Some Applications of Algebraic Geometry to Linear Cryptanalysis

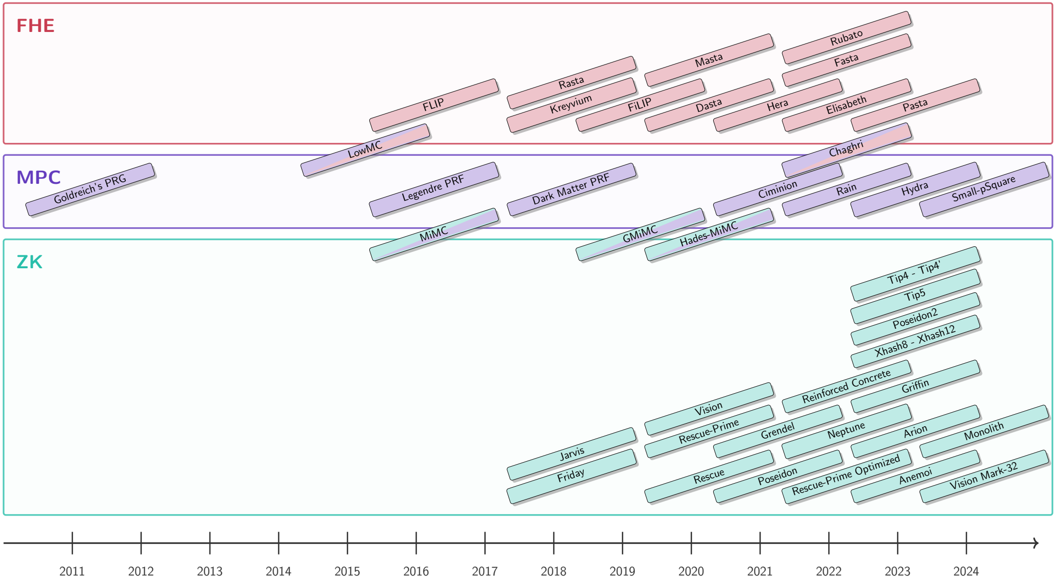
Clémence Bouvier

Université de Lorraine, CNRS, Inria, LORIA

(joint work with Tim Beyne)

Séminaire C2, Nancy, France
January 17th, 2025

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

≤ 8 years of cryptanalysis

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

Characters

Definition

A **character** of a finite abelian group G is a homomorphism

$$\chi : G \to \mathbb{C}^{\times} ,$$

where $\mathbb{C}^{\times}$ is the multiplicative group of nonzero complex numbers.

In particular, we have

$$\chi(1) = 1 ,$$

and for $a_1, a_2 \in G$

$$\chi(a_1 a_2) = \chi(a_1)\chi(a_2) .$$

$\chi(a)$ is a root of unity

Characters

Definition

A **character** of a finite abelian group G is a homomorphism

$$\chi : G \to \mathbb{C}^\times ,$$

where $\mathbb{C}^\times$ is the multiplicative group of nonzero complex numbers.

In particular, we have

$$\chi(1) = 1 ,$$

and for $a_1, a_2 \in G$

$$\chi(a_1 a_2) = \chi(a_1)\chi(a_2) .$$

$\chi(a)$ is a root of unity

Definition

A **linear approximation** of $\mathsf{F} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ is a pair of characters (χ, ψ).

Correlation of linear approximations

Definition

The **correlation of the linear approximation** (χ, ψ) of $F : \mathbb{F}_q^n \to \mathbb{F}_q^m$ is

$$C^F_{\chi,\psi} = \frac{1}{q^n} \sum_{x \in \mathbb{F}_q^n} \chi(F(x))\, \psi(-x)\ .$$

Let ω be a primitive character, $\mathbb{F}_q \to \mathbb{C}^\times$ s.t. $\chi(F(x)) = \omega^{\langle v, F(x)\rangle}$ and $\psi(x) = \omega^{\langle u, x\rangle}$. Then

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

Correlation of linear approximations

Definition

The **correlation of the linear approximation** (χ, ψ) of $F : \mathbb{F}_q^n \to \mathbb{F}_q^m$ is

$$C^F_{\chi,\psi} = \frac{1}{q^n} \sum_{x \in \mathbb{F}_q^n} \chi(F(x))\, \psi(-x)\ .$$

Let ω be a primitive character, $\mathbb{F}_q \to \mathbb{C}^\times$ s.t. $\chi(F(x)) = \omega^{\langle v, F(x)\rangle}$ and $\psi(x) = \omega^{\langle u, x\rangle}$. Then

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

Examples:

- If $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, then
$$C^F_{u,v} = \frac{1}{2^n} \sum_{x \in \mathbb{F}_2^n} (-1)^{(\langle v, F(x)\rangle + \langle u, x\rangle)}\ .$$
- If $F : \mathbb{F}_p^n \to \mathbb{F}_p^m$, then
$$C^F_{u,v} = \frac{1}{p^n} \sum_{x \in \mathbb{F}_p^n} e^{\left(\frac{2i\pi}{p}\right)(\langle v, F(x)\rangle - \langle u, x\rangle)}\ .$$

Walsh transform

Definition

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

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

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

Walsh transform

Definition

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

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

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

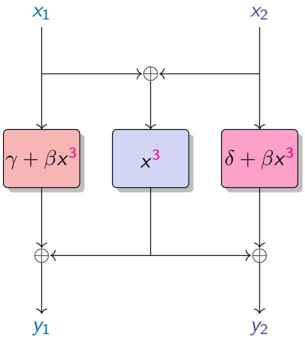
Definition

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

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

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

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



Closed Flystel.

Bounds

- Correlation bound

$$|C^{\mathsf{F}}_{u,v}| \leq 1/2^{n-1}$$

- Walsh transform bound

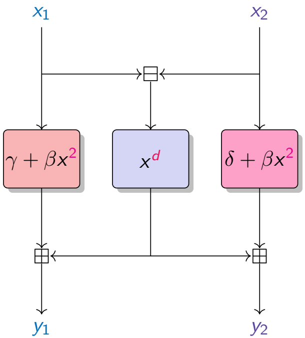
$$|\mathcal{W}^{\mathsf{F}}_{u,v}| \leq 2^{n+1}$$

- Linearity bound

$$\mathcal{L}_{\mathsf{F}} \leq 2^{n+1}$$

Closed Flystel in $\mathbb{F}_p$

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



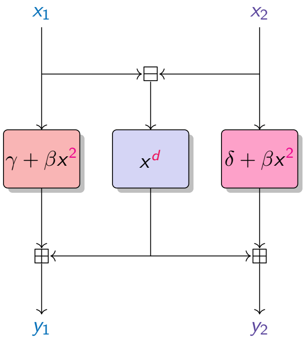
Closed Flystel.

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

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

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 $d = 3, 5$).

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

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

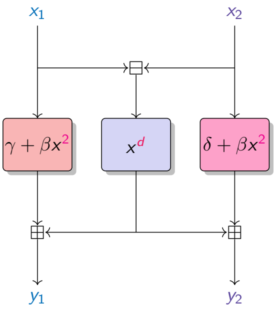
$$\mathcal{L}_f \leq (d-1)\sqrt{p}$$

Weil bound

Proposition [Weil, 1948]

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

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



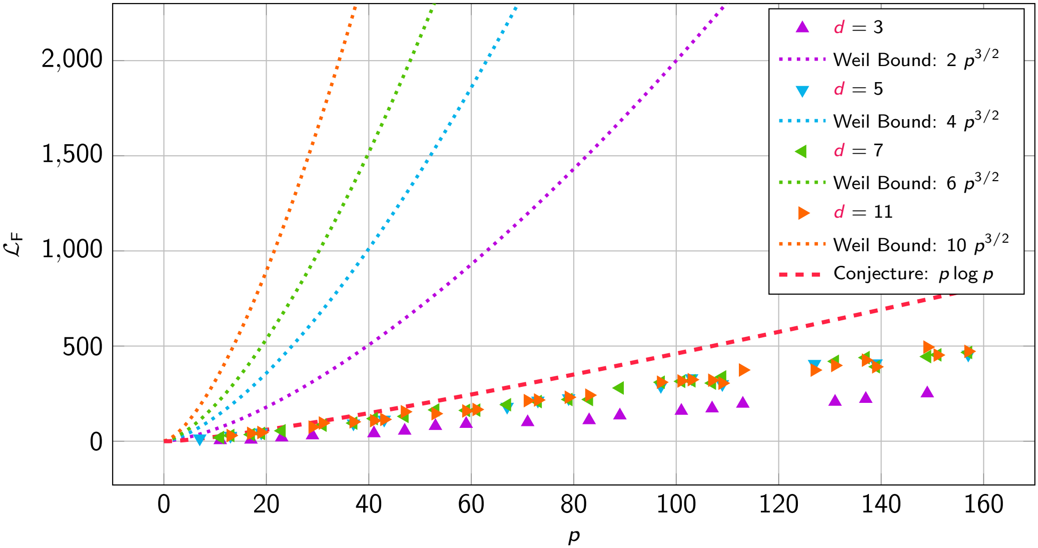
Closed Flystel.

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

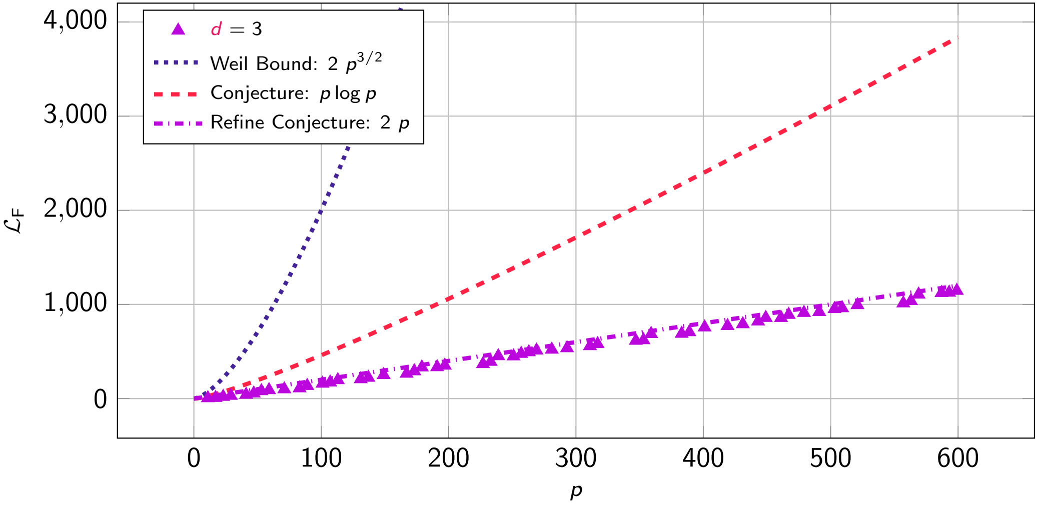
Conjecture

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

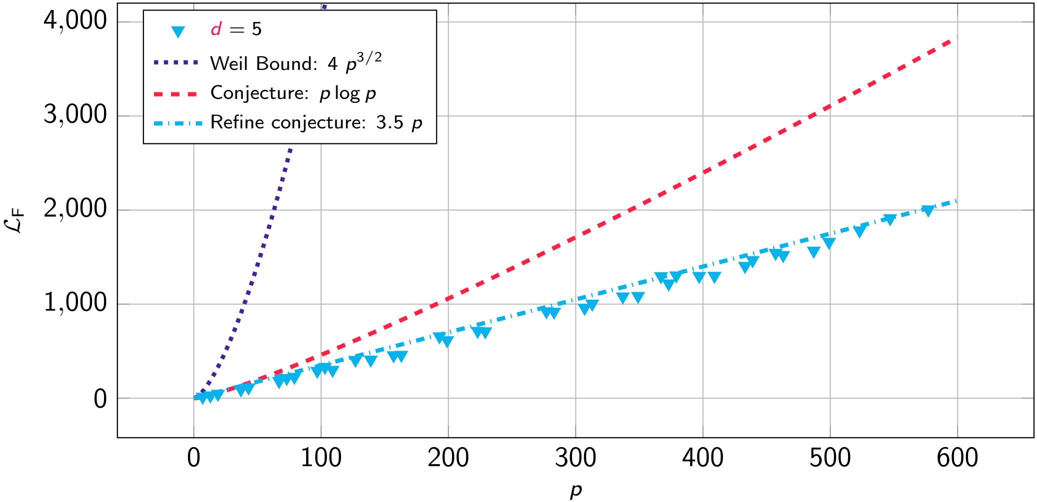
Experimental results



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:

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

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

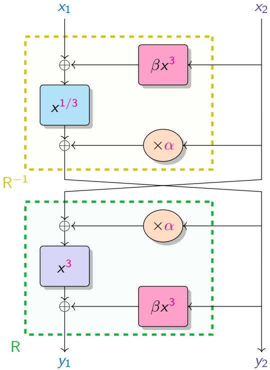
- ⋆ $\mathbb{F}_q$ is a finite field s.t. q is a power of a prime p.
- ⋆ Functions with 2 variables $\mathsf{F} \in \mathbb{F}_q[x_1, x_2]$.

Generalizations of Weil bound

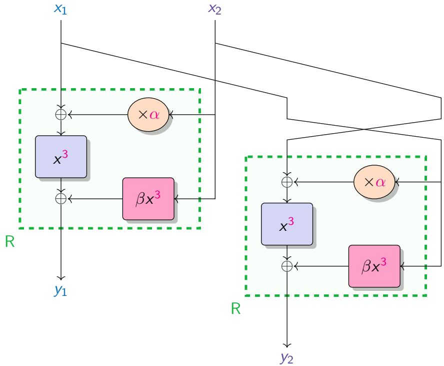
- ⋆ Deligne bound
  - ⋆ Application to the Generalized Butterfly construction
- ⋆ Denef and Loeser bound
  - ⋆ Application to 3-round Feistel construction
- ⋆ Rojas-León bound
  - ⋆ Application to the Generalized Flystel construction

Butterfly - Definition

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



Open variant.



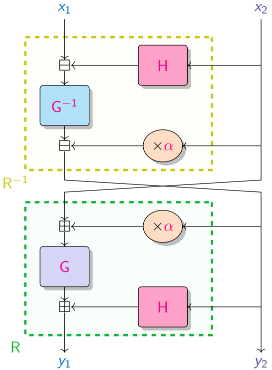
Closed variant.

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

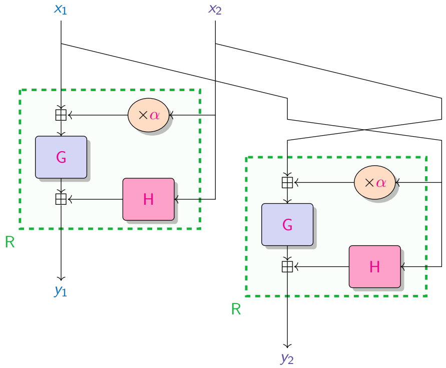
$$\begin{cases} y_1 &= (x_1 + \alpha x_2)^3 + (\beta x_2)^3 \\ y_2 &= (x_2 + \alpha x_1)^3 + (\beta x_1)^3 \,. \end{cases}$$

Generalized Butterfly - Definition

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



Open variant.



Closed variant.

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

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

Smoothness

Definition

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

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

has no non zero solutions.

Smoothness

Definition

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

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

has no non zero solutions.

Examples:

- $f(x_1, x_2) = 2{x_1}^3 + {x_2}^2 = 0$ is smooth, since

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

  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

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

has no non zero solutions.

Examples:

- ⋆ $f(x_1, x_2) = 2{x_1}^3 + {x_2}^2 = 0$ is smooth, since

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

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 $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ be a polynomial of degree d, with $\gcd(d, p) = 1$.
Let f_d be the **degree d homogeneous component** of f, i.e.

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

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 $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ be a polynomial of degree d, with $\gcd(d, p) = 1$.
Let f_d be the **degree d homogeneous component** of f, i.e.

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

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

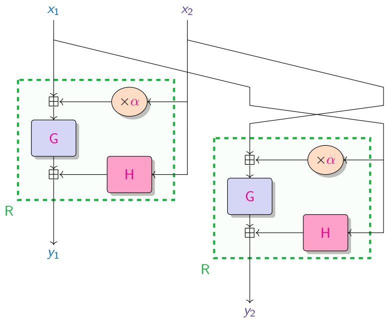
$$|S(f)| = \left| \sum_{x \in \mathbb{F}_q^n} \omega^{f(x)} \right| \leq (d-1)^n \cdot q^{n/2} \ .$$

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

Generalized Butterfly - Bound

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

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

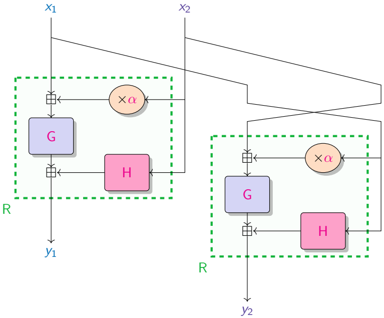


$$\begin{cases} y_1 &= \mathsf{G}(x_1 + \alpha x_2) + \mathsf{H}(x_2) \\ y_2 &= \mathsf{G}(x_2 + \alpha x_1) + \mathsf{H}(x_1) \, . \end{cases}$$

Generalized Butterfly - Bound

Let $F = \textsc{Butterfly}[G, H, \alpha]$, 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.

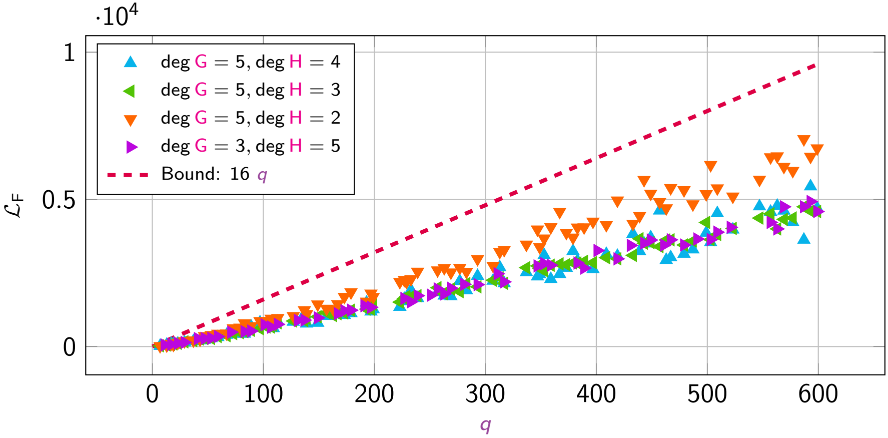
- If $d = \deg H > \deg G > 1$, then

  $f_d = {x_1}^d + v_1/v_2 {x_2}^d = 0$ is smooth.

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

Generalized Butterfly - Results

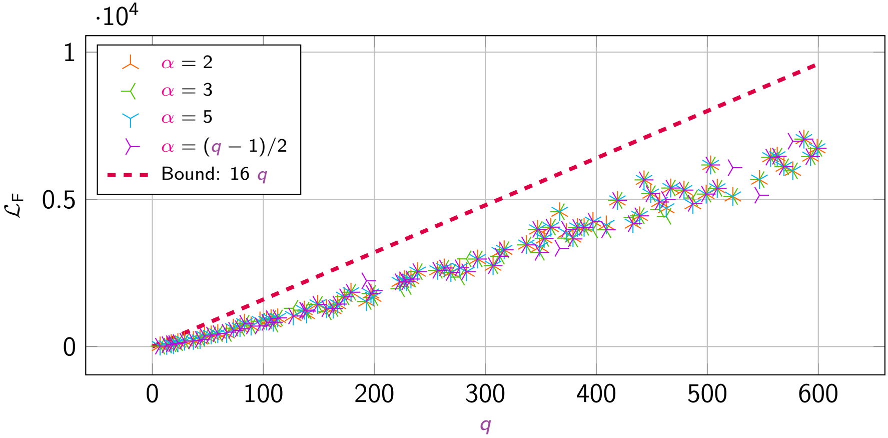
Let $\mathsf{F} = \textsc{Butterfly}[\mathsf{G}, \mathsf{H}, \alpha]$ with G and H monomial functions.



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

Generalized Butterfly - Results

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



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

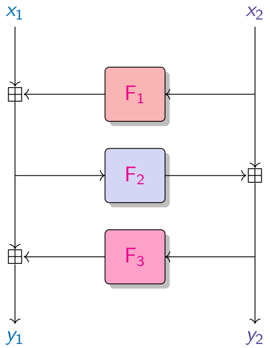
Generalizations of Weil bound

- ⋆ 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

3-round Feistel - Definition

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

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



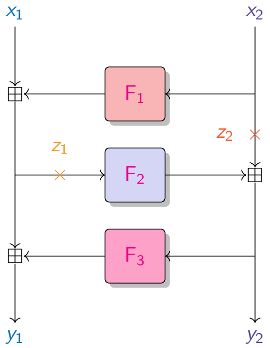
A 3-round Feistel.

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

3-round Feistel - Definition

Let $\textsc{Feistel}[F_1, F_2, F_3]$ 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

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

Newton Polyhedron

Definition

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

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

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

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

Newton Polyhedron

Definition

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

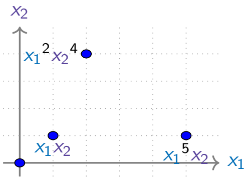
$$f(x_1, \ldots, x_n) = \sum_{e_1,\ldots,e_n} c_{e_1,\ldots,e_n} \prod_{i=1}^{n} x_i^{e_i} .$$

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

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

Examples:

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



Newton Polyhedron

Definition

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

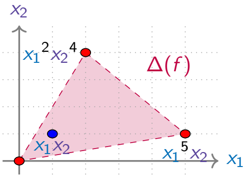
$$f(x_1, \ldots, x_n) = \sum_{e_1, \ldots, e_n} c_{e_1, \ldots, e_n} \prod_{i=1}^n x_i^{e_i} \ .$$

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

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

Examples:

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



Newton Polyhedron

Definition

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

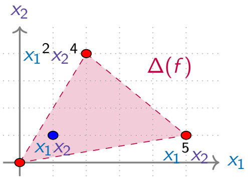
$$f(x_1, \ldots, x_n) = \sum_{e_1, \ldots, e_n} c_{e_1, \ldots, e_n} \prod_{i=1}^{n} x_i^{e_i} \ .$$

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

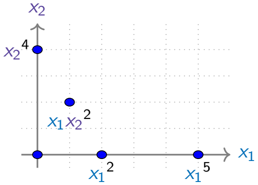
$$\{(0, \ldots, 0)\} \cup \{(e_1, \ldots, e_n) \mid c_{e_1, \ldots, e_n} \neq 0\} \subset \mathbb{R}^n \ .$$

Examples:

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



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



Newton Polyhedron

Definition

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

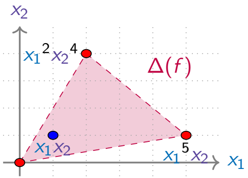
$$f(x_1, \ldots, x_n) = \sum_{e_1, \ldots, e_n} c_{e_1, \ldots, e_n} \prod_{i=1}^n x_i^{e_i} \ .$$

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

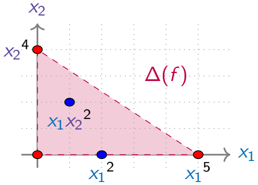
$$\{(0, \ldots, 0)\} \cup \{(e_1, \ldots, e_n) \mid c_{e_1, \ldots, e_n} \neq 0\} \subset \mathbb{R}^n \ .$$

Examples:

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



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



Newton Number

Definition

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

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

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

Newton Number

Definition

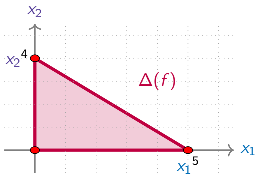
Let $f \in \mathbb{F}_q[x_1, \ldots, x_n]$. The **Newton number** $\nu(f)$ of f is

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

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

Example:

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



Newton Number

Definition

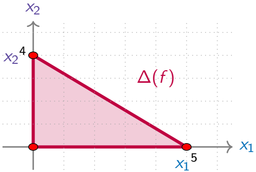
Let $f \in \mathbb{F}_q[x_1, \ldots, x_n]$. The **Newton number** $\nu(f)$ of f is

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

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

Example:

$f(x_1, x_2) = 3 - {x_1}^2 + 5x_1{x_2}^2 + {x_2}^4 + 9{x_1}^5$ $\quad \nu(f) = (-1)^0 \cdot 2! \cdot \mathrm{Vol}_{\Delta(f)}$ $\quad (I = \emptyset)$



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

Newton Number

Definition

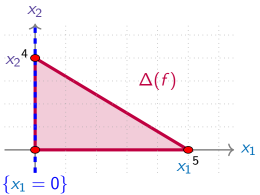
Let $f \in \mathbb{F}_q[x_1, \dots, x_n]$. The **Newton number** $\nu(f)$ of f is

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

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

Example:

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



$$\nu(f) = (-1)^0 \cdot 2! \cdot \mathrm{Vol}_{\Delta(f)} \qquad (I = \emptyset)$$

$$+ (-1)^1 \cdot 1! \cdot \mathrm{Vol}_{\Delta(f) \cap \{x_1 = 0\}} \qquad (I = \{1\})$$

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

Newton Number

Definition

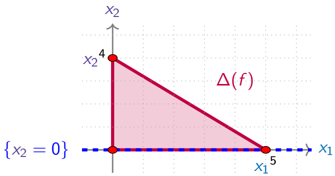
Let $f \in \mathbb{F}_q[x_1, \ldots, x_n]$. The **Newton number** $\nu(f)$ of f is

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

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

Example:

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



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

Newton Number

Definition

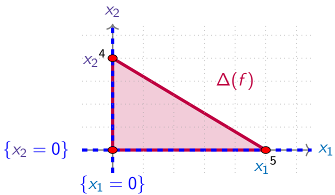
Let $f \in \mathbb{F}_q[x_1, \ldots, x_n]$. The **Newton number** $\nu(f)$ of f is

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

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

Example:

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



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

Newton Number

Definition

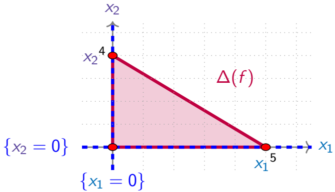
Let $f \in \mathbb{F}_q[x_1, \ldots, x_n]$. The **Newton number** $\nu(f)$ of f is

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

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

Example:

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



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

Commode functions

Definition

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

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

Commode functions

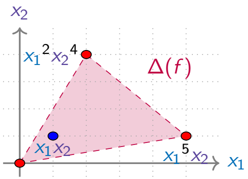
Definition

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

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

Examples:

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



f is not commode

Commode functions

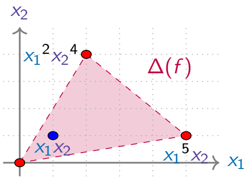
Definition

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

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

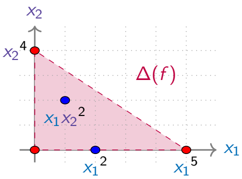
Examples:

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



f is not commode

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



f is commode

Denef-Loeser Theorem

Definition

A function f is **non-degenerate** if for every face τ of $\Delta(f)$ the following system has no nonzero solutions

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

Denef-Loeser Theorem

Definition

A function f is **non-degenerate** if for every face τ of $\Delta(f)$ the following system has no nonzero solutions

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

Theorem [Denef and Loeser, 1991]

Let $f \in \mathbb{F}_q[x_1, \ldots, x_n]$.
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 τ of $\Delta(f)$ the following system has no nonzero solutions

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

Theorem [Denef and Loeser, 1991]

Let $f \in \mathbb{F}_q[x_1, \ldots, x_n]$.
If f is **commode** and **non-degenerate** with respect to its **Newton polyhedron** $\Delta(f)$, then, we have

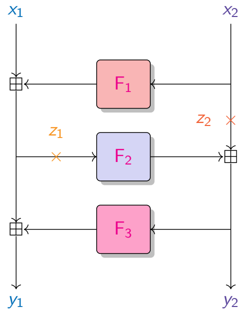
$$|S(f)| = \left| \sum_{x \in \mathbb{F}_q^n} \omega^{f(x)} \right| \leq \nu(f) \cdot q^{n/2} .$$

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

3-round Feistel - Bound

Let $\mathsf{F} = \textsc{Feistel}[\mathsf{F}_1, \mathsf{F}_2, \mathsf{F}_3]$, with round functions F_1, F_2 (permutation) and F_3. Let $d_1 \geq d_3$.

$$\begin{aligned} f(z_1, z_2) &= \langle (v_1, v_2), \mathsf{F}(z_1, z_2)\rangle - \langle (u_1, u_2), (z_1, z_2)\rangle \\ &= v_1 \mathsf{F}_3(z_2 + \mathsf{F}_2(z_1)) + v_2 \mathsf{F}_2(z_1) + u_1 \mathsf{F}_1(z_2) + (v_1 - u_1) z_1 + (v_2 - u_2) z_2 \ . \end{aligned}$$

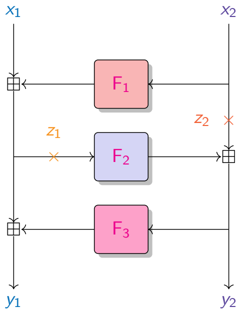


$$\begin{cases} y_1 &= z_1 + \mathsf{F}_3(z_2 + \mathsf{F}_2(z_1)) \\ y_2 &= z_2 + \mathsf{F}_2(z_1) \ . \end{cases}$$

3-round Feistel - Bound

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

$$f(z_1, z_2) = \langle (v_1, v_2), F(z_1, z_2) \rangle - \langle (u_1, u_2), (z_1, z_2) \rangle$$
$$= v_1 F_3(z_2 + F_2(z_1)) + v_2 F_2(z_1) + u_1 F_1(z_2) + (v_1 - u_1) z_1 + (v_2 - u_2) z_2 \ .$$

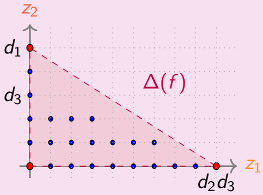


$$\begin{cases} y_1 &= z_1 + F_3(z_2 + F_2(z_1)) \\ y_2 &= z_2 + F_2(z_1) \ . \end{cases}$$

Linearity Bound

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

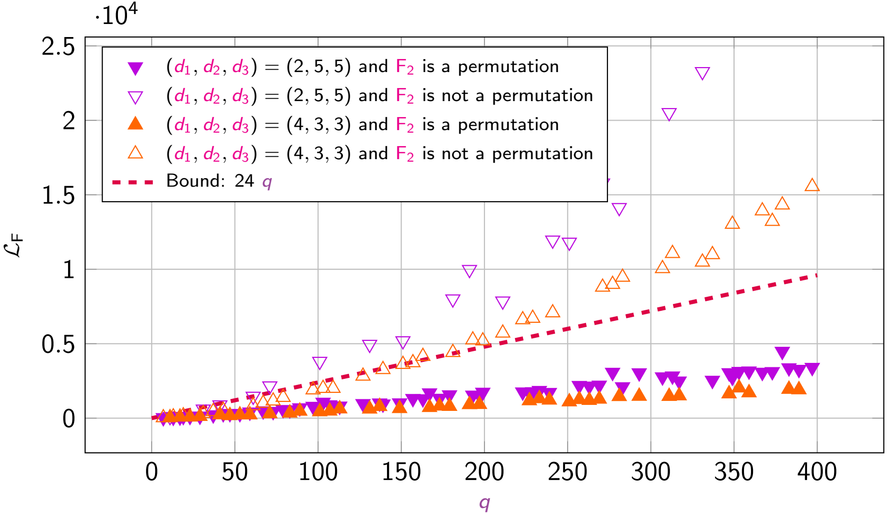
$$\nu(f) = (d_2 d_3 - 1)(d_1 - 1) \ .$$



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

3-round Feistel - Results

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

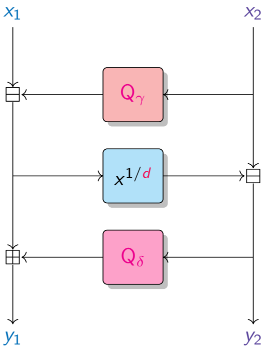


Generalizations of Weil bound

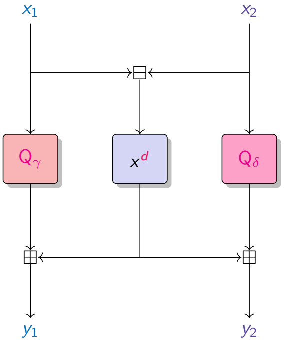
- ⋆ Deligne bound
  - ⋆ Application to the Generalized Butterfly construction
- ⋆ Denef and Loeser bound
  - ⋆ Application to 3-round Feistel construction
- ⋆ Rojas-León bound
  - ⋆ Application to the Generalized Flystel construction

Flystel - Definition

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



Open variant.



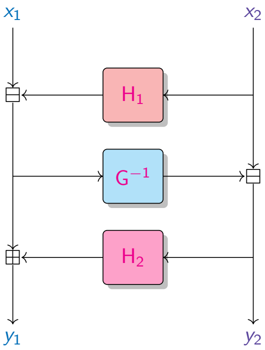
Closed variant.

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

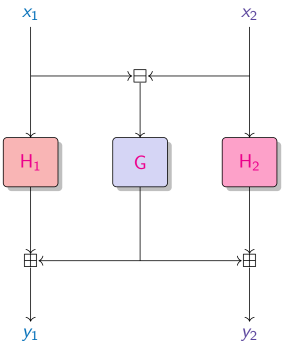
$$\begin{cases} y_1 &= (x_1 - x_2)^d + Q_\gamma(x_1) \\ y_2 &= (x_1 - x_2)^d + Q_\delta(x_2) . \end{cases}$$

Generalized Flystel - Definition

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



Open variant.



Closed variant.

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

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

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 is 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 is there exists $w_1, \ldots, w_n$ s.t.

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

- ⋆ 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: $g(x) = x^d$.

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

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

Rojas-León Theorem

Theorem [Rojas-León, 2006]

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

Suppose that $f = f_d + f_{d'} + \cdots$, 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** $\mu_1, \ldots, \mu_s$,
- ⋆ 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 $f \in \mathbb{F}_q[x_1, \ldots, x_n]$, s.t. $\deg(f) = d$.

Suppose that $f = f_d + f_{d'} + \cdots$, 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** $\mu_1, \ldots, \mu_s$,
- ⋆ the hypersurface defined by $f_{d'} = 0$ contains none of these singularities,

then we have

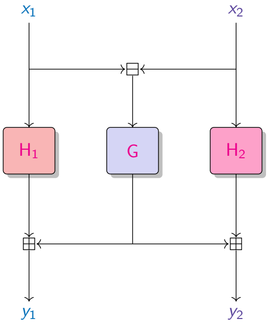
$$|S(f)| = \left| \sum_{x \in \mathbb{F}_q^n} \omega^{f(x)} \right| \leq \left((d-1)^n - (d-d') \sum_{i=1}^{s} \mu_i \right) \cdot q^{n/2} .$$

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

Generalized Flystel - Bound

Let $\mathsf{F} = \textsc{Flystel}[\mathsf{H}_1, \mathsf{G}, \mathsf{H}_2]$, with G a permutation, $\mathsf{H}_1, \mathsf{H}_2$ functions ($\deg \mathsf{G} > \deg \mathsf{H}_1, \deg \mathsf{H}_2$).

$$
\begin{aligned}
f(x_1, x_2) &= \langle (v_1, v_2), \mathsf{F}(x_1, x_2) \rangle - \langle (u_1, u_2), (x_1, x_2) \rangle \\
&= (v_1 + v_2)\, \mathsf{G}(x_1 - x_2) + v_1 \mathsf{H}_1(x_1) + v_2 \mathsf{H}_2(x_2) - u_1 x_1 - u_2 x_2 \ .
\end{aligned}
$$

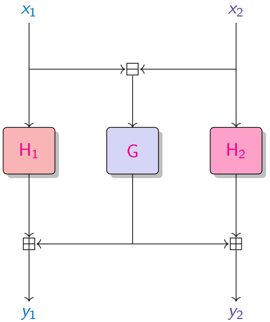


$$
\begin{cases}
y_1 &= \mathsf{G}(x_1 - x_2) + \mathsf{H}_1(x_1) \\
y_2 &= \mathsf{G}(x_1 - x_2) + \mathsf{H}_2(x_2) \, .
\end{cases}
$$

Generalized Flystel - Bound

Let $\mathsf{F} = \textsc{Flystel}[\mathsf{H}_1, \mathsf{G}, \mathsf{H}_2]$, with G a permutation, $\mathsf{H}_1, \mathsf{H}_2$ functions ($\deg \mathsf{G} > \deg \mathsf{H}_1, \deg \mathsf{H}_2$).

$$\begin{aligned} f(x_1, x_2) &= \langle (v_1, v_2), \mathsf{F}(x_1, x_2) \rangle - \langle (u_1, u_2), (x_1, x_2) \rangle \\ &= (v_1 + v_2)\,\mathsf{G}(x_1 - x_2) + v_1 \mathsf{H}_1(x_1) + v_2 \mathsf{H}_2(x_2) - u_1 x_1 - u_2 x_2 \ . \end{aligned}$$



$$\begin{cases} y_1 &= \mathsf{G}(x_1 - x_2) + \mathsf{H}_1(x_1) \\ y_2 &= \mathsf{G}(x_1 - x_2) + \mathsf{H}_2(x_2)\,. \end{cases}$$

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

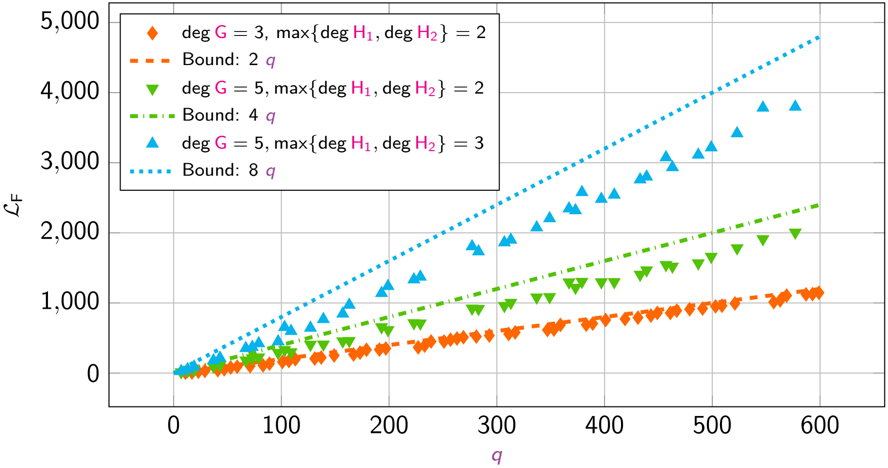
$$f_{d'} = v_i x_i^{\deg \mathsf{H}_i} = 0$$

does not contain this point.

$$\boxed{\mathcal{L}_{\mathsf{F}} \le (\deg \mathsf{G} - 1)(\max\{\deg \mathsf{H}_1, \deg \mathsf{H}_2\} - 1) \cdot q}$$

Generalized Flystel - Results

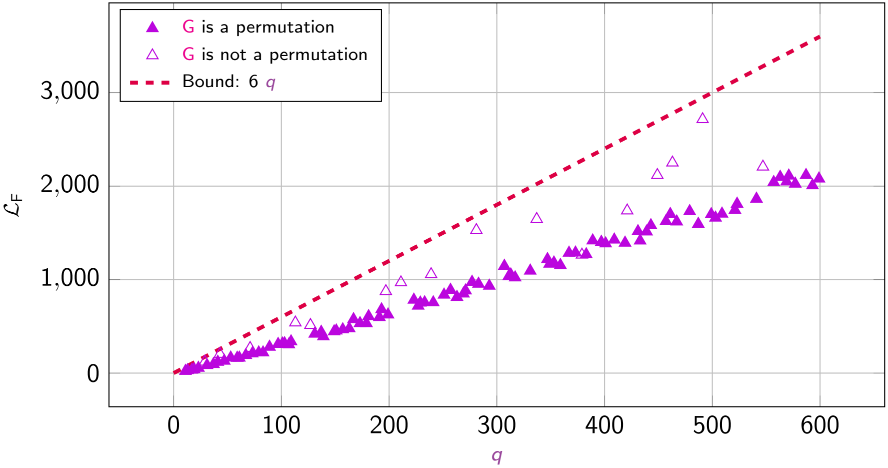
Let $\mathsf{F} = \textsc{Flystel}[\mathsf{H}_1, \mathsf{G}, \mathsf{H}_2]$ with H_1, G and H_2 monomials.



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.



$\deg G = 7$ *and* $\deg H_1 = \deg H_2 = 2$.

Solving conjecture

Conjecture

Let $\mathsf{F} = \textsc{Flystel}[\mathsf{H}_1, \mathsf{G}, \mathsf{H}_2]$ be defined by $\mathsf{H}_1(x) = \gamma + \beta x^2$, $\mathsf{G}(x) = x^d$ and $\mathsf{H}_2 = \delta + \beta x^2$, with $\gamma, \delta \in \mathbb{F}_p$ and $\beta \in \mathbb{F}_p^\times$. Then

$$\mathcal{L}_{\mathsf{F}} \leq p \log p \ .$$

Solving conjecture

Conjecture

Let $\mathsf{F} = \text{Flystel}[\mathsf{H}_1, \mathsf{G}, \mathsf{H}_2]$ be defined by $\mathsf{H}_1(x) = \gamma + \beta x^2$, $\mathsf{G}(x) = x^d$ and $\mathsf{H}_2 = \delta + \beta x^2$, with $\gamma, \delta \in \mathbb{F}_p$ and $\beta \in \mathbb{F}_p^\times$. Then

$$\mathcal{L}_\mathsf{F} \leq p \log p \ .$$

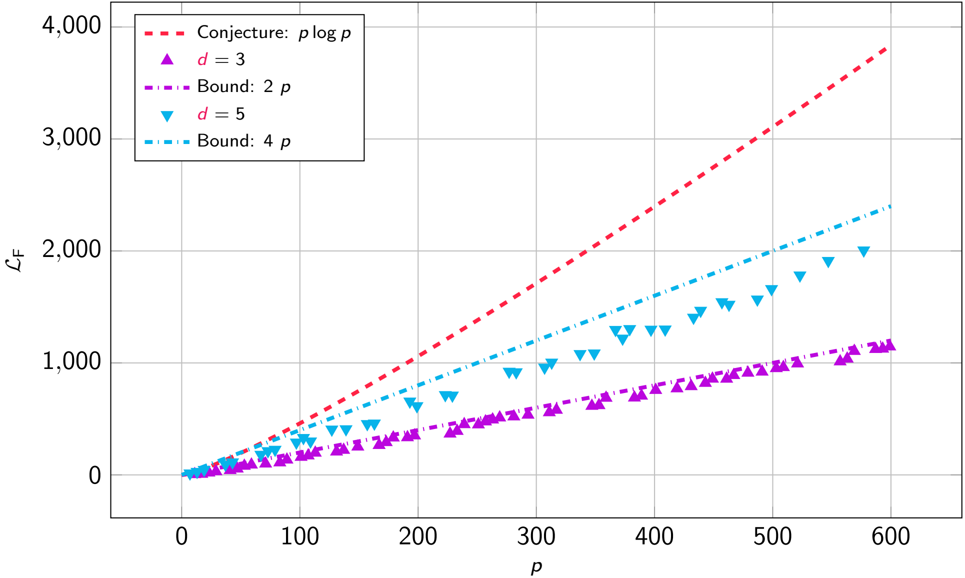
Conjecture proved for $d \leq \log p$

Proposition

Let $\mathsf{F} = \text{Flystel}[\mathsf{H}_1, \mathsf{G}, \mathsf{H}_2]$ be defined by $\mathsf{H}_1(x) = \gamma + \beta x^2$, $\mathsf{G}(x) = x^d$ and $\mathsf{H}_2 = \delta + \beta x^2$, with $\gamma, \delta \in \mathbb{F}_p$ and $\beta \in \mathbb{F}_p^\times$. Then

$$\mathcal{L}_\mathsf{F} \leq (d-1)p \ .$$

Solving conjecture



Conclusions

⋆ Bounds on exponential sums have direct application to linear cryptanalysis

Conclusions

- Bounds on exponential sums have direct application to linear cryptanalysis
- 3 different results...
  - Deligne, 1974
  - Denef and Loeser, 1991
  - Rojas-León, 2006

Conclusions

- Bounds on exponential sums have direct application to linear cryptanalysis
- 3 different results...
  - Deligne, 1974
  - Denef and Loeser, 1991
  - Rojas-León, 2006
- ... for 3 important constructions
  - Generalization of the Butterfly construction
  - 3-round Feistel network
  - Generalization of the Flystel construction

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

Conclusions

- Bounds on exponential sums have direct application to linear cryptanalysis
- 3 different results...
  - Deligne, 1974
  - Denef and Loeser, 1991
  - Rojas-León, 2006
- ... for 3 important constructions
  - Generalization of the Butterfly construction
  - 3-round Feistel network
  - Generalization of the Flystel construction

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

- Solving conjecture on the linearity of the Flystel construction

Conclusions

- Bounds on exponential sums have direct application to linear cryptanalysis
- 3 different results...
  - Deligne, 1974
  - Denef and Loeser, 1991
  - Rojas-León, 2006
- ... for 3 important constructions
  - Generalization of the Butterfly construction
  - 3-round Feistel network
  - Generalization of the Flystel construction

$$\mathrm{F} \in \mathbb{F}_q[x_1, x_2],\ \exists C \in \mathbb{F}_q,\ \mathcal{L}_{\mathrm{F}} \leq C \cdot q$$

- Solving conjecture on the linearity of the Flystel construction

Contribute to the cryptanalysis efforts for AOP.

Cohomological framework

$$S(f) = \sum_{x \in \mathbb{F}_q^n} \chi\big(\mathsf{F}(x)\big)\, \psi(-x)$$

Cohomological framework

$$S(f) = \sum_{x \in \mathbb{F}_q^n} \chi\big(\mathrm{F}(x)\big)\, \psi(-x)$$

$$\Downarrow$$

Cohomological framework

$$\Downarrow$$

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

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

Cohomological framework

$$S(f) = \sum_{x \in \mathbb{F}_q^n} \chi(\mathsf{F}(x))\, \psi(-x)$$

$$\Downarrow$$

Cohomological framework

$$\Downarrow$$

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

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

$$S(f) = \sum_{x \in \mathbb{F}_q^n} \chi\big(\mathsf{F}(x)\big)\, \psi(-x)$$

$$\Downarrow$$

Cohomological framework

$$\Downarrow$$

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

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?

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

Perspectives

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

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

- Can we generalize to other constructions?

stap-zoo.com

And propose a general framework for arithmetization-oriented primitives?

Perspectives

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

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

⋆ Can we generalize to other constructions?

stap-zoo.com

And propose a general framework for arithmetization-oriented primitives?

Thank you

Details on the bound

⋆ Generalized Butterfly bound

$$\left|C^{F}_{\chi,\psi}\right| \leq \frac{1}{q} \begin{cases} (\deg G - 1)(\deg H - 1) & \text{if } \chi_1 = 1 \text{ or } \chi_2 = 1\,, \\ (\max\{\deg G, \deg H\} - 1)^2 & \text{else}\,. \end{cases}$$

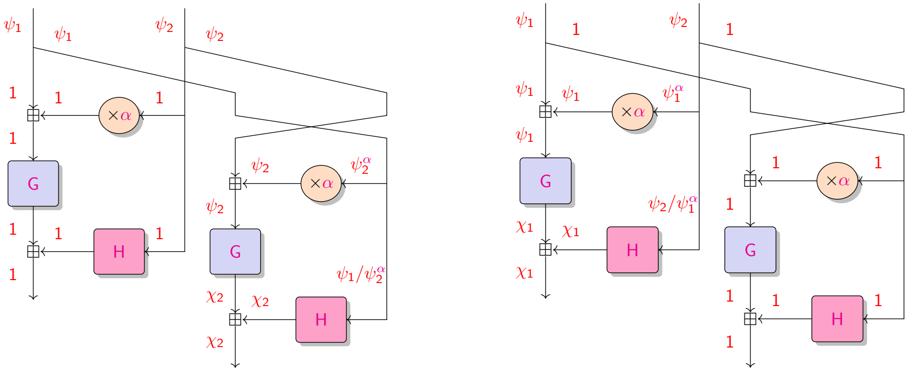
⋆ 3-round Feistel bound

$$\left|C^{F}_{\chi,\psi}\right| \leq \frac{1}{q} \begin{cases} (d_1 - 1)(d_2 - 1) & \text{if } \psi_1 \neq 1 \text{ and } \chi_1 = 1\,, \\ (d_3 - 1)(d_2 - 1) & \text{if } \psi_1 = 1 \text{ and } \chi_1 \neq 1\,, \\ (d_1 - 1)(d_3 - 1) & \text{if } \psi_1\chi_1 = 1\,, \\ (d_1 - 1)(d_2 d_3 - 1) & \text{else}\,. \end{cases}$$

⋆ Generalized Flystel bound

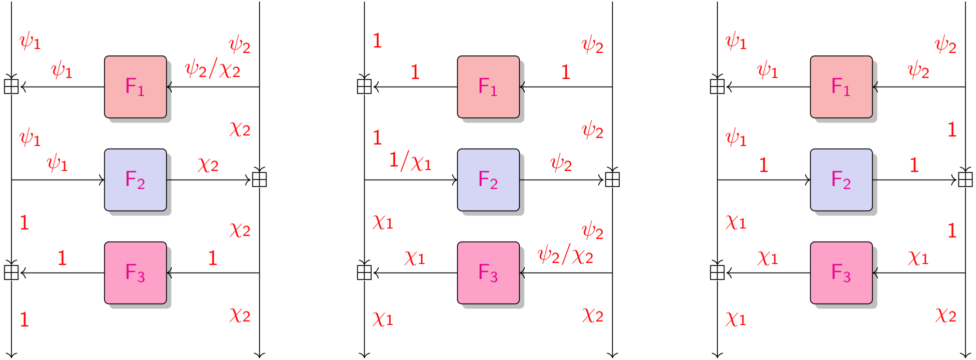
$$\left|C^{F}_{\chi,\psi}\right| \leq \frac{1}{q} \begin{cases} (\deg G - 1)(\deg H_2 - 1) & \text{if } \chi_1 = 1\,, \\ (\deg G - 1)(\deg H_1 - 1) & \text{if } \chi_2 = 1\,, \\ (\deg H_1 - 1)(\deg H_2 - 1) & \text{if } \chi_1\chi_2 = 1\,, \\ (\deg G - 1)(\max\{\deg H_1, \deg H_2\} - 1) & \text{else}\,. \end{cases}$$

Linear trails for a Generalized Butterfly



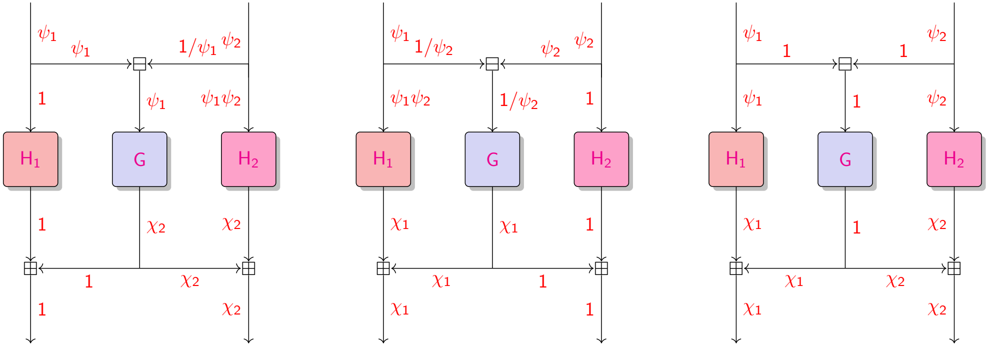
(a) $\chi_1 = 1$. **(b)** $\chi_2 = 1$.

Linear trails for a 3-round Feistel



(a) $\psi_1 \neq 1$ *and* $\chi_1 = 1$. **(b)** $\psi_1 = 1$ *and* $\chi_1 \neq 1$. **(c)** $\psi_1\chi_1 = 1$.

Linear trails for a Generalized Flystel



(a) $\chi_1 = 1.$ **(b)** $\chi_2 = 1.$ **(c)** $\chi_1\chi_2 = 1.$

Bound on exponential sums

The trace of F on $H^i_c(\mathbb{A}^n, \mathcal{L})$ is the sum of its eigenvalues $\lambda_1, \lambda_2, \ldots$.

$$\mathrm{Tr}\big(F \mid H^i_c(\mathbb{A}^n, \mathcal{L})\big) = \lambda_1 + \lambda_2 + \lambda_3 + \ldots$$

Suppose that, $\forall i$, $|\lambda_i| \leq \kappa$, then

$$\left|\mathrm{Tr}\big(F \mid H^i_c(\mathbb{A}^n, \mathcal{L})\big)\right| \leq \kappa \cdot \dim H^i_c(\mathbb{A}^n, \mathcal{L})$$

This gives an upper bound on $S(f)$:

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

$$\leq \kappa \sum_{i=0}^{2n} \dim H^i_c(\mathbb{A}^n, \mathcal{L})$$