Exponential sums and Linear cryptanalysis

Analysis of Butterfly-like constructions

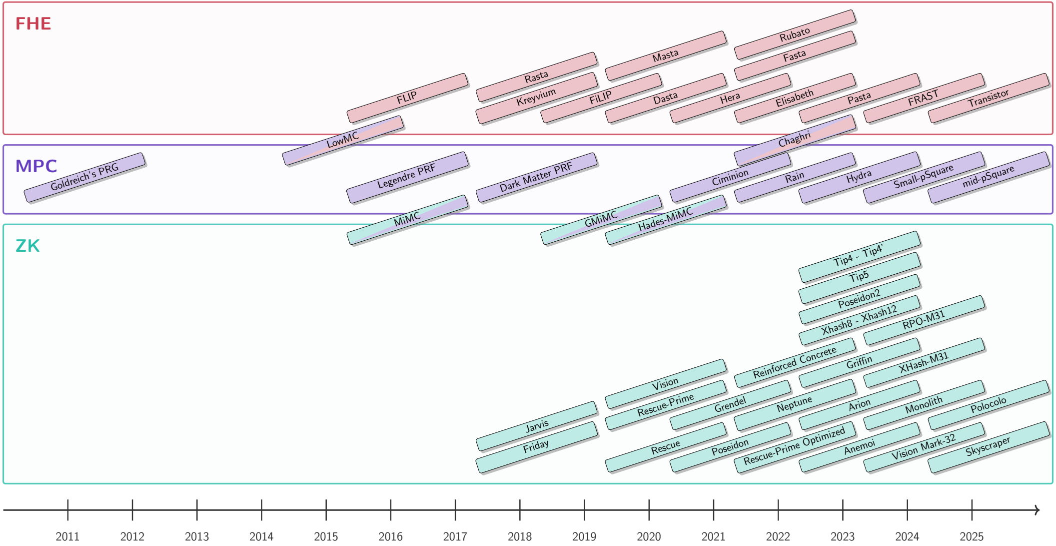
Clémence Bouvier

Université de Lorraine, CNRS, Inria, LORIA

(joint work with Tim Beyne)

Canari Seminar, Bordeaux, France
September 23rd, 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 $a_1, a_2 \in G$

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

$\boxed{\chi(a) \text{ is a root of unity}}$

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 $a_1, a_2 \in G$

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

$\boxed{\chi(a) \text{ is a root of unity}}$

Definition

A **linear approximation** of $F : \mathbb{F}_q^n \to \mathbb{F}_q^m$ 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

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

Let ω be a primitive element, $\mathbb{F}_q \to \mathbb{C}^\times$ 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 element, $\mathbb{F}_q \to \mathbb{C}^\times$ 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

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

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

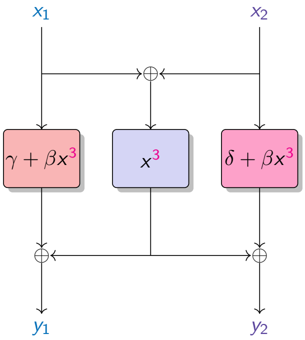
Definition

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.

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

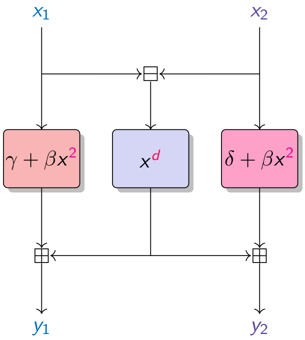
Bound

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].



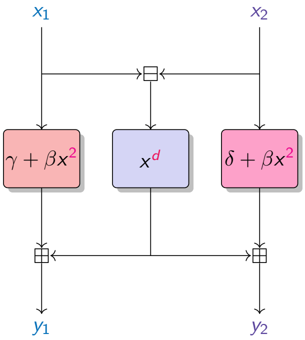
Closed Flystel.

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

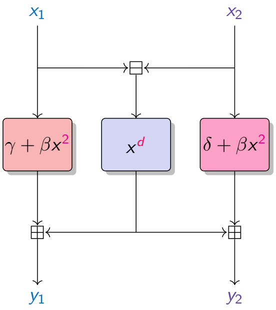
$$\mathcal{L}_f \leq (d-1)\sqrt{p}$$

Weil bound

Proposition [Weil, 1948]

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

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



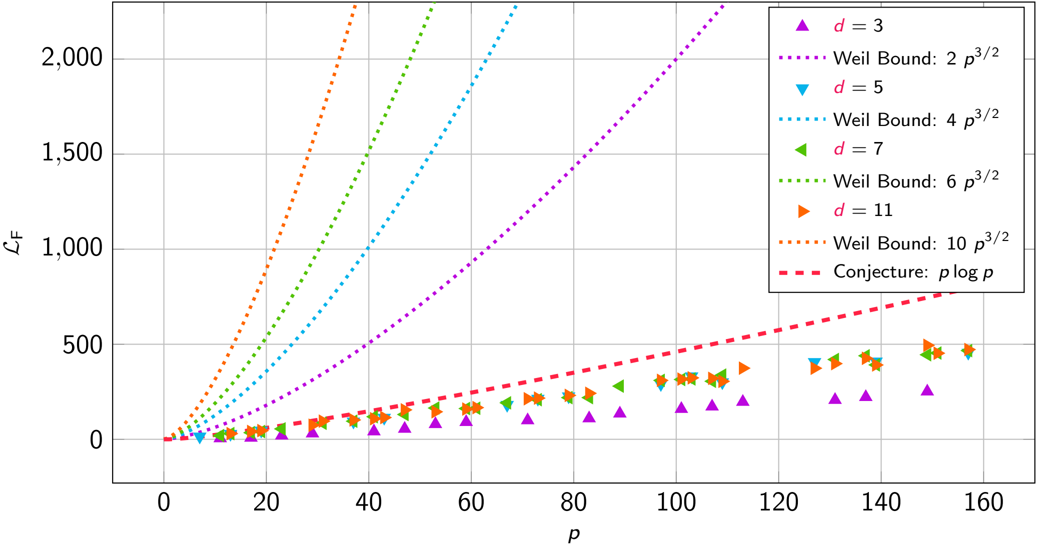
Closed Flystel.

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

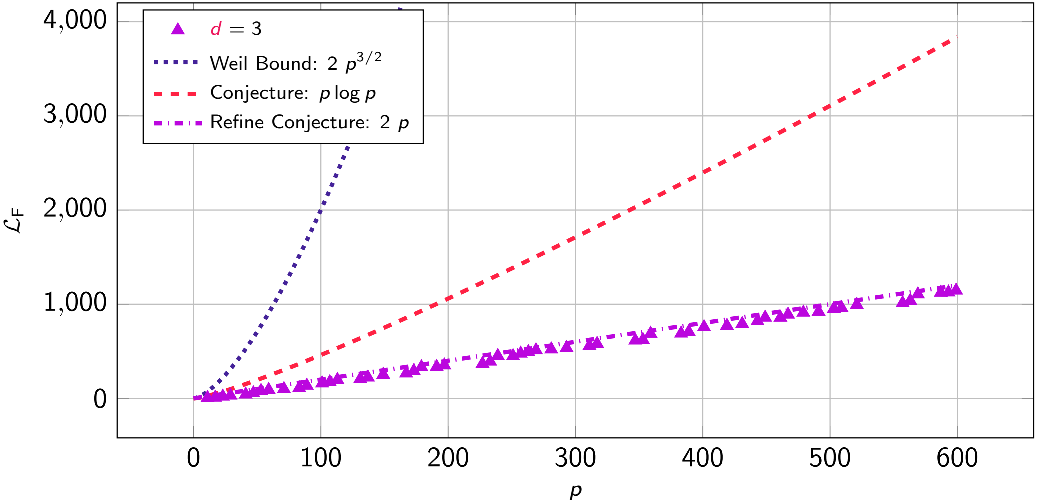
Conjecture

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

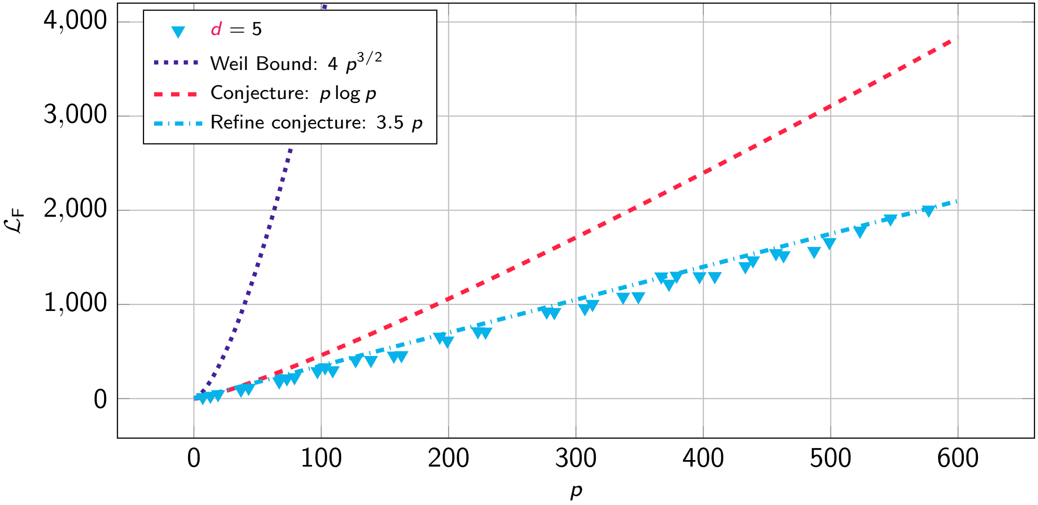
Experimental results



Experimental results ($d = 3$)



Experimental results ($d = 5$)



Take-away

AO primitives: new symmetric primitives defined over prime fields.

$\boxed{\text{Need for new linear cryptanalysis tools}}$

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

[Beyne and Bouvier, 2024]

- ⋆ 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 $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ 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.

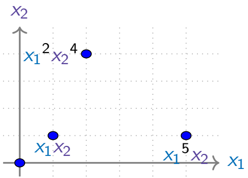
$$f(x_1, \ldots, x_n) = \sum_{e_1, \ldots, e_n} c_{e_1, \ldots, e_n} \prod_{i=1}^{n} x_i^{e_i} \; .$$

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:

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



Newton Polyhedron

Definition

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

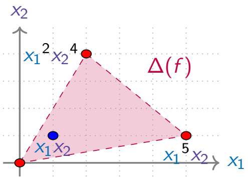
$$f(x_1, \dots, x_n) = \sum_{e_1, \dots, e_n} c_{e_1, \dots, e_n} \prod_{i=1}^{n} x_i^{e_i} .$$

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:

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



Newton Polyhedron

Definition

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

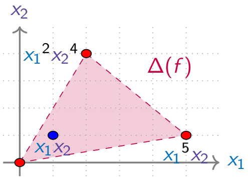
$$f(x_1, \ldots, x_n) = \sum_{e_1, \ldots, e_n} c_{e_1, \ldots, e_n} \prod_{i=1}^{n} x_i^{e_i} .$$

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

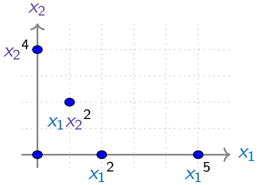
$$\{(0, \ldots, 0)\} \cup \{(e_1, \ldots, e_n) \mid c_{e_1, \ldots, e_n} \neq 0\} \subset \mathbb{R}^n .$$

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.

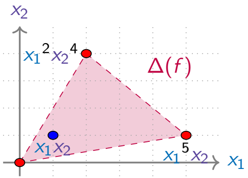
$$f(x_1, \ldots, x_n) = \sum_{e_1, \ldots, e_n} c_{e_1,\ldots,e_n} \prod_{i=1}^n x_i^{e_i} .$$

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

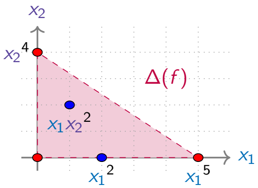
$$\{(0, \ldots, 0)\} \cup \{(e_1, \ldots, e_n) \mid c_{e_1,\ldots,e_n} \neq 0\} \subset \mathbb{R}^n .$$

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 $f \in \mathbb{F}_q[x_1, \ldots, x_n]$. 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 $\Delta(f) \bigcap_{i \in I} \{x_i = 0\}$

Newton Number

Definition

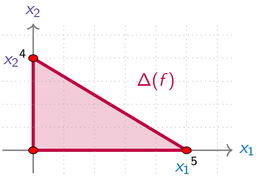
Let $f \in \mathbb{F}_q[x_1, \ldots, x_n]$. The **Newton number** $\nu(f)$ of f is

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

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

Example:

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



Newton Number

Definition

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

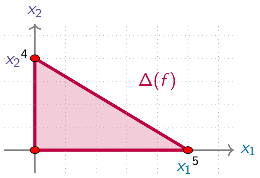
$$\nu(f) = \sum_{I \subseteq \{1,\dots,n\}} (-1)^{|I|}(n - |I|)!\, \mathrm{Vol}_I \Delta(f)\ ,$$

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

Example:

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

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



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

Newton Number

Definition

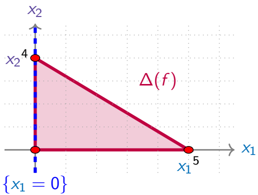
Let $f \in \mathbb{F}_q[x_1, \ldots, x_n]$. The **Newton number** $\nu(f)$ of f is

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

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

Example:

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



$$\nu(f) = (-1)^0 \cdot 2! \cdot \operatorname{Vol}_{\Delta(f)}$$
$$+ (-1)^1 \cdot 1! \cdot \operatorname{Vol}_{\Delta(f) \cap \{x_1 = 0\}} \qquad (I = \{1\})$$

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

Newton Number

Definition

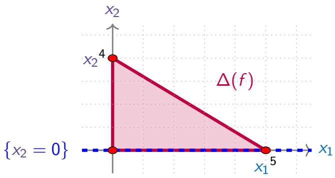
Let $f \in \mathbb{F}_q[x_1, \ldots, x_n]$. The **Newton number** $\nu(f)$ of f is

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

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

Example:

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



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

Newton Number

Definition

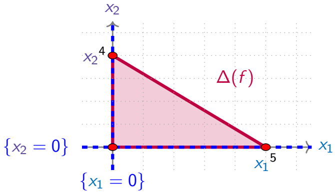
Let $f \in \mathbb{F}_q[x_1, \ldots, x_n]$. The **Newton number** $\nu(f)$ of f is

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

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

Example:

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



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

Newton Number

Definition

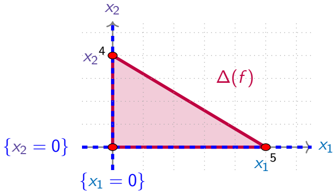
Let $f \in \mathbb{F}_q[x_1, \dots, x_n]$. The **Newton number** $\nu(f)$ of f is

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

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

Example:

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



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

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

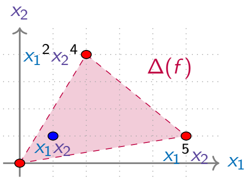
Definition

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:

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



f is not commode

Commode functions

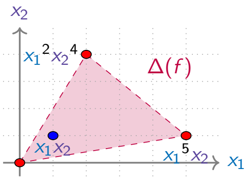
Definition

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

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

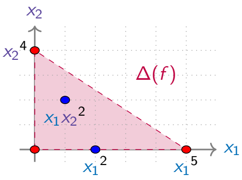
Examples:

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



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 (not containing the origin) 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 (not containing the origin) 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 (not containing the origin) 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

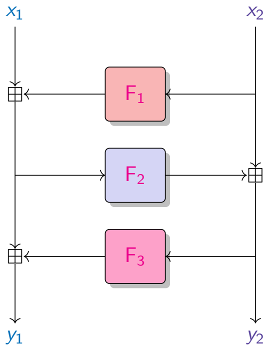
$$|S(f)| = \left| \sum_{x \in \mathbb{F}_q^n} \omega^{f(x)} \right| \leq \nu(f) \cdot q^{n/2} .$$

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

3-round Feistel - Definition

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

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



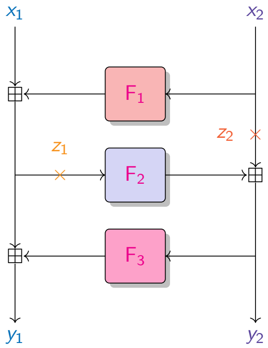
A 3-round Feistel.

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

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.

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

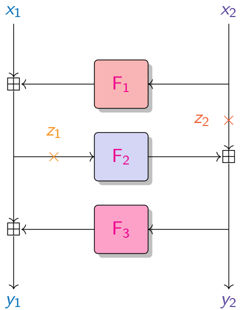
New equations with intermediate variables

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

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 $d_1 \geq d_3$.

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

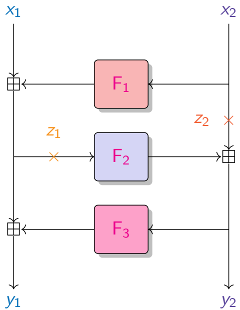


$$\begin{cases} y_1 &= z_1 + \mathsf{F}_3(z_2 + \mathsf{F}_2(z_1)) \\ y_2 &= z_2 + \mathsf{F}_2(z_1) \ . \end{cases}$$

3-round Feistel - Bound

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

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

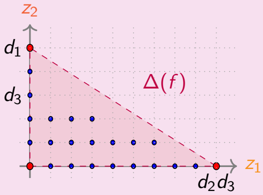


$$\begin{cases} y_1 &= z_1 + \mathsf{F}_3(z_2 + \mathsf{F}_2(z_1)) \\ y_2 &= z_2 + \mathsf{F}_2(z_1) \ . \end{cases}$$

Linearity Bound

- $\star$ f is commode
- $\star$ f is non-degenerate
- $\star$ its Newton number is

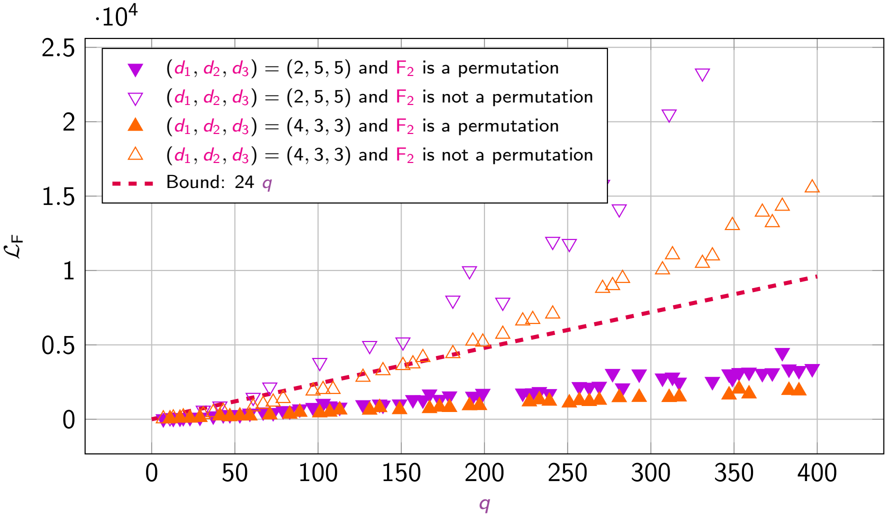
$$\nu(f) = (d_2 d_3 - 1)(d_1 - 1) \ .$$



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

3-round Feistel - Results

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



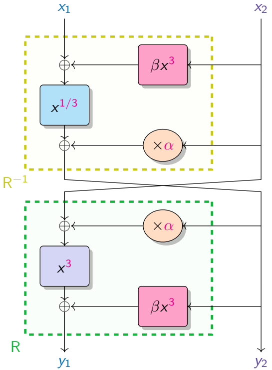
Generalizations of Weil bound

[Beyne and Bouvier, 2024]

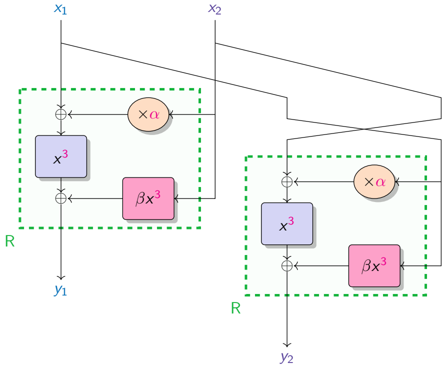
- ⋆ Deligne bound
  - ⋆ Application to the Generalized Butterfly construction
- ⋆ Denef and Loeser bound
  - ⋆ Application to 3-round Feistel construction
- ⋆ Rojas-León bound
  - ⋆ Application to the Generalized Flystel construction

Butterfly - Definition

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



Open variant.



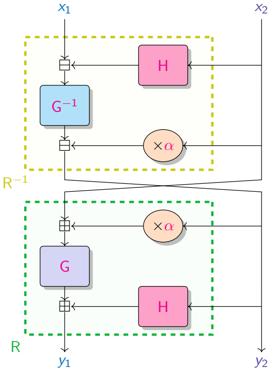
Closed variant.

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

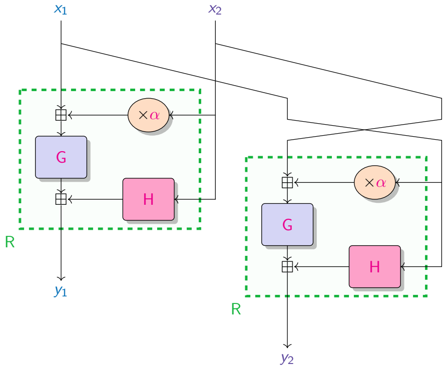
$$\begin{cases} y_1 &= (x_1 + \alpha x_2)^3 + (\beta x_2)^3 \\ y_2 &= (x_2 + \alpha x_1)^3 + (\beta x_1)^3 \,. \end{cases}$$

Generalized Butterfly - Definition

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

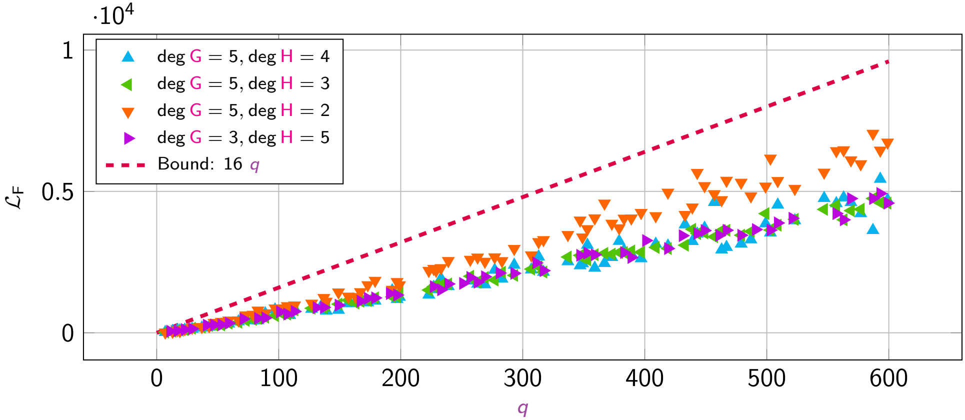
$$\begin{cases} y_1 &= G(x_2 + \alpha y_2) + H(y_2) \\ y_2 &= G^{-1}(x_1 - H(x_2)) - \alpha x_2 \,. \end{cases}$$

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

Generalized Butterfly - Results

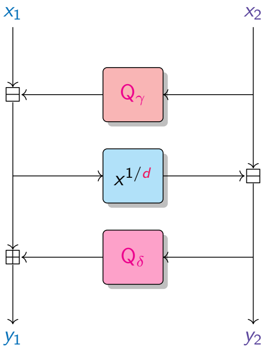
Let $F = \textsc{Butterfly}[G, H, \alpha]$ with G and H monomial functions.

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

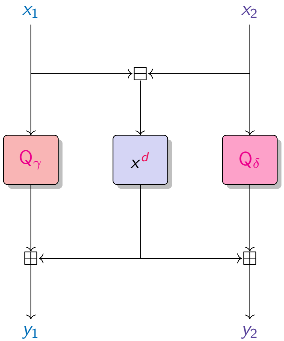


Flystel - Definition

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



Open variant.



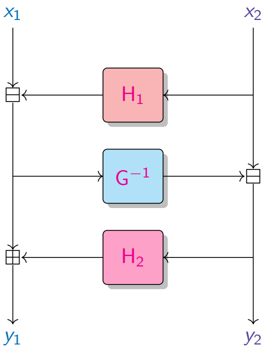
Closed variant.

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

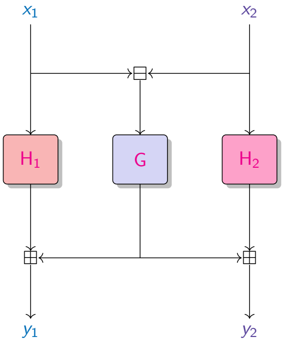
$$\begin{cases} y_1 &= (x_1 - x_2)^d + Q_\gamma(x_1) \\ y_2 &= (x_1 - x_2)^d + Q_\delta(x_2). \end{cases}$$

Generalized Flystel - Definition

$\mathsf{F} = \textsc{Flystel}[\mathsf{H}_1, \mathsf{G}, \mathsf{H}_2]$, with $\mathsf{G} : \mathbb{F}_q \rightarrow \mathbb{F}_q$ a permutation, and $\mathsf{H}_1, \mathsf{H}_2 : \mathbb{F}_q \rightarrow \mathbb{F}_q$ functions.



Open variant.



Closed variant.

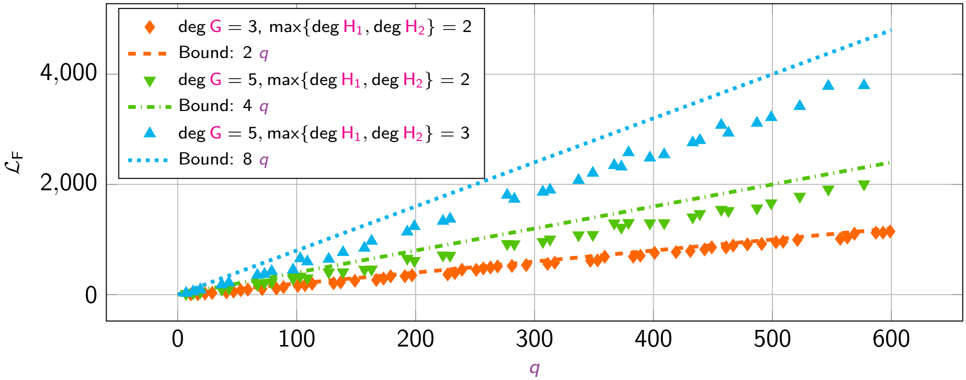
$$\begin{cases} y_1 & = x_1 - \mathsf{H}_1(x_2) + \mathsf{H}_2(x_2 - \mathsf{G}^{-1}(x_1 - \mathsf{H}_1(x_2))) \\ y_2 & = x_2 - \mathsf{G}^{-1}(x_1 - \mathsf{H}_1(x_2))\,. \end{cases}$$

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

Generalized Flystel - Results

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

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

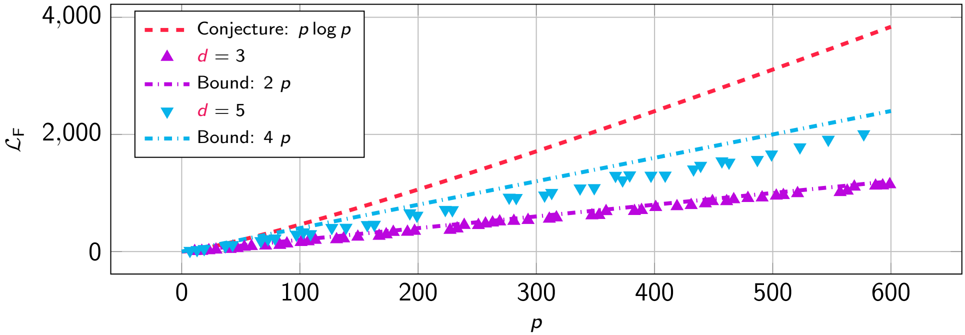


Solving conjecture

Proposition

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

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



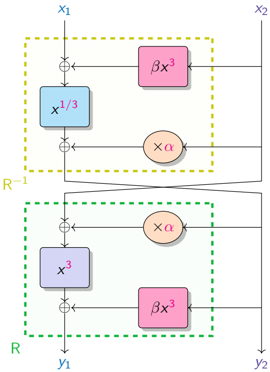
Classification

Can we say more about Butterflies in the context of ZKP?

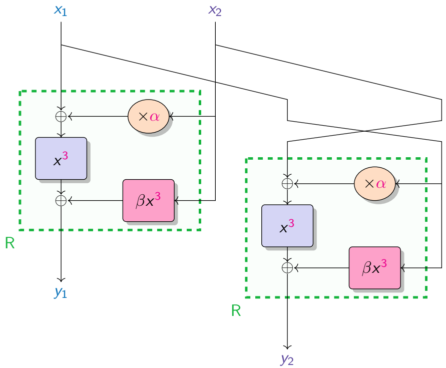
[Bouvier, Fq 2025]

- ⋆ Is the Flystel an optimal construction?
  - ⋆ Statistical properties (differential and linear)
  - ⋆ ZK-performance
- ⋆ How to classify Butterfly-like constructions?

Back to TU decomposition



Open variant.

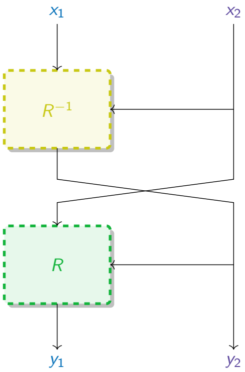


Closed variant.

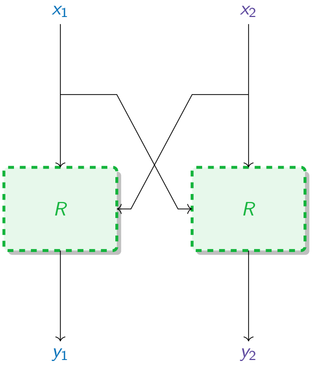
$$\begin{cases} y_1 &= (x_2 + \alpha y_2)^3 + \beta {y_2}^3 \\ y_2 &= (x_1 - \beta {x_2}^3)^{1/3} - \alpha x_2 \,. \end{cases}$$

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

Back to TU decomposition



Open variant.

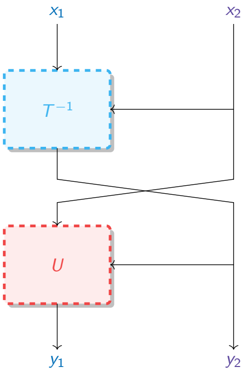


Closed variant.

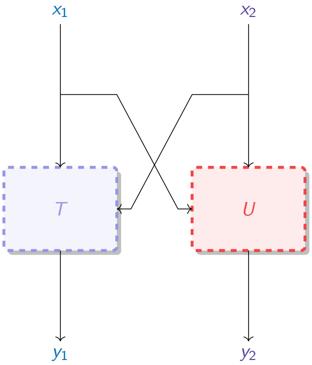
$$\begin{cases} y_1 &= R(x_2, R^{-1}(x_1, x_2)) \\ y_2 &= R^{-1}(x_1, x_2)\,. \end{cases}$$

$$\begin{cases} y_1 &= R(x_1, x_2) \\ y_2 &= R(x_2, x_1)\,. \end{cases}$$

Back to TU decomposition



Open variant.

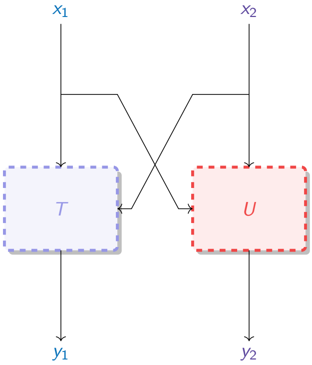


Closed variant.

$$\begin{cases} y_1 &= U(x_2, T^{-1}(x_1, x_2)) \\ y_2 &= T^{-1}(x_1, x_2)\,. \end{cases}$$

$$\begin{cases} y_1 &= T(x_1, x_2) \\ y_2 &= U(x_2, x_1)\,. \end{cases}$$

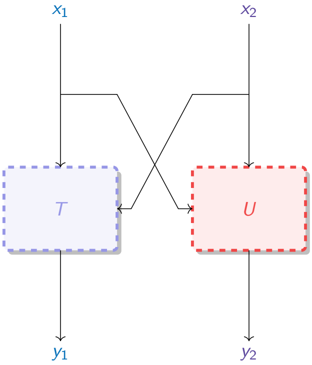
Specific cases



Closed variant.

$$\begin{cases} y_1 & = T(x_1, x_2) \\ y_2 & = U(x_2, x_1) \,. \end{cases}$$

Specific cases



Closed variant.

$$\begin{cases} y_1 &= T(x_1, x_2) \\ y_2 &= U(x_2, x_1)\,. \end{cases}$$

⋆ Asymmetric TU with

$$\text{s.t.} \quad \begin{array}{l} \mathsf{F} : \mathbb{F}_p^2 \to \mathbb{F}_p^2, (x_1, x_2) \mapsto (y_1, y_2) \\ \begin{cases} y_1 &= G_1(x_1, x_2) + H_1(x_1, x_2) \\ y_2 &= H_2(x_1, x_2)\ , \end{cases} \end{array}$$

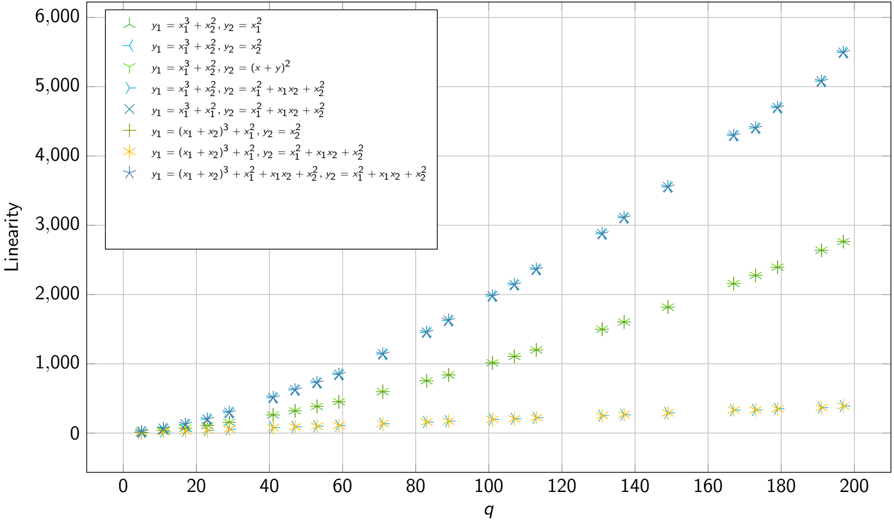
⋆ Symmetric TU with

$$\text{s.t.} \quad \begin{array}{l} \mathsf{F} : \mathbb{F}_p^2 \to \mathbb{F}_p^2, (x_1, x_2) \mapsto (y_1, y_2) \\ \begin{cases} y_1 &= G_1(x_1, x_2) + H_1(x_1, x_2) \\ y_2 &= G_2(x_1, x_2) + H_2(x_1, x_2)\ , \end{cases} \end{array}$$

where

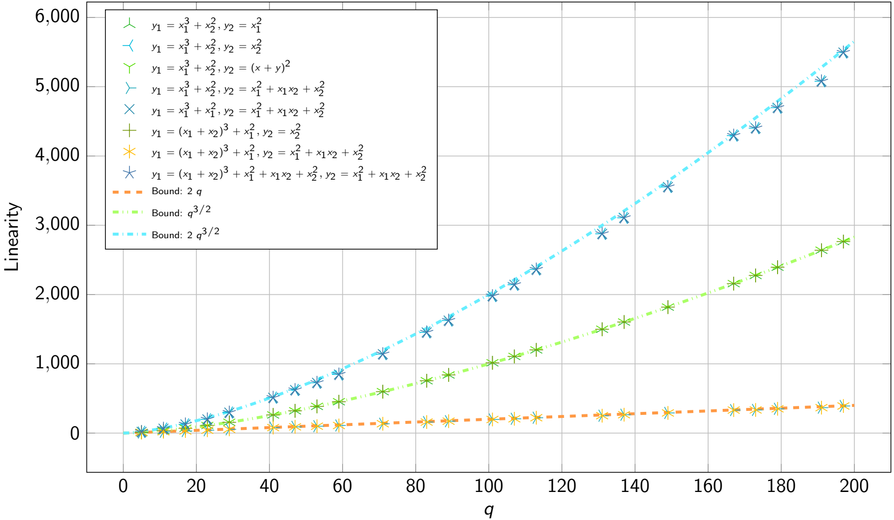
- ⋆ G_i: functions with only cubic terms
- ⋆ H_i: functions with only quadratic terms

Linear properties



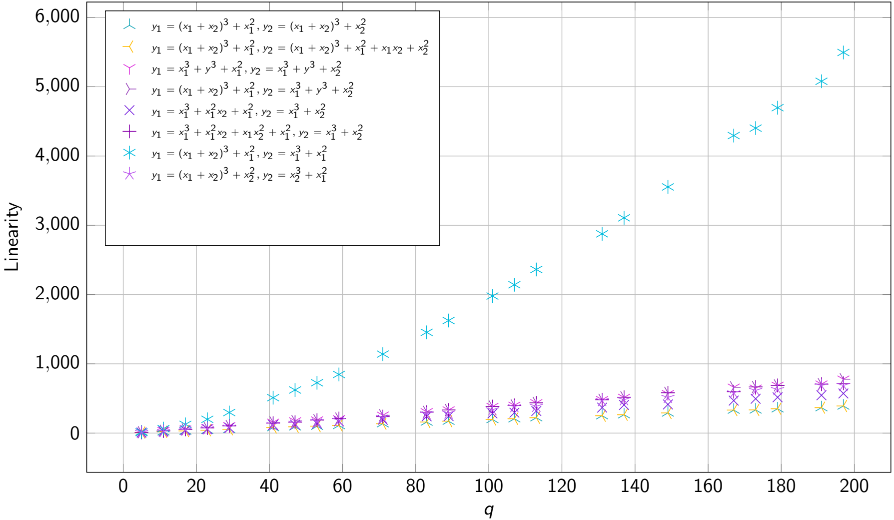
Asymmetric TU

Linear properties



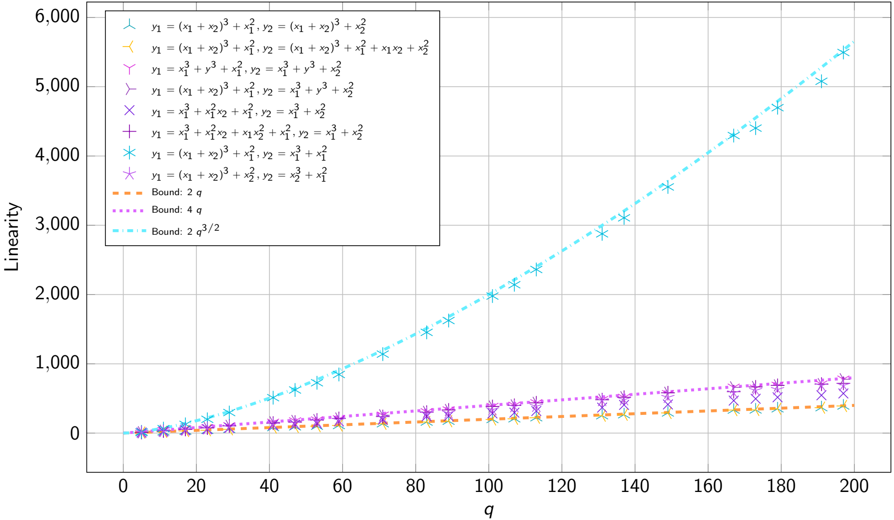
Asymmetric TU

Linear properties



Symmetric TU

Linear properties



Symmetric TU

Performance metric

What does "efficient" mean for Zero-Knowledge Proofs?

Performance metric

What does "efficient" mean for Zero-Knowledge Proofs?

"It depends"

Performance metric

What does "efficient" mean for Zero-Knowledge Proofs?

"It depends"

Example

R1CS (Rank-1 Constraint System): minimizing the number of multiplications

$$y = (ax + b)^3(cx + d) + ex$$

$t_0 = a \cdot x$	$t_3 = t_2 \times t_1$	$t_6 = t_3 \times t_5$
$t_1 = t_0 + b$	$t_4 = c \cdot x$	$t_7 = e \cdot x$
$t_2 = t_1 \times t_1$	$t_5 = t_4 + d$	$t_8 = t_6 + t_7$

Performance metric

What does "efficient" mean for Zero-Knowledge Proofs?

"It depends"

Example

R1CS (Rank-1 Constraint System): minimizing the number of multiplications

$$y = (ax + b)^3(cx + d) + ex$$

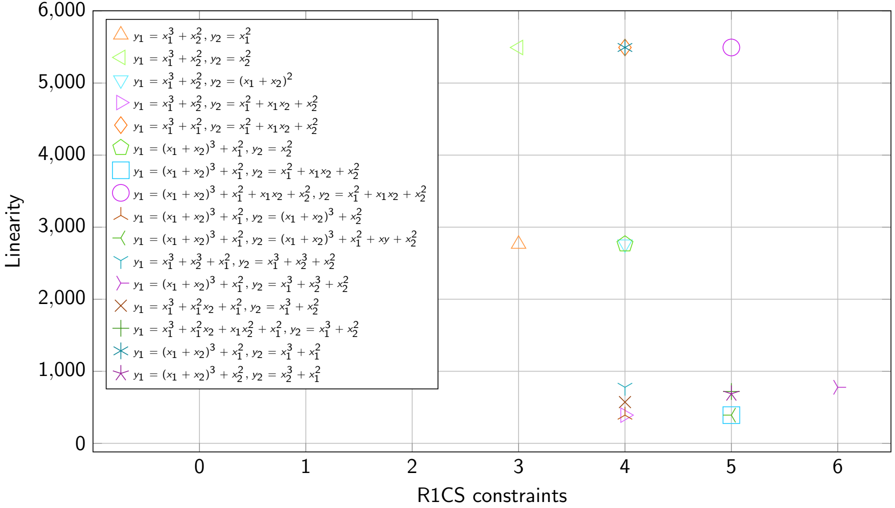
$t_0 = a \cdot x$ $\quad$ $t_3 = t_2 \times t_1$ $\quad$ $t_6 = t_3 \times t_5$

$t_1 = t_0 + b$ $\quad$ $t_4 = c \cdot x$ $\quad$ $t_7 = e \cdot x$

$t_2 = t_1 \times t_1$ $\quad$ $t_5 = t_4 + d$ $\quad$ $t_8 = t_6 + t_7$

3 constraints

ZK performance



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

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

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

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

- 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

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

⋆ Solving conjecture on the linearity of the Flystel construction in Anemoi

⋆ Classification of Butterfly-like constructions in the context of ZKP

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

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

⋆ Solving conjecture on the linearity of the Flystel construction in Anemoi

⋆ Classification of Butterfly-like constructions in the context of ZKP

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

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

$$\Downarrow$$

$$\boxed{\text{Cohomological framework}}$$

$$\Downarrow$$

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

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

Cohomological framework

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

$$\Downarrow$$

$$\boxed{\text{Cohomological framework}}$$

$$\Downarrow$$

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

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.

Cohomological framework

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

$$\Downarrow$$

$$\boxed{\text{Cohomological framework}}$$

$$\Downarrow$$

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

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?

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

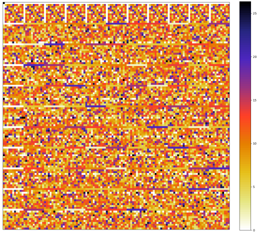
(on-going work with Christophe Levrat)

Perspectives

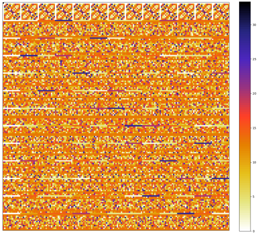
⋆ Can we provide detailed calculations of the cohomological spaces to refine bounds?

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

(on-going work with Christophe Levrat)



Closed Butterfly ($q = 11$)



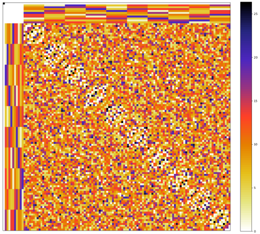
Closed Butterfly ($q = 13$)

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 ($q = 11$)

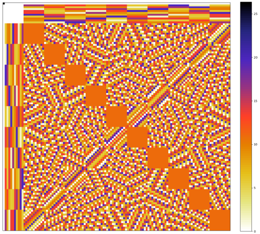
Open Butterfly ($q = 13$)

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)

- ⋆ 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?

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

(on-going work with Christophe Levrat)

⋆ Can we generalize to other constructions?

stap-zoo.com

And propose a general framework for arithmetization-oriented primitives?

More details at *ia.cr/2024/1755*

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)

- ⋆ Can we generalize to other constructions?

stap-zoo.com

And propose a general framework for arithmetization-oriented primitives?

More details at *ia.cr/2024/1755*

Thank you