

Algebraic Approaches to Linear Cryptanalysis of Symmetric Primitives over Prime Fields

Clémence Bouvier

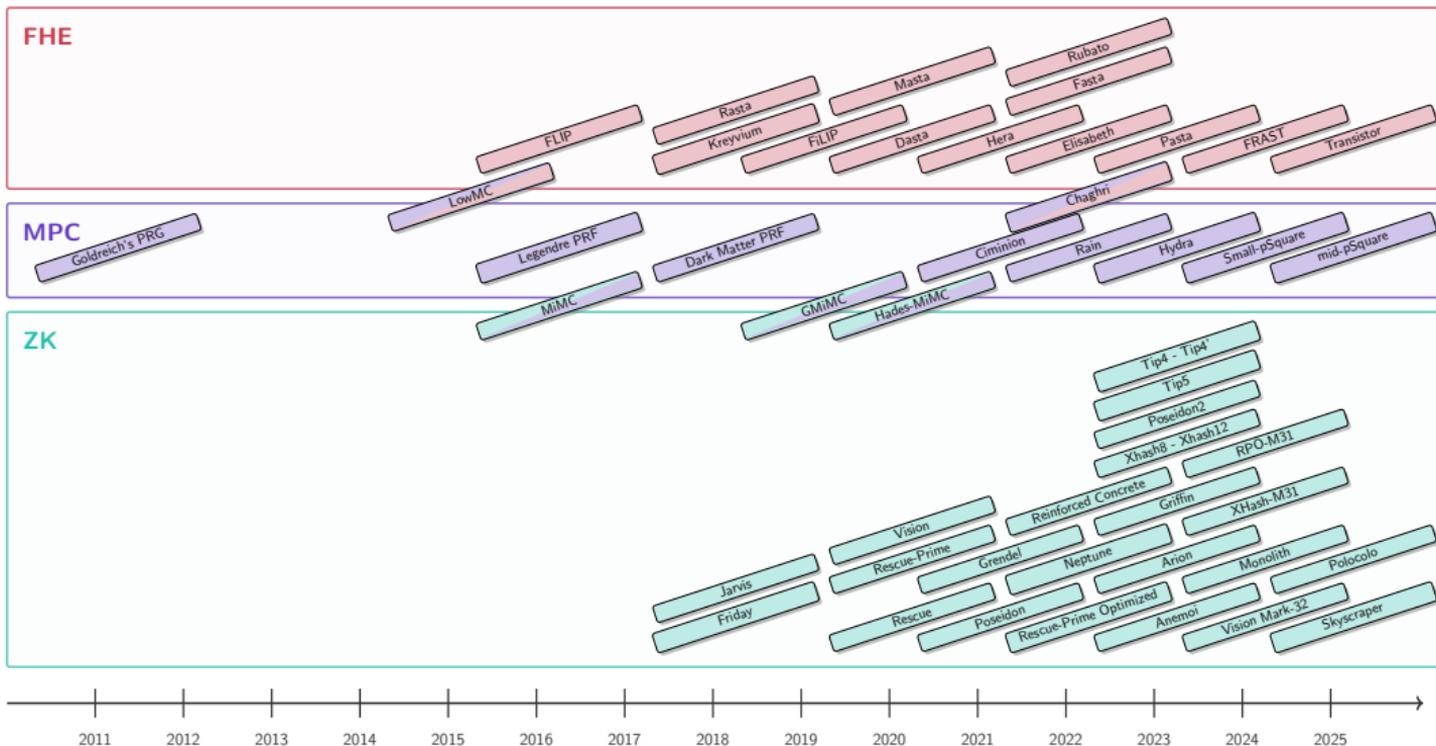
Université de Lorraine, CNRS, Inria, LORIA

(joint work with Tim Beyne)

ULB, Brussels, Belgium
February 19th, 2026



New symmetric primitives



A new context

Traditional case

Alphabet

Operations based on logical gates or CPU instructions.

$$\mathbb{F}_2^n, \text{ with } n \simeq 4, 8$$

Arithmetization-Oriented

Alphabet

Operations based on large finite-field arithmetic.

$$\mathbb{F}_q, \text{ with } q \in \{2^n, p\}, p \simeq 2^n, n \geq 32$$

A new context

Traditional case

Alphabet

Operations based on logical gates or CPU instructions.

$$\mathbb{F}_2^n, \text{ with } n \simeq 4, 8$$

Cryptanalysis

Decades of cryptanalysis

- ★ algebraic attacks ✓
- ★ differential attacks ✓
- ★ linear attacks ✓
- ★ ...

Arithmetization-Oriented

Alphabet

Operations based on large finite-field arithmetic.

$$\mathbb{F}_q, \text{ with } q \in \{2^n, p\}, p \simeq 2^n, n \geq 32$$

Cryptanalysis

≤ 10 years of cryptanalysis

- ★ algebraic attacks ✓
- ★ differential attacks ✗
- ★ linear attacks ✗
- ★ ...

Correlation of linear approximations

Definition

The **correlation of the linear approximation** (u, v) of $F : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^m$ is

$$C_{u,v}^F = \frac{1}{q^n} \sum_{x \in \mathbb{F}_q^n} \omega(\langle v, F(x) \rangle - \langle u, x \rangle),$$

where ω is a primitive element.

Correlation of linear approximations

Definition

The **correlation of the linear approximation** (u, v) of $F : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^m$ is

$$C_{u,v}^F = \frac{1}{q^n} \sum_{x \in \mathbb{F}_q^n} \omega(\langle v, F(x) \rangle - \langle u, x \rangle),$$

where ω is a primitive element.

Examples:

★ If $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$, then

$$C_{u,v}^F = \frac{1}{2^n} \sum_{x \in \mathbb{F}_2^n} (-1)^{\langle v, F(x) \rangle + \langle u, x \rangle}.$$

★ If $F : \mathbb{F}_p^n \rightarrow \mathbb{F}_p^m$, then

$$C_{u,v}^F = \frac{1}{p^n} \sum_{x \in \mathbb{F}_p^n} e^{\left(\frac{2i\pi}{p}\right)(\langle v, F(x) \rangle - \langle u, x \rangle)}.$$

Walsh transform

Definition

The **Walsh transform** for the character ω of the linear approximation (u, v) of $F : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^m$ is given by

$$\mathcal{W}_{u,v}^F = \sum_{x \in \mathbb{F}_q^n} \omega(\langle v, F(x) \rangle - \langle u, x \rangle) .$$

$$\mathcal{W}_{u,v}^F = q^n \cdot C_{u,v}^F$$

Walsh transform

Definition

The **Walsh transform** for the character ω of the linear approximation (u, v) of $F : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^m$ is given by

$$\mathcal{W}_{u,v}^F = \sum_{x \in \mathbb{F}_q^n} \omega(\langle v, F(x) \rangle - \langle u, x \rangle) .$$

$$\mathcal{W}_{u,v}^F = q^n \cdot C_{u,v}^F$$

Definition

The **Linearity** \mathcal{L}_F of $F : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^m$ is the highest Walsh coefficient.

$$\mathcal{L}_F = \max_{u,v \in \mathbb{F}_q, v \neq 0} |\mathcal{W}_{u,v}^F| .$$

Walsh transform

Definition

The **Walsh transform** for the character ω of the linear approximation (u, v) of $F : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^m$ is given by

$$\mathcal{W}_{u,v}^F = \sum_{x \in \mathbb{F}_q^n} \omega(\langle v, F(x) \rangle - \langle u, x \rangle) .$$

$$\mathcal{W}_{u,v}^F = q^n \cdot C_{u,v}^F$$

Definition

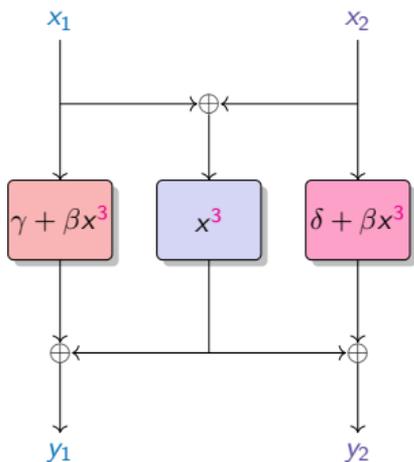
The **Linearity** \mathcal{L}_F of $F : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^m$ is the highest Walsh coefficient.

$$\mathcal{L}_F = \max_{u,v \in \mathbb{F}_q, v \neq 0} |\mathcal{W}_{u,v}^F| .$$

Example: If $F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}, x \mapsto Lx + c$, then $\mathcal{L}_F = 2^n$ and $C_F = 1$.

Closed Flystel in \mathbb{F}_{2^n}

Introduced by [Bouvier, Briaud, Chaidos, Perrin, Salen, Velichkov and Willems, 2023].



Closed Flystel.

$$\mathcal{L}_F = \max_{u, v \neq 0} \left| \sum_{x \in \mathbb{F}_{2^n}^2} (-1)^{(\langle v, F(x) \rangle - \langle u, x \rangle)} \right|$$

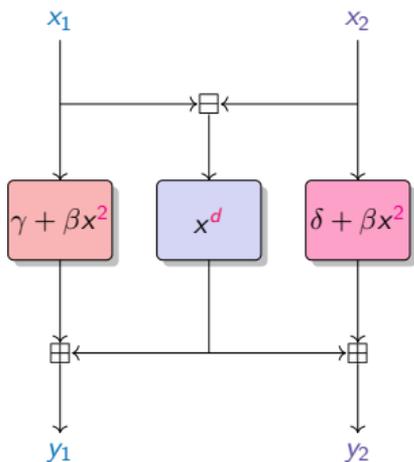
Bound

Linearity bound for the Flystel:

$$\mathcal{L}_F \leq 2^{n+1}$$

Closed Flystel in \mathbb{F}_p

Introduced by [Bouvier, Briaud, Chaidos, Perrin, Salen, Velichkov and Willems, 2023].



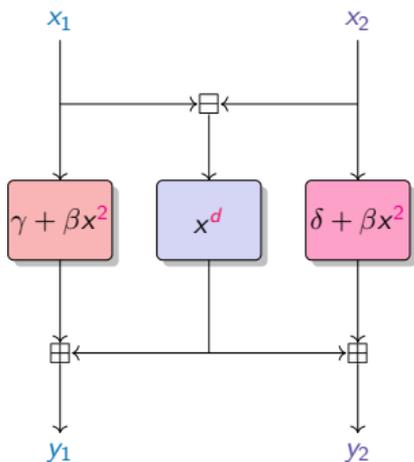
Closed Flystel.

d is a small integer s.t.
 $x \mapsto x^d$ is a permutation of \mathbb{F}_p
 (usually $d = 3, 5$).

$$\mathcal{L}_F = \max_{u, v \neq 0} \left| \sum_{x \in \mathbb{F}_p^2} e\left(\frac{2i\pi}{p}\right) (\langle v, F(x) \rangle - \langle u, x \rangle) \right|$$

Closed Flystel in \mathbb{F}_p

Introduced by [Bouvier, Briaud, Chaidos, Perrin, Salen, Velichkov and Willems, 2023].



Closed Flystel.

d is a small integer s.t.
 $x \mapsto x^d$ is a permutation of \mathbb{F}_p
 (usually $d = 3, 5$).

$$\mathcal{L}_F = \max_{u, v \neq 0} \left| \sum_{x \in \mathbb{F}_p^2} e\left(\frac{2i\pi}{p}\right) (\langle v, F(x) \rangle - \langle u, x \rangle) \right|$$

How to determine an accurate bound for the linearity of the Closed Flystel in \mathbb{F}_p ?

Weil bound

Proposition [Weil, 1948]

Let $f \in \mathbb{F}_p[x]$ be a univariate polynomial with $\deg(f) = d$. Then

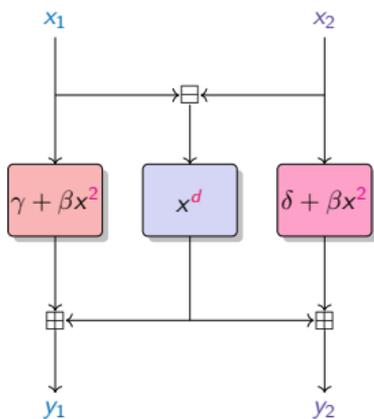
$$\mathcal{L}_f \leq (d - 1)\sqrt{p}$$

Weil bound

Proposition [Weil, 1948]

Let $f \in \mathbb{F}_p[x]$ be a univariate polynomial with $\deg(f) = d$. Then

$$\mathcal{L}_f \leq (d - 1)\sqrt{p}$$



Closed Flystel.

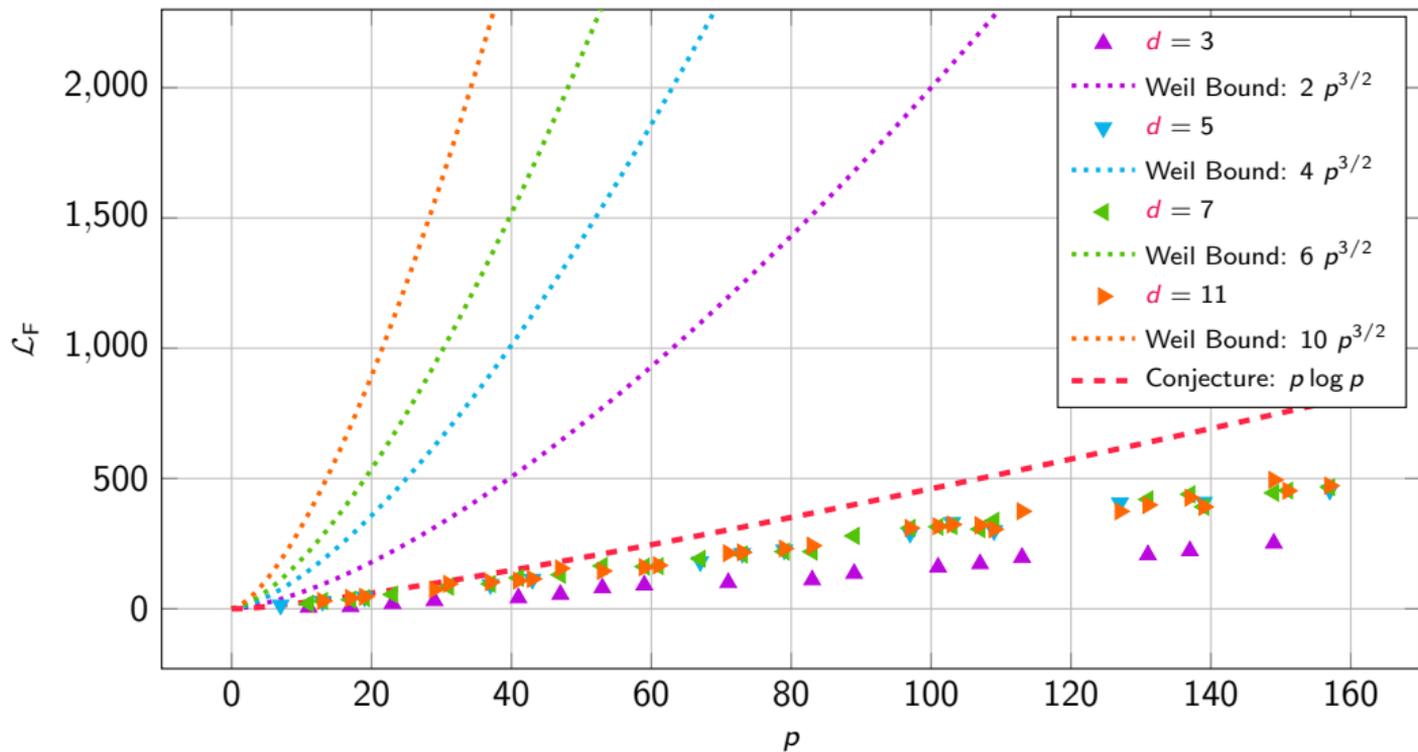
$$\mathcal{L}_F \leq (d - 1)p\sqrt{p} ?$$

$$\begin{cases} \mathcal{L}_{\gamma + \beta x^2} \leq \sqrt{p}, \\ \mathcal{L}_{x^d} \leq (d - 1)\sqrt{p}, \\ \mathcal{L}_{\delta + \beta x^2} \leq \sqrt{p}. \end{cases}$$

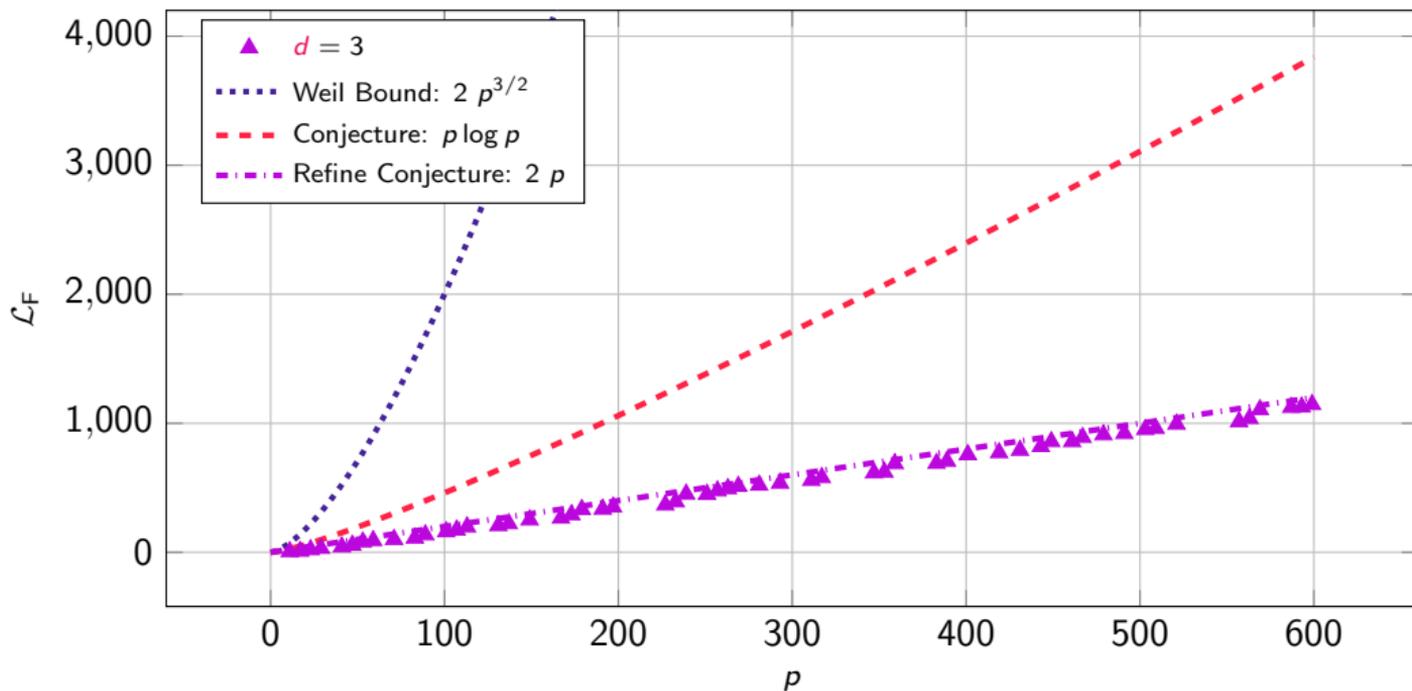
Conjecture

$$\mathcal{L}_F = \sum_{x \in \mathbb{F}_p^2} e\left(\frac{2i\pi}{p}\right)(\langle v, F(x) \rangle - \langle u, x \rangle) \leq p \log p$$

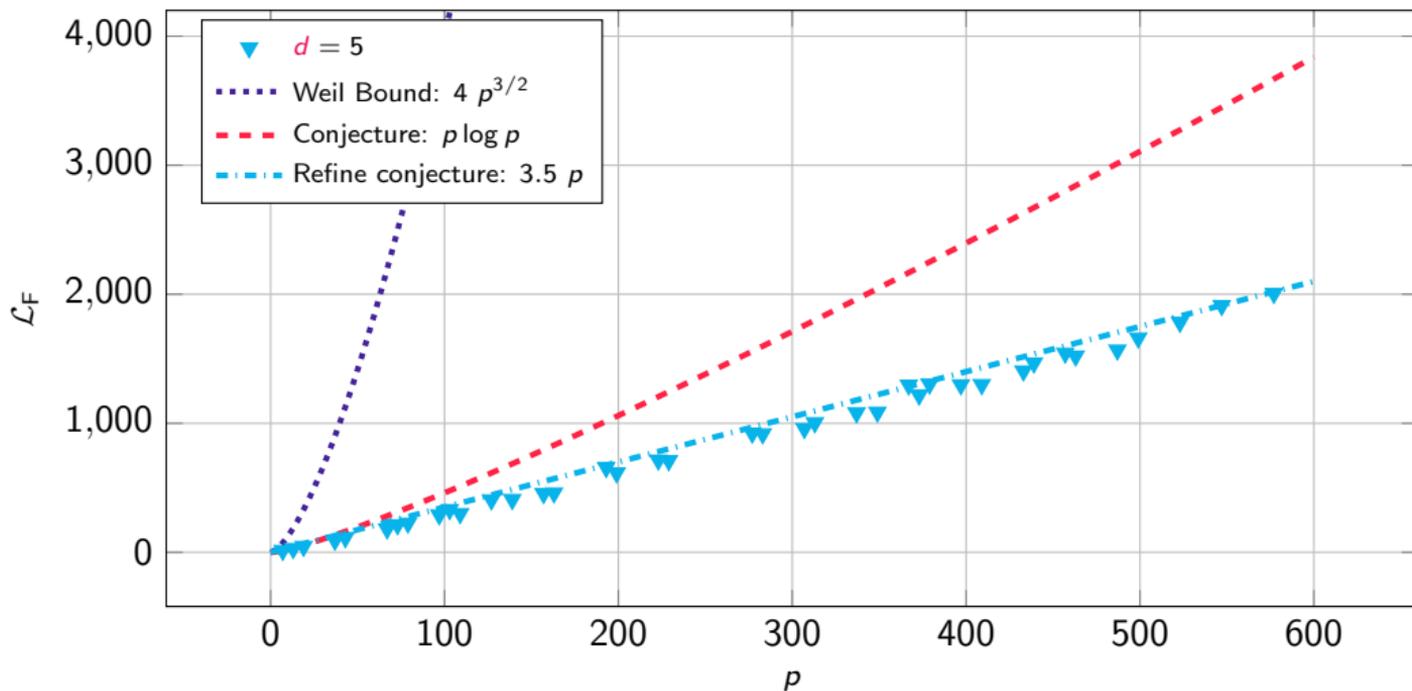
Experimental results



Experimental results ($d = 3$)



Experimental results ($d = 5$)



Take-away

AO primitives: new symmetric primitives defined over prime fields.

Need for new linear cryptanalysis tools

Take-away

AO primitives: new symmetric primitives defined over prime fields.

Need for new linear cryptanalysis tools

This Talk:

Beyne and Bouvier, JoC 2026 - to appear
(more details at ia.cr/2024/1755)

- ★ Applications of results for **exponential sums** (generalization of **Weil bound**)

$$\mathcal{W}_{u,v}^F = \sum_{x \in \mathbb{F}_q^n} \omega(\langle v, F(x) \rangle - \langle u, x \rangle) \quad \rightarrow \quad S(f) = \sum_{x \in \mathbb{F}_q^n} \omega^{f(x)} .$$

- ★ \mathbb{F}_q is a **finite field** s.t. q is a power of a prime p .
- ★ Functions with **2 variables** $F \in \mathbb{F}_q[x_1, x_2]$.

Generalizations of Weil bound

- ★ **Deligne** bound

 - ★ Application to the **Generalized Butterfly** construction

- ★ Denef and Loeser bound

 - ★ Application to 3-round Feistel construction

- ★ Rojas-León bound

 - ★ Application to the Generalized Flystel construction

Smoothness

Definition

Let $f \in \mathbb{F}_q[x_1, \dots, x_n]$. A hypersurface defined by $f = 0$ is **smooth**, if the system

$$f = \partial f / \partial x_1 = \dots = \partial f / \partial x_n = 0$$

has no non zero solutions.

Smoothness

Definition

Let $f \in \mathbb{F}_q[x_1, \dots, x_n]$. A hypersurface defined by $f = 0$ is **smooth**, if the system

$$f = \partial f / \partial x_1 = \dots = \partial f / \partial x_n = 0$$

has no non zero solutions.

Examples:

★ $f(x_1, x_2) = 2x_1^3 + x_2^2 = 0$ is **smooth**, since

$$\partial f / \partial x_1 = 6x_1^2 \quad \text{and} \quad \partial f / \partial x_2 = 2x_2,$$

so that

$$f = \partial f / \partial x_1 = \partial f / \partial x_2 = 0 \quad \Leftrightarrow \quad (x_1, x_2) = (0, 0).$$

Smoothness

Definition

Let $f \in \mathbb{F}_q[x_1, \dots, x_n]$. A hypersurface defined by $f = 0$ is **smooth**, if the system

$$f = \partial f / \partial x_1 = \dots = \partial f / \partial x_n = 0$$

has no non zero solutions.

Examples:

★ $f(x_1, x_2) = 2x_1^3 + x_2^2 = 0$ is **smooth**, since

$$\partial f / \partial x_1 = 6x_1^2 \quad \text{and} \quad \partial f / \partial x_2 = 2x_2,$$

so that

$$f = \partial f / \partial x_1 = \partial f / \partial x_2 = 0 \quad \Leftrightarrow \quad (x_1, x_2) = (0, 0).$$

★ $f(x_1, x_2) = x_1^2 + x_2^2 - 2x_2 + 1 = 0$ is **not smooth**, since

$$\partial f / \partial x_1 = 2x_1 \quad \text{and} \quad \partial f / \partial x_2 = 2x_2 - 2,$$

so that

$$f = \partial f / \partial x_1 = \partial f / \partial x_2 = 0 \quad \Leftrightarrow \quad (x_1, x_2) = (0, 1).$$

Deligne Theorem

Theorem [Deligne, 1974]

Let q be a power of a prime p .

Let $f \in \mathbb{F}_q[x_1, \dots, x_n]$ be a polynomial of degree d , with $\gcd(d, p) = 1$.

Let f_d be the **degree d homogeneous component** of f , i.e.

$$f = f_d + g, \quad \deg(g) < d .$$

If the hypersurface defined by $f_d = 0$ is **smooth**, then, we have

$$|S(f)| = \left| \sum_{x \in \mathbb{F}_q^n} \omega^{f(x)} \right| \leq (d-1)^n \cdot q^{n/2} .$$

Deligne Theorem

Theorem [Deligne, 1974]

Let q be a power of a prime p .

Let $f \in \mathbb{F}_q[x_1, \dots, x_n]$ be a polynomial of degree d , with $\gcd(d, p) = 1$.

Let f_d be the **degree d homogeneous component** of f , i.e.

$$f = f_d + g, \quad \deg(g) < d.$$

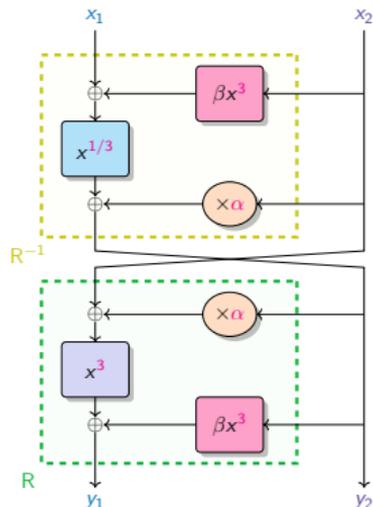
If the hypersurface defined by $f_d = 0$ is **smooth**, then, we have

$$|S(f)| = \left| \sum_{x \in \mathbb{F}_q^n} \omega^{f(x)} \right| \leq (d-1)^n \cdot q^{n/2}.$$

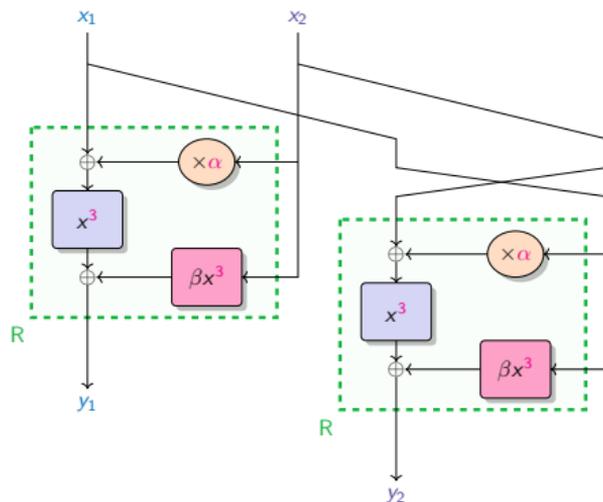
$\text{Linearity bound for } n = 2: \mathcal{L}_F \leq (d-1)^2 \cdot q.$

Butterfly - Definition

Introduced by [Perrin, Udovenko and Biryukov, 2016] over binary fields, $\mathbb{F}_{2^n}^2$, n odd.



Open variant.



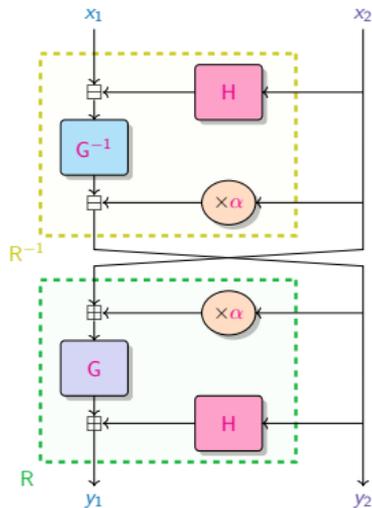
Closed variant.

$$\begin{cases} y_1 = (x_2 + \alpha y_2)^3 + (\beta y_2)^3 \\ y_2 = (x_1 - (\beta x_2)^3)^{1/3} - \alpha x_2 \end{cases}$$

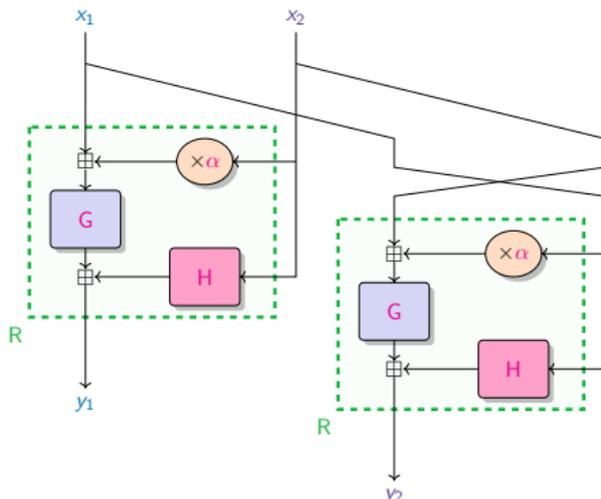
$$\begin{cases} y_1 = (x_1 + \alpha x_2)^3 + (\beta x_2)^3 \\ y_2 = (x_2 + \alpha x_1)^3 + (\beta x_1)^3 \end{cases}$$

Generalized Butterfly - Definition

BUTTERFLY[G, H, α], with $G : \mathbb{F}_q \rightarrow \mathbb{F}_q$ a permutation, $H : \mathbb{F}_q \rightarrow \mathbb{F}_q$ a function and $\alpha \in \mathbb{F}_q$.



Open variant.



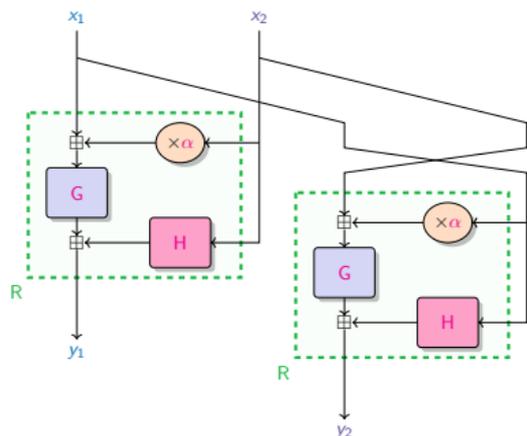
Closed variant.

$$\begin{cases} y_1 &= G(x_2 + \alpha y_2) + H(y_2) \\ y_2 &= G^{-1}(x_1 - H(x_2)) - \alpha x_2. \end{cases}$$

$$\begin{cases} y_1 &= G(x_1 + \alpha x_2) + H(x_2) \\ y_2 &= G(x_2 + \alpha x_1) + H(x_1). \end{cases}$$

Generalized Butterfly - Bound

Let $F = \text{BUTTERFLY}[G, H, \alpha]$, with G a permutation, H a function and α in \mathbb{F}_q .



$$\begin{cases} y_1 &= G(x_1 + \alpha x_2) + H(x_2) \\ y_2 &= G(x_2 + \alpha x_1) + H(x_1). \end{cases}$$

Reminder

Linearity of $F : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$:

$$\mathcal{L}_F = \max_{u, v \in \mathbb{F}_q^n, v \neq 0} \left| \sum_{x \in \mathbb{F}_q^n} \omega^{\langle v, F(x) \rangle - \langle u, x \rangle} \right|.$$

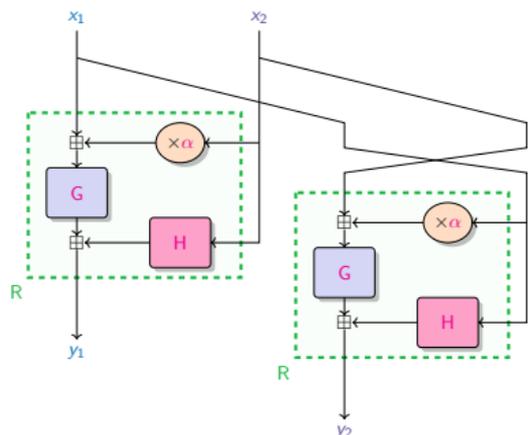
We denote:

$$S(f) = \sum_{x \in \mathbb{F}_q^n} \omega^{f(x)}.$$

Generalized Butterfly - Bound

Let $F = \text{BUTTERFLY}[G, H, \alpha]$, with G a permutation, H a function and α in \mathbb{F}_q .

$$\begin{aligned} f(x_1, x_2) &= \langle (v_1, v_2), F(x_1, x_2) \rangle - \langle (u_1, u_2), (x_1, x_2) \rangle \\ &= v_1 G(x_1 + \alpha x_2) + v_2 G(x_2 + \alpha x_1) + v_1 H(x_2) + v_2 H(x_1) - u_1 x_1 - u_2 x_2 . \end{aligned}$$



$$\begin{cases} y_1 = G(x_1 + \alpha x_2) + H(x_2) \\ y_2 = G(x_2 + \alpha x_1) + H(x_1) . \end{cases}$$

Reminder

Linearity of $F : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$:

$$\mathcal{L}_F = \max_{u, v \in \mathbb{F}_q^n, v \neq 0} \left| \sum_{x \in \mathbb{F}_q^n} \omega^{\langle (v, F(x)) - \langle u, x \rangle \rangle} \right| .$$

We denote:

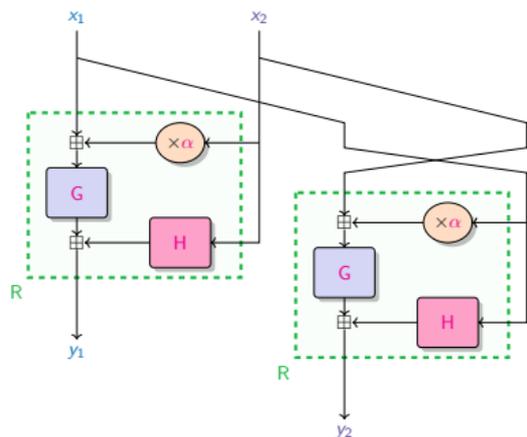
$$S(f) = \sum_{x \in \mathbb{F}_q^n} \omega^{f(x)} .$$

Generalized Butterfly - Bound

Let $F = \text{BUTTERFLY}[G, H, \alpha]$, with G a permutation, H a function and α in \mathbb{F}_q .

$$f(x_1, x_2) = \langle (v_1, v_2), F(x_1, x_2) \rangle - \langle (u_1, u_2), (x_1, x_2) \rangle$$

$$= v_1 G(x_1 + \alpha x_2) + v_2 G(x_2 + \alpha x_1) + v_1 H(x_2) + v_2 H(x_1) - u_1 x_1 - u_2 x_2 .$$



$$\begin{cases} y_1 = G(x_1 + \alpha x_2) + H(x_2) \\ y_2 = G(x_2 + \alpha x_1) + H(x_1) . \end{cases}$$

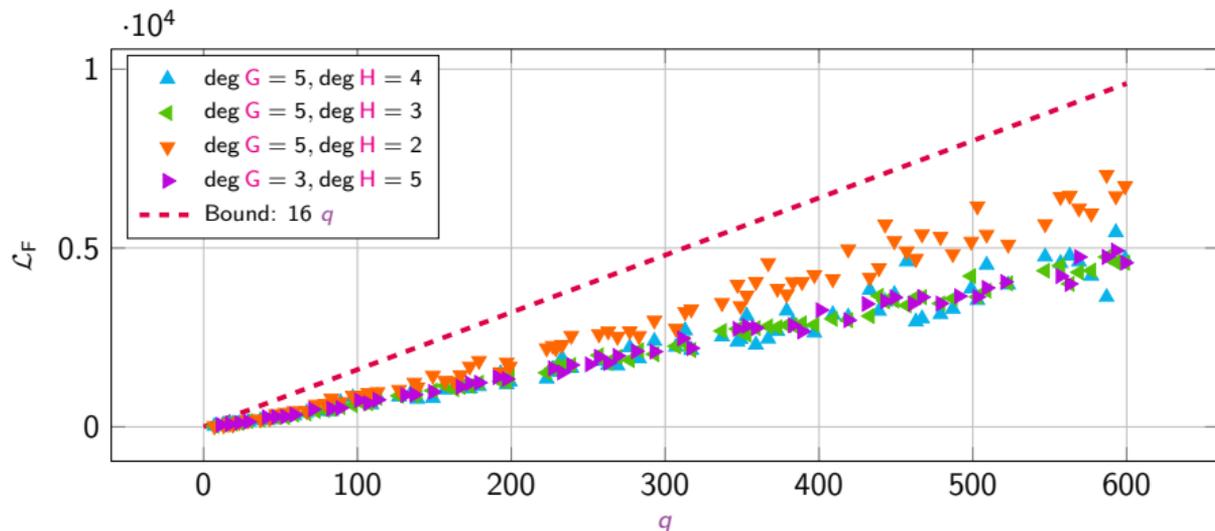
Linearity Bound

- ★ If $d = \deg G > \deg H > 1$, then and $\alpha \neq \pm 1$,
 $f_d = (x_1 + \alpha x_2)^d + v_2/v_1(x_2 + \alpha x_1)^d = 0$ is smooth.
- ★ If $d = \deg H > \deg G > 1$, then
 $f_d = x_1^d + v_1/v_2 x_2^d = 0$ is smooth.

$$\mathcal{L}_F \leq (\max\{\deg G, \deg H\} - 1)^2 \cdot q$$

Generalized Butterfly - Results

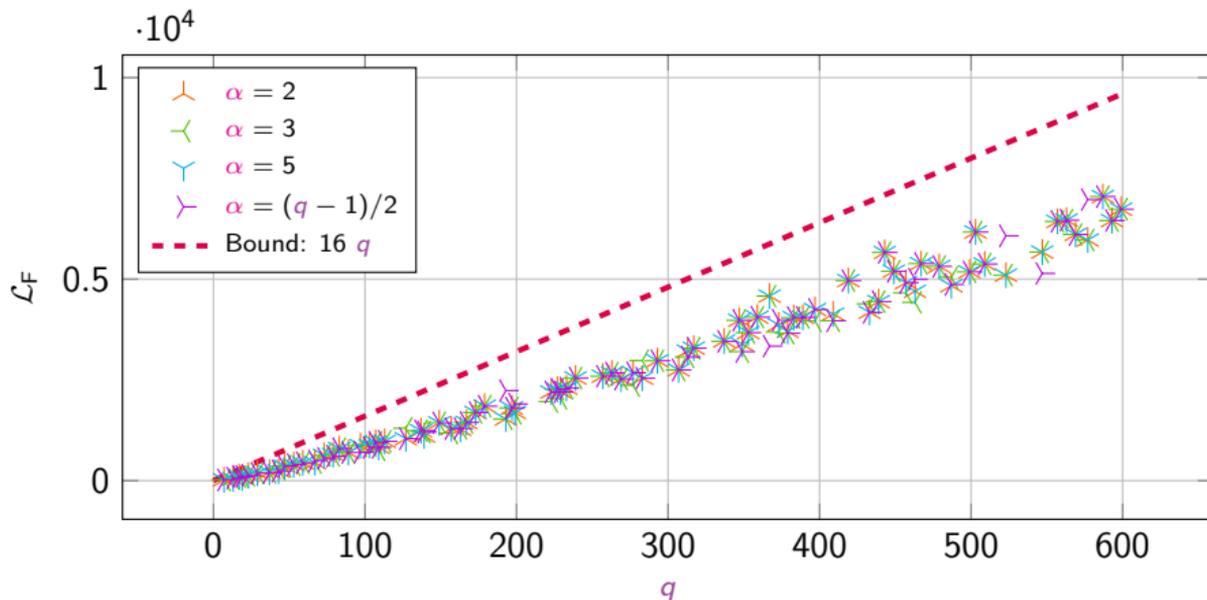
Let $F = \text{BUTTERFLY}[G, H, \alpha]$ with G and H monomial functions.



Low-degree functions ($\max\{\deg G, \deg H\} = 5$ and $\alpha = 2$).

Generalized Butterfly - Results

Let $F = \text{BUTTERFLY}[G, H, \alpha]$ with G and H monomial functions.



Influence of α (deg $G = 5$ and deg $H = 2$).

Generalizations of Weil bound

- ★ Deligne bound
 - ★ Application to the Generalized Butterfly construction
- ★ **Denef and Loeser** bound
 - ★ Application to **3-round Feistel** construction
- ★ Rojas-León bound
 - ★ Application to the Generalized Flystel construction

Newton Polyhedron

Definition

Let $f \in \mathbb{F}_q[x_1, \dots, x_n]$ s.t.

$$f(x_1, \dots, x_n) = \sum_{e_1, \dots, e_n} c_{e_1, \dots, e_n} \prod_{i=1}^n x_i^{e_i} .$$

The **Newton polyhedron** $\Delta(f)$ of f is the convex hull defined by

$$\{(0, \dots, 0)\} \cup \{(e_1, \dots, e_n) \mid c_{e_1, \dots, e_n} \neq 0\} \subset \mathbb{R}^n .$$

Newton Polyhedron

Definition

Let $f \in \mathbb{F}_q[x_1, \dots, x_n]$ s.t.

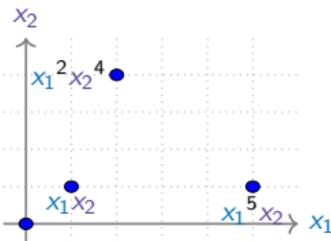
$$f(x_1, \dots, x_n) = \sum_{e_1, \dots, e_n} c_{e_1, \dots, e_n} \prod_{i=1}^n x_i^{e_i} .$$

The **Newton polyhedron** $\Delta(f)$ of f is the convex hull defined by

$$\{(0, \dots, 0)\} \cup \{(e_1, \dots, e_n) \mid c_{e_1, \dots, e_n} \neq 0\} \subset \mathbb{R}^n .$$

Examples:

$$f(x_1, x_2) = 1 + x_1 x_2 - 2x_1^2 x_2^4 + 3x_1^5 x_2$$



Newton Polyhedron

Definition

Let $f \in \mathbb{F}_q[x_1, \dots, x_n]$ s.t.

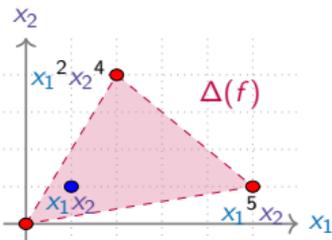
$$f(x_1, \dots, x_n) = \sum_{e_1, \dots, e_n} c_{e_1, \dots, e_n} \prod_{i=1}^n x_i^{e_i}.$$

The **Newton polyhedron** $\Delta(f)$ of f is the convex hull defined by

$$\{(0, \dots, 0)\} \cup \{(e_1, \dots, e_n) \mid c_{e_1, \dots, e_n} \neq 0\} \subset \mathbb{R}^n.$$

Examples:

$$f(x_1, x_2) = 1 + x_1 x_2 - 2x_1^2 x_2^4 + 3x_1^5 x_2$$



Newton Polyhedron

Definition

Let $f \in \mathbb{F}_q[x_1, \dots, x_n]$ s.t.

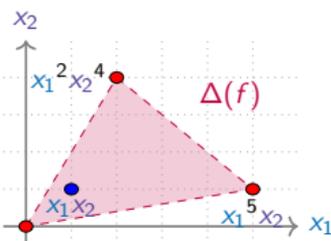
$$f(x_1, \dots, x_n) = \sum_{e_1, \dots, e_n} c_{e_1, \dots, e_n} \prod_{i=1}^n x_i^{e_i}.$$

The **Newton polyhedron** $\Delta(f)$ of f is the convex hull defined by

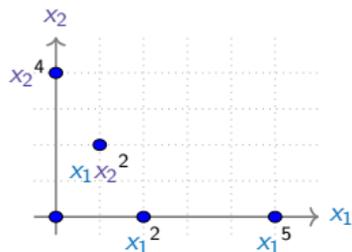
$$\{(0, \dots, 0)\} \cup \{(e_1, \dots, e_n) \mid c_{e_1, \dots, e_n} \neq 0\} \subset \mathbb{R}^n.$$

Examples:

$$f(x_1, x_2) = 1 + x_1 x_2 - 2x_1^2 x_2^4 + 3x_1^5 x_2$$



$$f(x_1, x_2) = 3 - x_1^2 + 5x_1 x_2^2 + x_2^4 + 9x_1^5$$



Newton Polyhedron

Definition

Let $f \in \mathbb{F}_q[x_1, \dots, x_n]$ s.t.

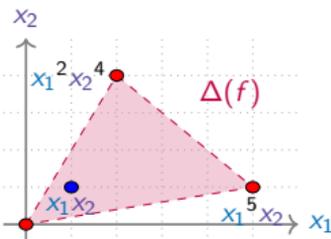
$$f(x_1, \dots, x_n) = \sum_{e_1, \dots, e_n} c_{e_1, \dots, e_n} \prod_{i=1}^n x_i^{e_i} .$$

The **Newton polyhedron** $\Delta(f)$ of f is the convex hull defined by

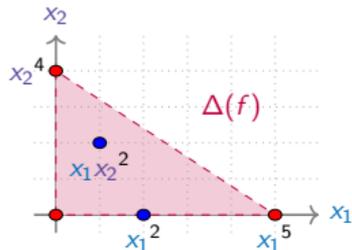
$$\{(0, \dots, 0)\} \cup \{(e_1, \dots, e_n) \mid c_{e_1, \dots, e_n} \neq 0\} \subset \mathbb{R}^n .$$

Examples:

$$f(x_1, x_2) = 1 + x_1 x_2 - 2x_1^2 x_2^4 + 3x_1^5 x_2$$



$$f(x_1, x_2) = 3 - x_1^2 + 5x_1 x_2^2 + x_2^4 + 9x_1^5$$



Newton Number

Definition

Let $f \in \mathbb{F}_q[x_1, \dots, x_n]$. The **Newton number** $\nu(f)$ of f is

$$\nu(f) = \sum_{I \subseteq \{1, \dots, n\}} (-1)^{|I|} (n - |I|)! \text{Vol}_I \Delta(f),$$

where $\text{Vol}_I \Delta(f)$ is the volume of $\Delta(f) \cap_{i \in I} \{x_i = 0\}$

Newton Number

Definition

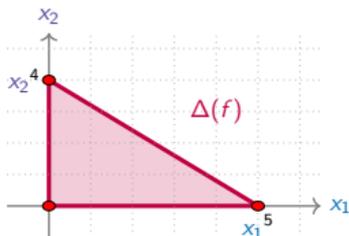
Let $f \in \mathbb{F}_q[x_1, \dots, x_n]$. The **Newton number** $\nu(f)$ of f is

$$\nu(f) = \sum_{I \subseteq \{1, \dots, n\}} (-1)^{|I|} (n - |I|)! \text{Vol}_I \Delta(f),$$

where $\text{Vol}_I \Delta(f)$ is the volume of $\Delta(f) \cap_{i \in I} \{x_i = 0\}$

Example:

$$f(x_1, x_2) = 3 - x_1^2 + 5x_1x_2^2 + x_2^4 + 9x_1^5$$



Newton Number

Definition

Let $f \in \mathbb{F}_q[x_1, \dots, x_n]$. The **Newton number** $\nu(f)$ of f is

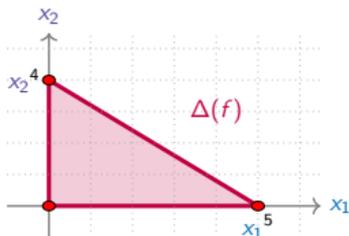
$$\nu(f) = \sum_{I \subseteq \{1, \dots, n\}} (-1)^{|I|} (n - |I|)! \text{Vol}_I \Delta(f),$$

where $\text{Vol}_I \Delta(f)$ is the volume of $\Delta(f) \cap_{i \in I} \{x_i = 0\}$

Example:

$$f(x_1, x_2) = 3 - x_1^2 + 5x_1x_2^2 + x_2^4 + 9x_1^5$$

$$\nu(f) = (-1)^0 \cdot 2! \cdot \text{Vol}_{\Delta(f)}$$



$$= 2 \times (5 \times 4) / 2$$

Newton Number

Definition

Let $f \in \mathbb{F}_q[x_1, \dots, x_n]$. The **Newton number** $\nu(f)$ of f is

$$\nu(f) = \sum_{I \subseteq \{1, \dots, n\}} (-1)^{|I|} (n - |I|)! \text{Vol}_I \Delta(f),$$

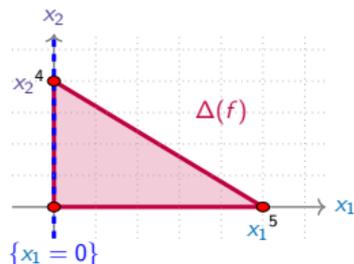
where $\text{Vol}_I \Delta(f)$ is the volume of $\Delta(f) \cap \bigcap_{i \in I} \{x_i = 0\}$

Example:

$$f(x_1, x_2) = 3 - x_1^2 + 5x_1x_2^2 + x_2^4 + 9x_1^5$$

$$\begin{aligned} \nu(f) &= (-1)^0 \cdot 2! \cdot \text{Vol}_{\Delta(f)} \\ &\quad + (-1)^1 \cdot 1! \cdot \text{Vol}_{\Delta(f) \cap \{x_1=0\}} \end{aligned} \quad (I = \{1\})$$

$$= 2 \times (5 \times 4) / 2 - 4$$



Newton Number

Definition

Let $f \in \mathbb{F}_q[x_1, \dots, x_n]$. The **Newton number** $\nu(f)$ of f is

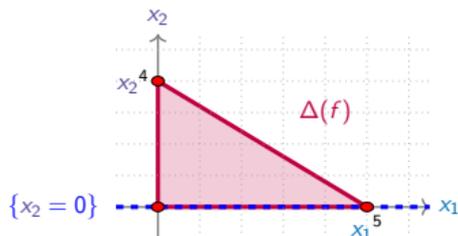
$$\nu(f) = \sum_{I \subseteq \{1, \dots, n\}} (-1)^{|I|} (n - |I|)! \text{Vol}_I \Delta(f),$$

where $\text{Vol}_I \Delta(f)$ is the volume of $\Delta(f) \cap_{i \in I} \{x_i = 0\}$

Example:

$$f(x_1, x_2) = 3 - x_1^2 + 5x_1x_2^2 + x_2^4 + 9x_1^5$$

$$\begin{aligned} \nu(f) &= (-1)^0 \cdot 2! \cdot \text{Vol}_{\Delta(f)} \\ &+ (-1)^1 \cdot 1! \cdot \text{Vol}_{\Delta(f) \cap \{x_1=0\}} \quad (I = \{1\}) \\ &+ (-1)^1 \cdot 1! \cdot \text{Vol}_{\Delta(f) \cap \{x_2=0\}} \quad (I = \{2\}) \\ &= 2 \times (5 \times 4)/2 - 4 - 5 \end{aligned}$$



Newton Number

Definition

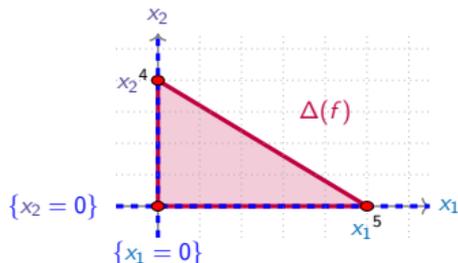
Let $f \in \mathbb{F}_q[x_1, \dots, x_n]$. The **Newton number** $\nu(f)$ of f is

$$\nu(f) = \sum_{I \subseteq \{1, \dots, n\}} (-1)^{|I|} (n - |I|)! \text{Vol}_I \Delta(f),$$

where $\text{Vol}_I \Delta(f)$ is the volume of $\Delta(f) \cap_{i \in I} \{x_i = 0\}$

Example:

$$f(x_1, x_2) = 3 - x_1^2 + 5x_1x_2^2 + x_2^4 + 9x_1^5$$



$$\begin{aligned} \nu(f) &= (-1)^0 \cdot 2! \cdot \text{Vol}_{\Delta(f)} \\ &+ (-1)^1 \cdot 1! \cdot \text{Vol}_{\Delta(f) \cap \{x_1=0\}} \quad (I = \{1\}) \\ &+ (-1)^1 \cdot 1! \cdot \text{Vol}_{\Delta(f) \cap \{x_2=0\}} \quad (I = \{2\}) \\ &+ (-1)^2 \cdot 0! \cdot \text{Vol}_{\Delta(f) \cap \{x_1=0\} \cap \{x_2=0\}} \quad (I = \{1, 2\}) \\ &= 2 \times (5 \times 4) / 2 - 4 - 5 + 1 \end{aligned}$$

Newton Number

Definition

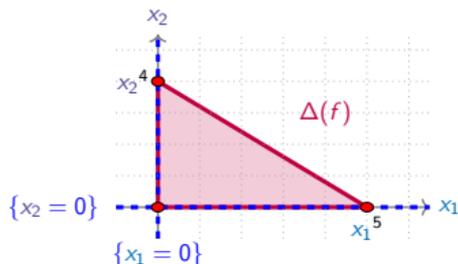
Let $f \in \mathbb{F}_q[x_1, \dots, x_n]$. The **Newton number** $\nu(f)$ of f is

$$\nu(f) = \sum_{I \subseteq \{1, \dots, n\}} (-1)^{|I|} (n - |I|)! \text{Vol}_I \Delta(f),$$

where $\text{Vol}_I \Delta(f)$ is the volume of $\Delta(f) \cap_{i \in I} \{x_i = 0\}$

Example:

$$f(x_1, x_2) = 3 - x_1^2 + 5x_1x_2^2 + x_2^4 + 9x_1^5$$



$$\begin{aligned} \nu(f) &= (-1)^0 \cdot 2! \cdot \text{Vol}_{\Delta(f)} \\ &+ (-1)^1 \cdot 1! \cdot \text{Vol}_{\Delta(f) \cap \{x_1=0\}} \quad (I = \{1\}) \\ &+ (-1)^1 \cdot 1! \cdot \text{Vol}_{\Delta(f) \cap \{x_2=0\}} \quad (I = \{2\}) \\ &+ (-1)^2 \cdot 0! \cdot \text{Vol}_{\Delta(f) \cap \{x_1=0\} \cap \{x_2=0\}} \quad (I = \{1, 2\}) \\ &= 2 \times (5 \times 4) / 2 - 4 - 5 + 1 \\ &= 12 \end{aligned}$$

Commode functions

Definition

A function f is **commode** if there exist nonzero d_1, d_2, \dots, d_n such that

$$(d_1, 0, 0, \dots, 0), (0, d_2, 0, \dots, 0), \dots, (0, 0, \dots, 0, d_n) \in \Delta(f)$$

Commode functions

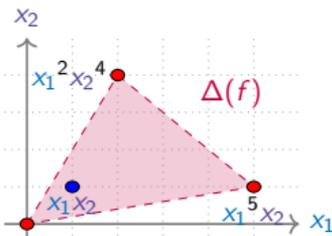
Definition

A function f is **commode** if there exist nonzero d_1, d_2, \dots, d_n such that

$$(d_1, 0, 0, \dots, 0), (0, d_2, 0, \dots, 0), \dots, (0, 0, \dots, 0, d_n) \in \Delta(f)$$

Examples:

$$f(x_1, x_2) = 1 + x_1 x_2 - 2x_1^2 x_2^4 + 3x_1^5 x_2$$



f is not **commode**

Commode functions

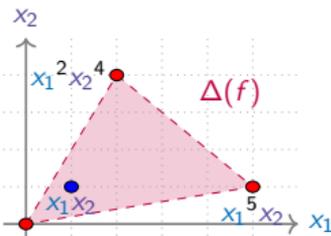
Definition

A function f is **commode** if there exist nonzero d_1, d_2, \dots, d_n such that

$$(d_1, 0, 0, \dots, 0), (0, d_2, 0, \dots, 0), \dots, (0, 0, \dots, 0, d_n) \in \Delta(f)$$

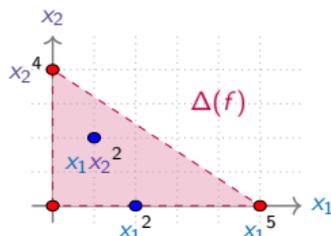
Examples:

$$f(x_1, x_2) = 1 + x_1x_2 - 2x_1^2x_2^4 + 3x_1^5x_2$$



f is not **commode**

$$f(x_1, x_2) = 3 - x_1^2 + 5x_1x_2^2 + x_2^4 + 9x_1^5$$



f is **commode**

Denef-Loeser Theorem

Definition

A function f is **non-degenerate** if for every face (not containing the origin) τ of $\Delta(f)$, the following system has no nonzero solutions

$$\partial f_{\tau} / \partial x_1 = \dots = \partial f_{\tau} / \partial x_n = 0$$

Denef-Loeser Theorem

Definition

A function f is **non-degenerate** if for every face (not containing the origin) τ of $\Delta(f)$, the following system has no nonzero solutions

$$\partial f_{\tau} / \partial x_1 = \dots = \partial f_{\tau} / \partial x_n = 0$$

Theorem [Denef and Loeser, 1991]

Let $f \in \mathbb{F}_q[x_1, \dots, x_n]$.

If f is **commode** and **non-degenerate** with respect to its **Newton polyhedron** $\Delta(f)$, then, we have

$$|S(f)| = \left| \sum_{x \in \mathbb{F}_q^n} \omega^{f(x)} \right| \leq \nu(f) \cdot q^{n/2} .$$

Denef-Loeser Theorem

Definition

A function f is **non-degenerate** if for every face (not containing the origin) τ of $\Delta(f)$, the following system has no nonzero solutions

$$\partial f_\tau / \partial x_1 = \dots = \partial f_\tau / \partial x_n = 0$$

Theorem [Denef and Loeser, 1991]

Let $f \in \mathbb{F}_q[x_1, \dots, x_n]$.

If f is **commod** and **non-degenerate** with respect to its **Newton polyhedron** $\Delta(f)$, then, we have

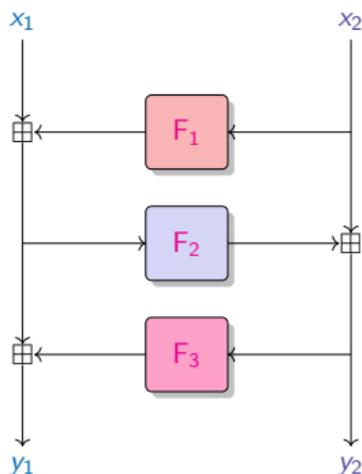
$$|S(f)| = \left| \sum_{x \in \mathbb{F}_q^n} \omega^{f(x)} \right| \leq \nu(f) \cdot q^{n/2}.$$

Linearity bound for $n = 2$: $\mathcal{L}_F \leq \nu(f) \cdot q$.

3-round Feistel - Definition

Let $\text{FEISTEL}[F_1, F_2, F_3]$ be a 3-round Feistel network with

$$d_1 = \deg(F_1), d_2 = \deg(F_2), \text{ and } d_3 = \deg(F_3).$$



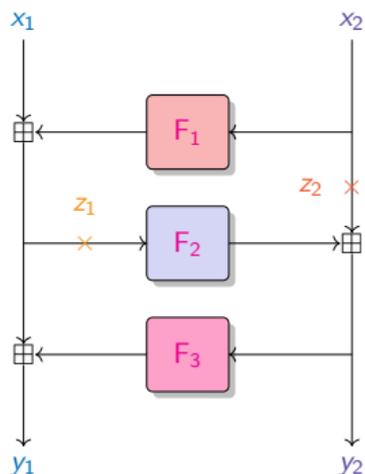
$$\begin{cases} y_1 &= x_1 + F_1(x_2) + F_3(x_2 + F_2(x_1 + F_1(x_2))) \\ y_2 &= x_2 + F_2(x_1 + F_1(x_2)). \end{cases}$$

A 3-round Feistel.

3-round Feistel - Definition

Let $\text{FEISTEL}[F_1, F_2, F_3]$ be a 3-round Feistel network with

$$d_1 = \deg(F_1), d_2 = \deg(F_2), \text{ and } d_3 = \deg(F_3).$$



A 3-round Feistel.

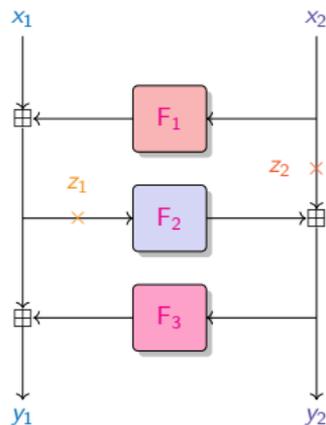
$$\begin{cases} y_1 &= x_1 + F_1(x_2) + F_3(x_2 + F_2(x_1 + F_1(x_2))) \\ y_2 &= x_2 + F_2(x_1 + F_1(x_2)). \end{cases}$$

New equations with intermediate variables

$$\begin{cases} x_1 &= z_1 - F_1(z_2) \\ x_2 &= z_2 \\ y_1 &= z_1 + F_3(z_2 + F_2(z_1)) \\ y_2 &= z_2 + F_2(z_1). \end{cases}$$

3-round Feistel - Bound

Let $F = \text{FEISTEL}[F_1, F_2, F_3]$, with round functions F_1, F_2 (permutation) and F_3 . Let $d_1 \geq d_3$.



$$\begin{cases} y_1 = z_1 + F_3(z_2 + F_2(z_1)) \\ y_2 = z_2 + F_2(z_1) . \end{cases}$$

Reminder

Linearity of $F : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$:

$$\mathcal{L}_F = \max_{u, v \in \mathbb{F}_q^n, v \neq 0} \left| \sum_{x \in \mathbb{F}_q^n} \omega(\langle v, F(x) \rangle - \langle u, x \rangle) \right| .$$

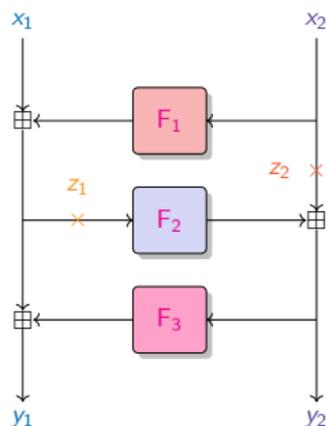
We denote:

$$S(f) = \sum_{x \in \mathbb{F}_q^n} \omega^{f(x)} .$$

3-round Feistel - Bound

Let $F = \text{FEISTEL}[F_1, F_2, F_3]$, with round functions F_1, F_2 (permutation) and F_3 . Let $d_1 \geq d_3$.

$$\begin{aligned}
 f(z_1, z_2) &= \langle (v_1, v_2), F(z_1, z_2) \rangle - \langle (u_1, u_2), (z_1, z_2) \rangle \\
 &= v_1 F_3(z_2 + F_2(z_1)) + v_2 F_2(z_1) + u_1 F_1(z_2) + (v_1 - u_1)z_1 + (v_2 - u_2)z_2 .
 \end{aligned}$$



$$\begin{cases}
 y_1 = z_1 + F_3(z_2 + F_2(z_1)) \\
 y_2 = z_2 + F_2(z_1) .
 \end{cases}$$

Reminder

Linearity of $F : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$:

$$\mathcal{L}_F = \max_{u, v \in \mathbb{F}_q^n, v \neq 0} \left| \sum_{x \in \mathbb{F}_q^n} \omega(\langle v, F(x) \rangle - \langle u, x \rangle) \right| .$$

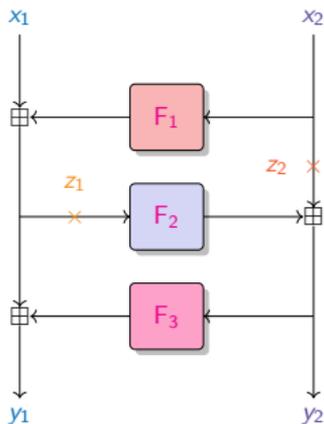
We denote:

$$S(f) = \sum_{x \in \mathbb{F}_q^n} \omega^{f(x)} .$$

3-round Feistel - Bound

Let $F = \text{FEISTEL}[F_1, F_2, F_3]$, with round functions F_1, F_2 (permutation) and F_3 . Let $d_1 \geq d_3$.

$$\begin{aligned}
 f(z_1, z_2) &= \langle (v_1, v_2), F(z_1, z_2) \rangle - \langle (u_1, u_2), (z_1, z_2) \rangle \\
 &= v_1 F_3(z_2 + F_2(z_1)) + v_2 F_2(z_1) + u_1 F_1(z_2) + (v_1 - u_1)z_1 + (v_2 - u_2)z_2 .
 \end{aligned}$$

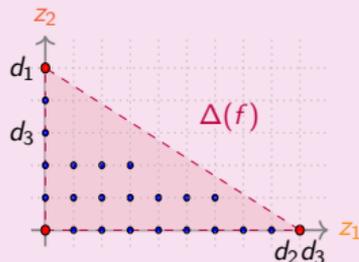


$$\begin{cases}
 y_1 = z_1 + F_3(z_2 + F_2(z_1)) \\
 y_2 = z_2 + F_2(z_1) .
 \end{cases}$$

Linearity Bound

- ★ f is commode
- ★ f is non-degenerate
- ★ its Newton number is

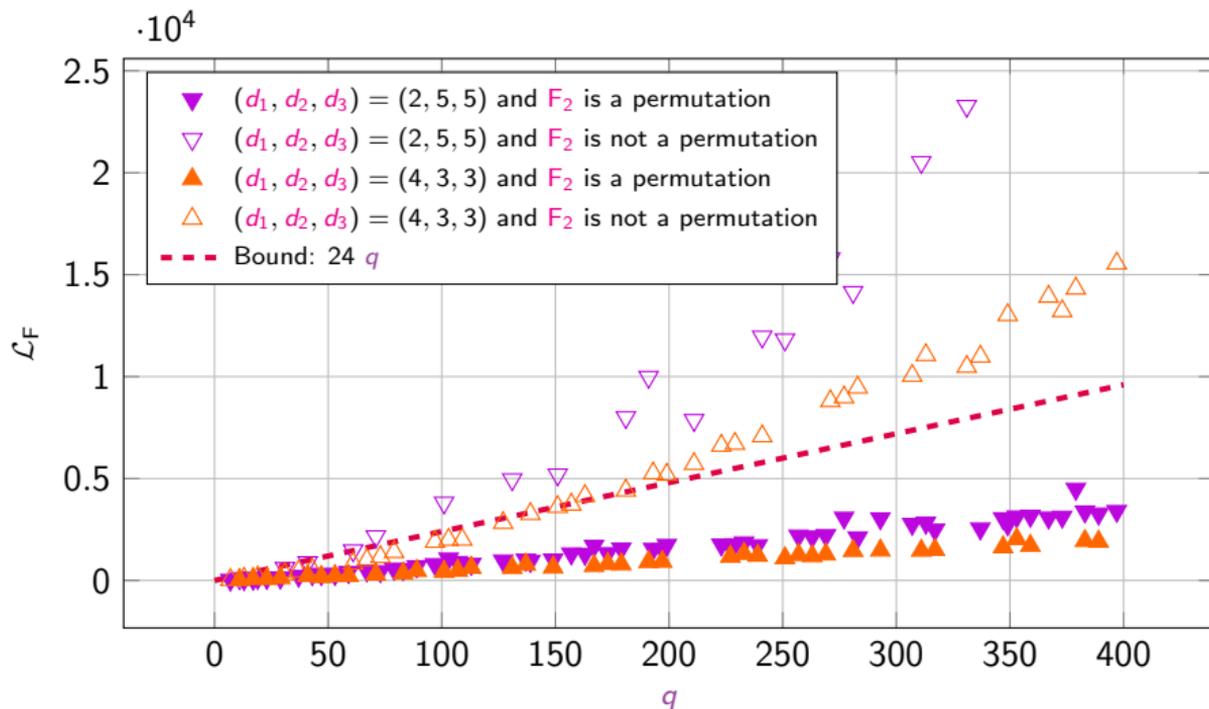
$$\nu(f) = (d_2 d_3 - 1)(d_1 - 1) .$$



$$\mathcal{L}_F \leq (d_1 - 1)(d_2 d_3 - 1) \cdot q$$

3-round Feistel - Results

Let $F = \text{FEISTEL}[F_1, F_2, F_3]$ with F_1 , F_2 and F_3 monomial functions.



Generalizations of Weil bound

- ★ Deligne bound
 - ★ Application to the Generalized Butterfly construction
- ★ Denef and Loeser bound
 - ★ Application to 3-round Feistel construction
- ★ **Rojas-León** bound
 - ★ Application to the **Generalized Flystel** construction

Isolated singularities

Definition

- ★ A singular point of a hypersurface is **isolated** if there exists a Zariski neighborhood of the point that contains no other singular points.
- ★ A polynomial g is **quasi-homogeneous** of degree δ if there exists w_1, \dots, w_n s.t.

$$g(\lambda^{w_1}x_1, \dots, \lambda^{w_n}x_n) = \lambda^\delta g(x_1, \dots, x_n) .$$

- ★ The **Milnor number** of the singularity is equal to $\prod_{i=1}^n (\delta/w_i - 1)$

Isolated singularities

Definition

- ★ A singular point of a hypersurface is **isolated** if there exists a Zariski neighborhood of the point that contains no other singular points.
- ★ A polynomial g is **quasi-homogeneous** of degree δ if there exists w_1, \dots, w_n s.t.

$$g(\lambda^{w_1} x_1, \dots, \lambda^{w_n} x_n) = \lambda^\delta g(x_1, \dots, x_n) .$$

- ★ The **Milnor number** of the singularity is equal to $\prod_{i=1}^n (\delta/w_i - 1)$

Example: Let $f(x) = (x - 1)^d$.

- ★ $x = 1$ is the **only singular point** of $f = 0$.
- ★ Up to translation, we can consider the singularity in the origin: $g(x) = x^d$.

$$g(\lambda^w x) = (\lambda^w x)^d = \lambda^{w \cdot d} x^d = \lambda^{w \cdot d} g(x) \quad \text{so that } \delta = w \cdot d$$

- ★ **Milnor number** of the singularity: $\delta/w - 1 = d - 1$.

Rojas-León Theorem

Theorem [Rojas-León, 2006]

Let $f \in \mathbb{F}_q[x_1, \dots, x_n]$, s.t. $\deg(f) = d$.

Suppose that $f = f_d + f_{d'} + \dots$, where $f_d, f_{d'}$, are resp. **the degree- d , degree- d' , homogeneous component** of f , with $\gcd(d, p) = \gcd(d', p) = 1$ and $d'/d > p/(p + (p - 1)^2)$.

If the following conditions are satisfied

- ★ the hypersurface defined by $f_d = 0$ has at worst **quasi-homogeneous isolated singularities** of degrees prime to p with **Milnor numbers** μ_1, \dots, μ_s ,
- ★ the hypersurface defined by $f_{d'} = 0$ contains none of these singularities,

then we have

$$|S(f)| = \left| \sum_{x \in \mathbb{F}_q^n} \omega^{f(x)} \right| \leq \left((d-1)^n - (d-d') \sum_{i=1}^s \mu_i \right) \cdot q^{n/2}.$$

Rojas-León Theorem

Theorem [Rojas-León, 2006]

Let $f \in \mathbb{F}_q[x_1, \dots, x_n]$, s.t. $\deg(f) = d$.

Suppose that $f = f_d + f_{d'} + \dots$, where $f_d, f_{d'}$, are resp. **the degree- d , degree- d' , homogeneous component** of f , with $\gcd(d, p) = \gcd(d', p) = 1$ and $d'/d > p/(p + (p - 1)^2)$.

If the following conditions are satisfied

- ★ the hypersurface defined by $f_d = 0$ has at worst **quasi-homogeneous isolated singularities** of degrees prime to p with **Milnor numbers** μ_1, \dots, μ_s ,
- ★ the hypersurface defined by $f_{d'} = 0$ contains none of these singularities,

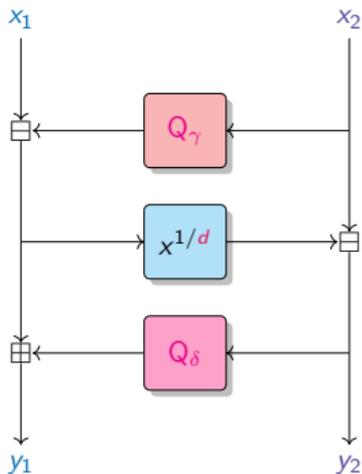
then we have

$$|S(f)| = \left| \sum_{x \in \mathbb{F}_q^n} \omega^{f(x)} \right| \leq \left((d-1)^n - (d-d') \sum_{i=1}^s \mu_i \right) \cdot q^{n/2}.$$

$$\text{Linearity bound for } n = 2: \mathcal{L}_F \leq ((d-1)^2 - (d-d') \sum_{i=1}^s \mu_i) \cdot q.$$

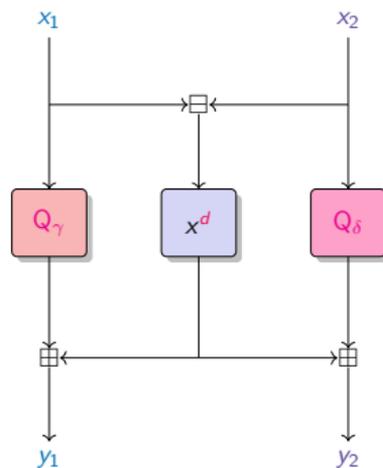
Flystel - Definition

Introduced by [Bouvier, Briaud, Chaidos, Perrin, Salen, Velichkov and Willems, 2023].



Open variant.

$$\begin{cases} y_1 &= x_1 - Q_\gamma(x_2) + Q_\delta(x_2 - (x_1 - Q_\gamma(x_2))^{1/d}) \\ y_2 &= x_2 - (x_1 - Q_\gamma(x_2))^{1/d}. \end{cases}$$

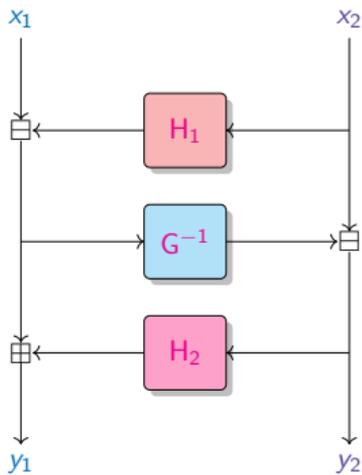


Closed variant.

$$\begin{cases} y_1 &= (x_1 - x_2)^d + Q_\gamma(x_1) \\ y_2 &= (x_1 - x_2)^d + Q_\delta(x_2). \end{cases}$$

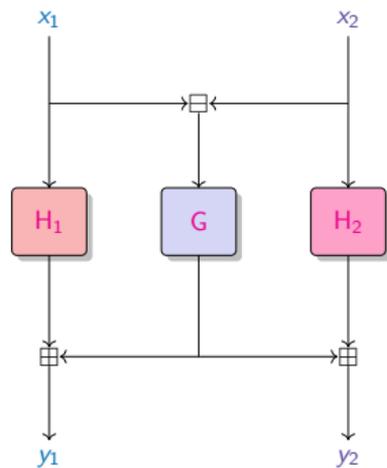
Generalized Flystel - Definition

$F = \text{FLYSTEL}[H_1, G, H_2]$, with $G : \mathbb{F}_q \rightarrow \mathbb{F}_q$ a permutation, and $H_1, H_2 : \mathbb{F}_q \rightarrow \mathbb{F}_q$ functions.



Open variant.

$$\begin{cases} y_1 &= x_1 - H_1(x_2) + H_2(x_2 - G^{-1}(x_1 - H_1(x_2))) \\ y_2 &= x_2 - G^{-1}(x_1 - H_1(x_2)). \end{cases}$$

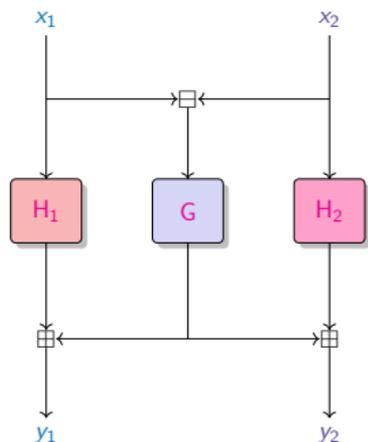


Closed variant.

$$\begin{cases} y_1 &= G(x_1 - x_2) + H_1(x_1) \\ y_2 &= G(x_1 - x_2) + H_2(x_2). \end{cases}$$

Generalized Flystel - Bound

Let $F = \text{FLYSTEL}[H_1, G, H_2]$, with G a permutation, H_1, H_2 functions ($\deg G > \deg H_1, \deg H_2$).



$$\begin{cases} y_1 = G(x_1 - x_2) + H_1(x_1) \\ y_2 = G(x_1 - x_2) + H_2(x_2). \end{cases}$$

Reminder

Linearity of $F : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$:

$$\mathcal{L}_F = \max_{u, v \in \mathbb{F}_q^n, v \neq 0} \left| \sum_{x \in \mathbb{F}_q^n} \omega(\langle v, F(x) \rangle - \langle u, x \rangle) \right|.$$

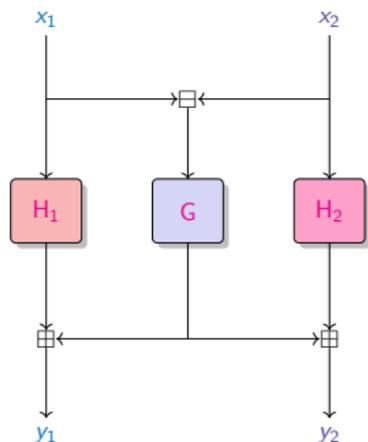
We denote:

$$S(f) = \sum_{x \in \mathbb{F}_q^n} \omega^{f(x)}.$$

Generalized Flystel - Bound

Let $F = \text{FLYSTEL}[H_1, G, H_2]$, with G a permutation, H_1, H_2 functions ($\deg G > \deg H_1, \deg H_2$).

$$\begin{aligned} f(x_1, x_2) &= \langle (v_1, v_2), F(x_1, x_2) \rangle - \langle (u_1, u_2), (x_1, x_2) \rangle \\ &= (v_1 + v_2)G(x_1 - x_2) + v_1H_1(x_1) + v_2H_2(x_2) - u_1x_1 - u_2x_2. \end{aligned}$$



$$\begin{cases} y_1 = G(x_1 - x_2) + H_1(x_1) \\ y_2 = G(x_1 - x_2) + H_2(x_2). \end{cases}$$

Reminder

Linearity of $F : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$:

$$\mathcal{L}_F = \max_{u, v \in \mathbb{F}_q^n, v \neq 0} \left| \sum_{x \in \mathbb{F}_q^n} \omega^{\langle (v, F(x)) - \langle u, x \rangle \rangle} \right|.$$

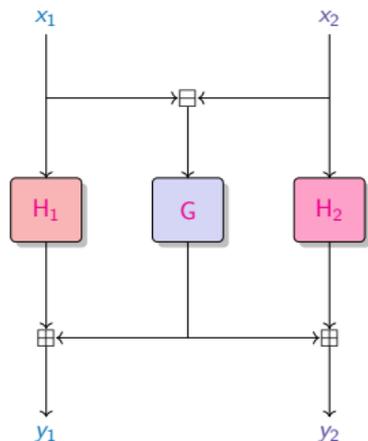
We denote:

$$S(f) = \sum_{x \in \mathbb{F}_q^n} \omega^{f(x)}.$$

Generalized Flystel - Bound

Let $F = \text{FLYSTEL}[H_1, G, H_2]$, with G a permutation, H_1, H_2 functions ($\deg G > \deg H_1, \deg H_2$).

$$\begin{aligned} f(x_1, x_2) &= \langle (v_1, v_2), F(x_1, x_2) \rangle - \langle (u_1, u_2), (x_1, x_2) \rangle \\ &= (v_1 + v_2)G(x_1 - x_2) + v_1H_1(x_1) + v_2H_2(x_2) - u_1x_1 - u_2x_2. \end{aligned}$$



$$\begin{cases} y_1 = G(x_1 - x_2) + H_1(x_1) \\ y_2 = G(x_1 - x_2) + H_2(x_2). \end{cases}$$

Linearity Bound

- ★ The hypersurface

$$f_d = (v_1 + v_2)(x_1 - x_2)^d = 0$$

contains one singular point $[1 : 1]$ of quasi-homogeneous type with Milnor number $d - 1$.

- ★ The hypersurface

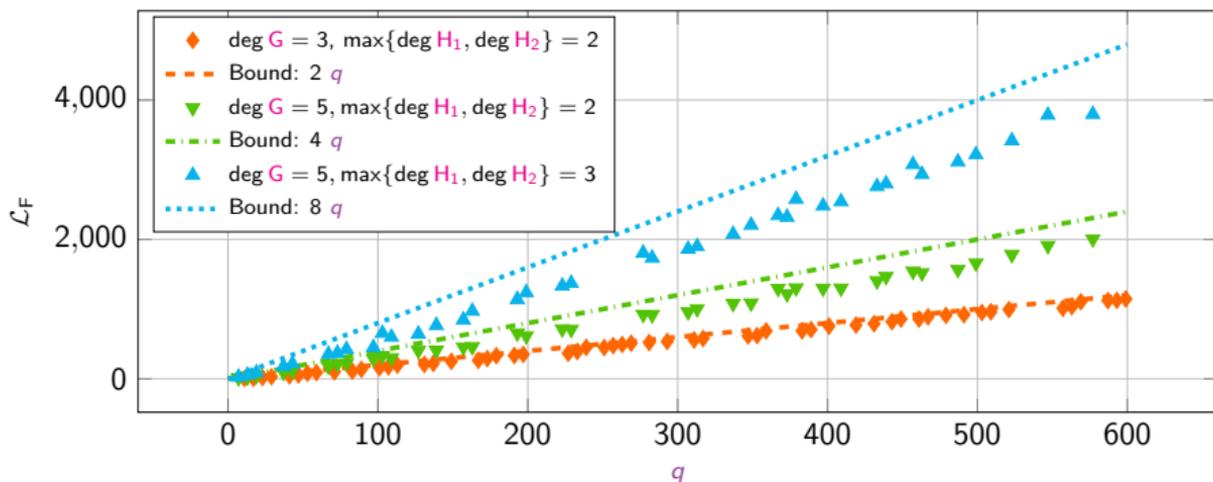
$$f_{d'} = v_i x_i^{\deg H_i} = 0$$

does not contain this point.

$$\mathcal{L}_F \leq (\deg G - 1)(\max\{\deg H_1, \deg H_2\} - 1) \cdot q$$

Generalized Flystel - Results

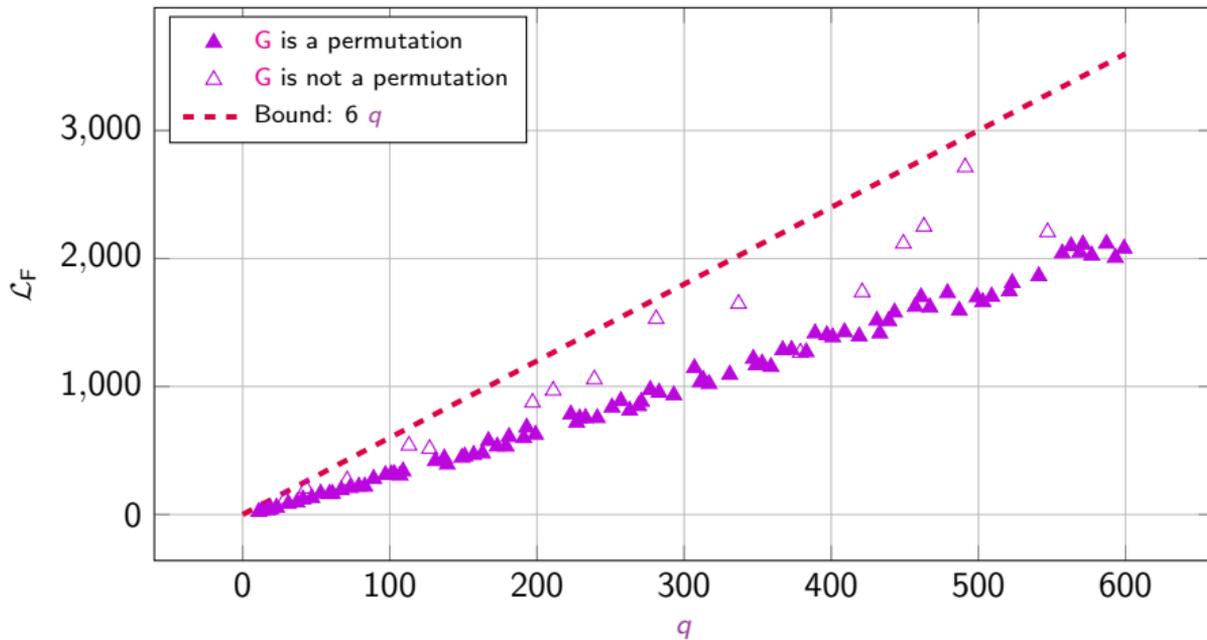
Let $F = \text{FLYSTEL}[H_1, G, H_2]$ with H_1 , G and H_2 monomials.



Low-degree permutations G , H_1 and H_2 .

Generalized Flystel - Results

Let $F = \text{FLYSTEL}[H_1, G, H_2]$ with H_1 , G and H_2 monomials.



$\text{deg } G = 7$ and $\text{deg } H_1 = \text{deg } H_2 = 2$.

Solving conjecture

Conjecture

Let $F = \text{FLYSTEEL}[H_1, G, H_2]$ be defined by $H_1(x) = \gamma + \beta x^2$, $G(x) = x^d$ and $H_2 = \delta + \beta x^2$, with $\gamma, \delta \in \mathbb{F}_p$ and $\beta \in \mathbb{F}_p^\times$. Then

$$\mathcal{L}_F \leq p \log p .$$

Solving conjecture

Conjecture

Let $F = \text{FLYSTEEL}[H_1, G, H_2]$ be defined by $H_1(x) = \gamma + \beta x^2$, $G(x) = x^d$ and $H_2 = \delta + \beta x^2$, with $\gamma, \delta \in \mathbb{F}_p$ and $\beta \in \mathbb{F}_p^\times$. Then

$$\mathcal{L}_F \leq p \log p .$$

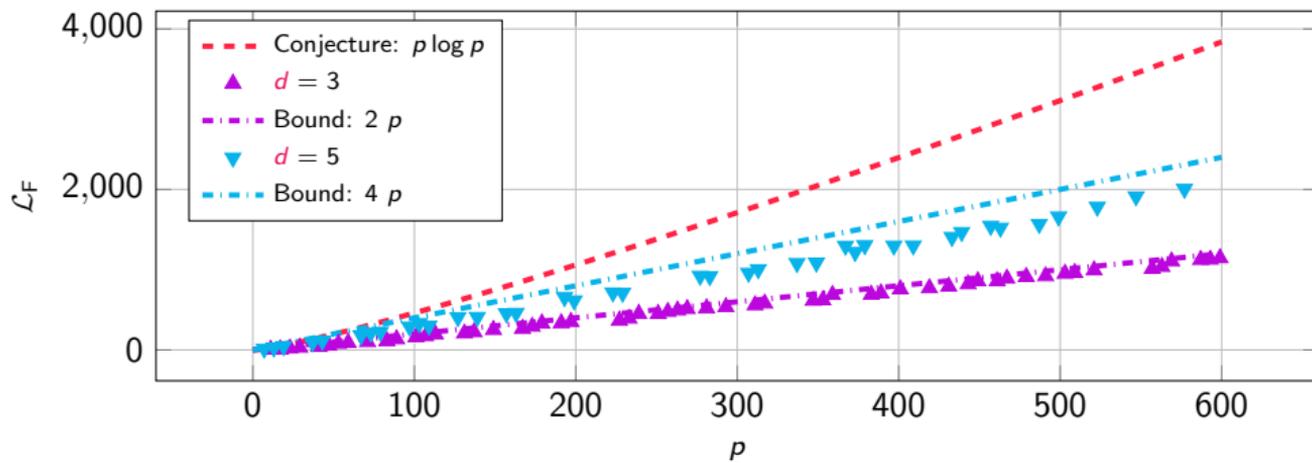
Conjecture proved for $d \leq \log p$

Proposition

Let $F = \text{FLYSTEEL}[H_1, G, H_2]$ be defined by $H_1(x) = \gamma + \beta x^2$, $G(x) = x^d$ and $H_2 = \delta + \beta x^2$, with $\gamma, \delta \in \mathbb{F}_p$ and $\beta \in \mathbb{F}_p^\times$. Then

$$\mathcal{L}_F \leq (d - 1)p .$$

Solving conjecture



Conclusions

- ★ **Bounds on exponential sums** have direct application to linear cryptanalysis
 - ★ Deligne, 1974
 - ★ Denef and Loeser, 1991
 - ★ Rojas-León, 2006

Conclusions

- ★ **Bounds on exponential sums** have direct application to linear cryptanalysis
 - ★ Deligne, 1974 Generalization of the **Butterfly** construction
 - ★ Denef and Loeser, 1991 3-round **Feistel** network
 - ★ Rojas-León, 2006 Generalization of the **Flystel** construction

$$F \in \mathbb{F}_q[x_1, x_2], \exists C \in \mathbb{F}_q, \mathcal{L}_F \leq C \times q$$

Conclusions

- ★ **Bounds on exponential sums** have direct application to linear cryptanalysis
 - ★ **Deligne, 1974** Generalization of the **Butterfly** construction
 - ★ **Denef and Loeser, 1991** 3-round **Feistel** network
 - ★ **Rojas-León, 2006** Generalization of the **Flystel** construction

$$F \in \mathbb{F}_q[x_1, x_2], \exists C \in \mathbb{F}_q, \mathcal{L}_F \leq C \times q$$

- ★ **Solving conjecture** on the linearity of the Flystel construction in Anemoi

Conclusions

- ★ **Bounds on exponential sums** have direct application to linear cryptanalysis
 - ★ **Deligne, 1974** Generalization of the **Butterfly** construction
 - ★ **Denef and Loeser, 1991** 3-round **Feistel** network
 - ★ **Rojas-León, 2006** Generalization of the **Flystel** construction

$$F \in \mathbb{F}_q[x_1, x_2], \exists C \in \mathbb{F}_q, \mathcal{L}_F \leq C \times q$$

- ★ **Solving conjecture** on the linearity of the Flystel construction in Anemoi

Contribute to the cryptanalysis efforts for AOP.

Cohomological framework

$$S(f) = \sum_{x \in \mathbb{F}_q^n} \omega(\langle v, F(x) \rangle - \langle u, x \rangle)$$

Cohomological framework

$$S(f) = \sum_{x \in \mathbb{F}_q^n} \omega(\langle v, F(x) \rangle - \langle u, x \rangle)$$



Cohomological framework



$$|S(f)| = \left| \sum_{i=0}^{2n} (-1)^i \text{Tr}(F \mid H_c^i(\mathbb{A}^n, \mathcal{L})) \right|$$

Sum of **traces** of the **Frobenius automorphism** on ℓ -adic cohomology groups.

Cohomological framework

$$S(f) = \sum_{x \in \mathbb{F}_q^n} \omega(\langle v, F(x) \rangle - \langle u, x \rangle)$$



Cohomological framework



$$|S(f)| = \left| \sum_{i=0}^{2n} (-1)^i \text{Tr}(F \mid H_c^i(\mathbb{A}^n, \mathcal{L})) \right|$$

Sum of **traces** of the **Frobenius automorphism** on ℓ -adic cohomology groups.

Sum of **traces** of a **linear map** on a vector space of finite dimension.

Cohomological framework

$$S(f) = \sum_{x \in \mathbb{F}_q^n} \omega(\langle v, F(x) \rangle - \langle u, x \rangle)$$



Cohomological framework



$$|S(f)| = \left| \sum_{i=0}^{2n} (-1)^i \text{Tr}(F \mid H_c^i(\mathbb{A}^n, \mathcal{L})) \right|$$

Sum of **traces** of the **Frobenius automorphism** on ℓ -adic cohomology groups.

Sum of **traces** of a **linear map** on a vector space of finite dimension.

$$|S(f)| \leq \kappa \sum_{i=0}^{2n} \dim H_c^i(\mathbb{A}^n, \mathcal{L})$$

Perspectives

Can we provide **detailed calculations of the cohomological spaces** to refine bounds?

$$|S(f)| \leq \kappa \sum_{i=0}^{2n} \dim H_c^i(\mathbb{A}^n, \mathcal{L})$$

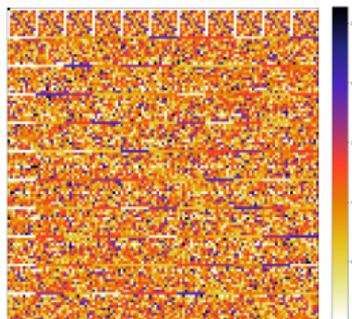
(on-going work with Christophe Levrat)

Perspectives

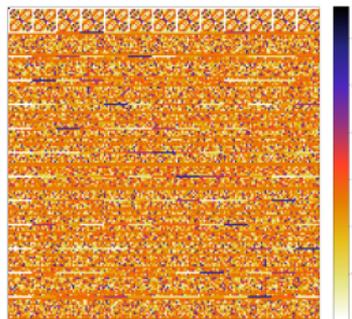
Can we provide **detailed calculations of the cohomological spaces** to refine bounds?

$$|S(f)| \leq \kappa \sum_{i=0}^{2n} \dim H_c^i(\mathbb{A}^n, \mathcal{L})$$

(on-going work with Christophe Levrat)



Closed Butterfly ($q = 11$)



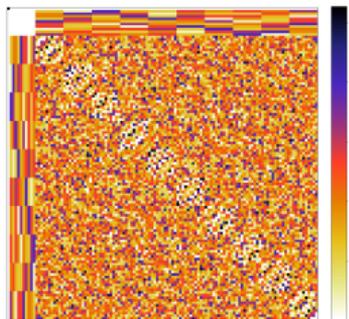
Closed Butterfly ($q = 13$)

Perspectives

Can we provide **detailed calculations of the cohomological spaces** to refine bounds?

$$|S(f)| \leq \kappa \sum_{i=0}^{2n} \dim H_c^i(\mathbb{A}^n, \mathcal{L})$$

(on-going work with Christophe Levrat)



Open Butterfly ($q = 11$)



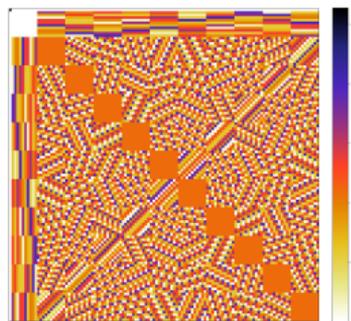
Open Butterfly ($q = 13$)

Perspectives

Can we provide **detailed calculations of the cohomological spaces** to refine bounds?

$$|S(f)| \leq \kappa \sum_{i=0}^{2n} \dim H_c^i(\mathbb{A}^n, \mathcal{L})$$

(on-going work with Christophe Levrat)



Open Flystel (q = 11)



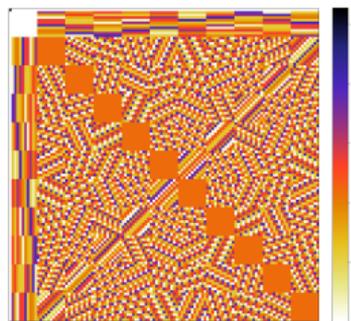
Open Flystel (q = 13)

Perspectives

Can we provide **detailed calculations of the cohomological spaces** to refine bounds?

$$|S(f)| \leq \kappa \sum_{i=0}^{2n} \dim H_c^i(\mathbb{A}^n, \mathcal{L})$$

(on-going work with Christophe Levrat)



Open Flystel ($q = 11$)



Open Flystel ($q = 13$)

Thank you

