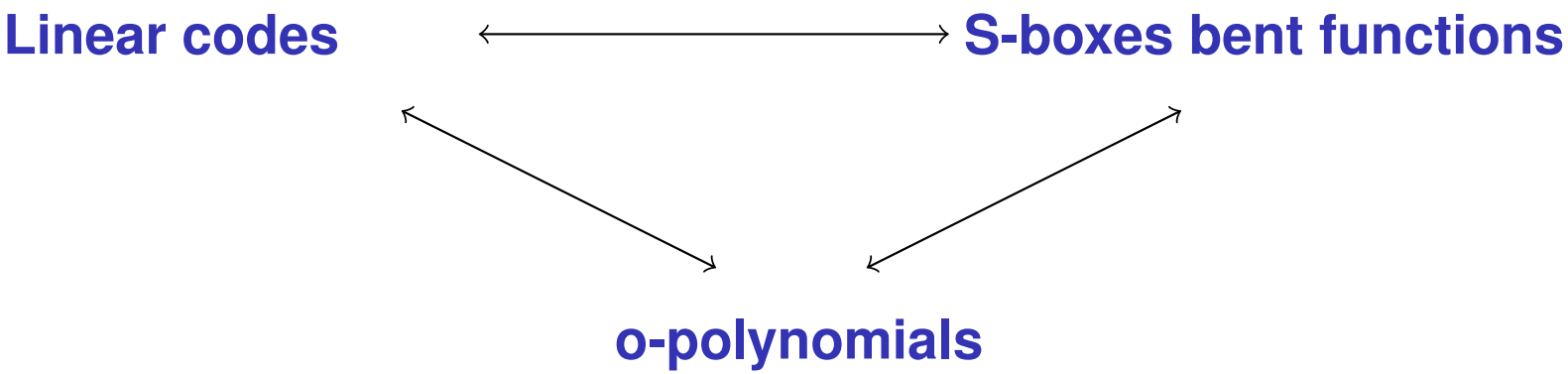
A codeword c is *minimal* if $\forall c' \in \mathcal{C}, (supp(c') \subset supp(c)) \Rightarrow (c, c')$ linearly dependent.

DEFINITION (MINIMAL LINEAR CODE)

A linear code $\mathcal{C}$ is *minimal* if every non-zero codeword $c \in \mathcal{C}$ is minimal.

- the motivation for finding minimal linear codes is no longer secret sharing but in a new proposal for secure two-party computation, where it is required that minimal linear codes are used to ensure privacy.

Codes and S-box from o-polynomials



Minimal codes : algebraic approach

Let m be a positive integer and r a divisor of m.
Let G be an o-polynomial over $\mathbb{F}_{2^m}$ such that $G(0) = 0$. For any $\alpha \in \mathbb{F}_{2^m}$, we define the $(2m, r)$-function f_α as follows :

$$\begin{array}{rccc} f_\alpha & : & \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} & \longrightarrow & \mathbb{F}_{2^r} \\ & & (x, y) & \longmapsto & f_\alpha(x, y) := Tr_r^m(\alpha x G(y x^{2^m-2})). \end{array}$$

Set $\{E_a, E_\infty\}$ where $E_a := \{(x, ax) \mid x \in \mathbb{F}_{2^m}\}$ and $E_\infty := \{(0, y) \mid y \in \mathbb{F}_{2^m}\}$.
$(\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}) \setminus (E_0 \cup E_\infty)$ can be described as $\{(\gamma_i, \zeta_i) \mid 1 \leq i \leq (2^m - 1)^2\}$.
We define a linear code $\mathcal{C}_G$ over (the ambient space) $\mathbb{F}_{2^r}$ as :

$$\begin{aligned} \mathcal{C}_G &:= \{\bar{c}_\alpha = (f_\alpha(\gamma_1, \zeta_1), \cdots, f_\alpha(\gamma_{(2^m-1)^2}, \zeta_{(2^m-1)^2})) \mid \alpha \in \mathbb{F}_{2^m}\} \\ &= \{\bar{c}_\alpha = (Tr_r^m(\alpha \gamma_i G(\zeta_i {\gamma_i}^{2^m-2})) \mid 1 \leq i \leq (2^m - 1)^2); \alpha \in \mathbb{F}_{2^m}\}. \end{aligned} \tag{7}$$

Linear codes from hyperovals give rise to minimal codes !

THEOREM (INCLUDING THE DEFINITION OF q-ARY SIMPLEX CODES)

The q-ary simplex code $\mathcal{S}_k(q)$ is a q-ary code with generator matrix having for columns any set of $\frac{q^k-1}{q-1}$ representatives of the distinct 1-dimensional subspaces of $\mathbb{F}_q^k$.

The q-ary simplex code $\mathcal{S}_k(q)$ has parameters $[\frac{q^k-1}{q-1}, k, q^{k-1}]$

THEOREM ([SM 2014])

Let G be an o-polynomial on $\mathbb{F}_{2^m}$ such that $G(0) = 0$. Then the hyperoval $D(G) = \{(1, t, G(t)), t \in \mathbb{F}_{2^m}\} \cup \{(0, 1, 0), (0, 0, 1)\}$ in the projective space $PG_2(2^m)$ give rise to linear codes $\mathcal{C}$ (constructed via vectorial functions) of a constant weight code with parameters $[(2^m - 1)^2, \frac{m}{r}, 2^{m-r}(2^r - 1)(2^m - 1)]$. Such codes $\mathcal{C}$ are equivalent to $(2^m - 1)(2^r - 1)$-multiples of 2^r-ary simplex codes $\mathcal{S}_{\frac{m}{r}}(2^r)$ where r is a divisor of m whose duals are the 2^r-ary perfect single error-correcting Hamming codes.

Minimal Linear codes : asymptotic approach

Asymptotic approach : Upper bound, non-existence, construction by concatenation, etc.[Cohen-SM-Patey 2013] :

Theorem (Maximal Bound)

Let $\mathcal{C}$ a minimal linear $[n, k, d]$ q-ary code, then, asymptotically, $R := k/n \leq \log_q(2)$.

Definition (Quasi-minimal codeword)

A codeword c is *quasi-minimal* if $\forall c' \in \mathcal{C}, (supp(c') = supp(c)) \implies (c, c')$ linearly dependent.

Definition (Quasi-minimal linear code)

A linear code $\mathcal{C}$ is *quasi-minimal* if every non-zero codeword $c \in \mathcal{C}$ is quasi-minimal.

Theorem (Maximal Bound)

Let $\mathcal{C}$ be a quasi-minimal linear $[n, k, d]_q$ code, then, asymptotically, $R := k/n \leq \log_q(2)$.

Combinatorial approach : constructions, finite properties, etc.
[Cohen-SM-Patey 2013] :

THEOREM (SUFFICIENT CONDITION FOR QUASI-MINIMALITY)

Let C be a linear $[n,k,d]_q$ code ; if $d/n > (q-2)/(q-1)$, then C is quasi-minimal.

PROPOSITION

The product $\mathcal{C}_1 \otimes \mathcal{C}_2$ of a minimal $[n_1,k_1,d_1]_q$ code $\mathcal{C}_1$ and of a minimal $[n_2,k_2,d_2]_q$ code $\mathcal{C}_2$ is a minimal $[n_1 \times n_2, k_1 \times k_2, d_1 \times d_2]_q$ code.

Probabilistic approach : results of existence, non-constructive,etc.
[Cohen-SM-Patey 2013] :

THEOREM (MINIMAL BOUND)

For any R, $0 \leq R = k/n \leq \frac{1}{2}\log_q(\frac{q^2}{q^2-q+1})$, there exists an infinite sequence of $[n,k]$ minimal linear codes.

Open questions :

- Study the difference sets related to the class of hyperbent functions ;
- Improve the upper bound on the number of bent functions ; asymptotic bounds (asymptotic approach, etc).
- Study further the combinatorial aspect of the minimal codes in order to exhibit more "good" codes
- Improve the upper bound on the covering radius using combinatorial idea (combinatorial words, etc).
- Links between finite geometry and combinatoric (? !)