Butterfly Constructions:

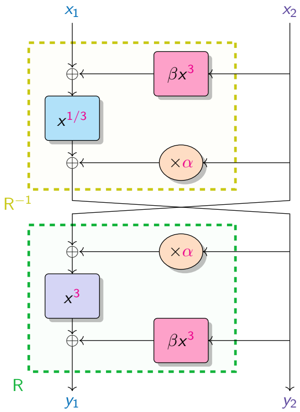
From Boolean Foundations to Remaining Challenges over Prime Fields.

Clémence Bouvier

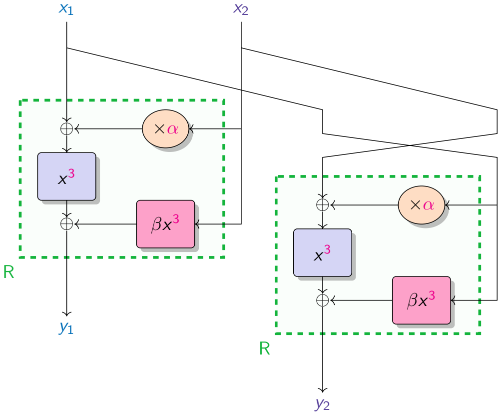
Université de Lorraine, CNRS, Inria, LORIA

Cryptis Seminar, Limoges, France
January 13th, 2026

Butterfly

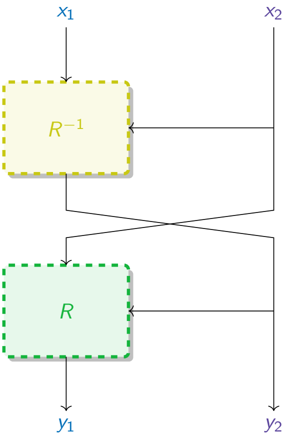


Open variant.

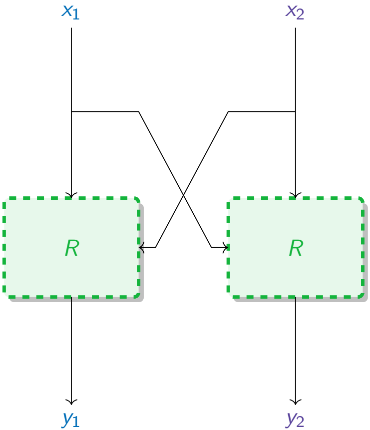


Closed variant.

Butterfly



Open variant.



Closed variant.

Outline

From the original Butterfly construction in $\mathbb{F}_{2^n}^2$...

Preliminaries

and definitions

... to new challenges in prime fields.

Context

and recents results

Differential Uniformity

Differential uniformity

Let $F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ be a function, then

$$\delta_F = \max_{a \neq 0, b} |\{x \in \mathbb{F}_{2^n}, F(x+a) + F(x) = b\}|$$

Differential Uniformity

Differential uniformity

Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a function, then

$$\delta_F = \max_{a \neq 0, b} |\{x \in \mathbb{F}_{2^n}, F(x+a) + F(x) = b\}|$$

Examples:

- If $F : x \mapsto x^{2^n - 2}$, then
$$\delta_F = \begin{cases} 4 & \text{if } n \text{ is even} \\ 2 & \text{if } n \text{ is odd} \end{cases} .$$
- If $F : x \mapsto x^{2^k + 1}$, then
$$\delta_F = 2 .$$

Differential Uniformity

Differential uniformity

Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a function, then

$$\delta_F = \max_{a \neq 0, b} |\{x \in \mathbb{F}_{2^n}, F(x+a) + F(x) = b\}|$$

Examples:

⋆ If $F : x \mapsto x^{2^n-2}$, then

$$\delta_F = \begin{cases} 4 & \text{if } n \text{ is even} \\ 2 & \text{if } n \text{ is odd} \end{cases} .$$

⋆ If $F : x \mapsto x^{2^k+1}$, then

$$\delta_F = 2 .$$

APN (Almost Perfect Non-linear) functions

A function F is APN if for all $a \neq 0$ and b, we have $\delta_F \leq 2$.

Linearity

Linearity

Let $F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ be a function, then

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

Correlation

The maximum correlation for a linear approximation (u, v) is

$$C_F = 2^{-n} \cdot \mathcal{W}_F$$

Linearity

Linearity

Let F : $\mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a function, then

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

Correlation

The maximum correlation for a linear approximation (u, v) is

$$C_F = 2^{-n} \cdot \mathcal{W}_F$$

Examples:

- If $F : x \mapsto Lx + c$, then

$$\mathcal{W}_F = 2^n \quad \text{and} \quad C_F = 1 \ .$$

- If $F : x \mapsto x^{-1}$, with n even, then

$$\mathcal{W}_F = 2^{n/2+1} \quad \text{and} \quad C_F = 2^{-n/2+1} \ .$$

CCZ-equivalence

Inversion

$$\Gamma_F = \{(x, F(x)), x \in \mathbb{F}_{2^n}\} \quad \text{and} \quad \Gamma_{F^{-1}} = \{(y, F^{-1}(y)), y \in \mathbb{F}_{2^n}\}$$

Noting that

$$\Gamma_F = \{(F^{-1}(y), y), y \in \mathbb{F}_{2^n}\} ,$$

then, we have:

$$\Gamma_F = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \Gamma_{F^{-1}} .$$

CCZ-equivalence

Inversion

$$\Gamma_F = \{(x, F(x)), x \in \mathbb{F}_{2^n}\} \quad \text{and} \quad \Gamma_{F^{-1}} = \left\{\left(y, F^{-1}(y)\right), y \in \mathbb{F}_{2^n}\right\}$$

Noting that

$$\Gamma_F = \left\{\left(F^{-1}(y), y\right), y \in \mathbb{F}_{2^n}\right\} \ ,$$

then, we have:

$$\Gamma_F = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \Gamma_{F^{-1}} \ .$$

Definition [Carlet, Charpin and Zinoviev, 1998]

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and $G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are **CCZ-equivalent** if

$$\Gamma_F \ = \ \mathcal{L}(\Gamma_G) + c \ , \quad \text{where } \mathcal{L} \text{ is linear.}$$

Advantages of CCZ-equivalence

If $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and $G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are **CCZ-equivalent**. Then

⋆ **Differential** properties are the same: $\delta_F = \delta_G$.

Differential uniformity

$$\delta_F = \max_{a \neq 0, b} |\{x \in \mathbb{F}_{2^n}, F(x+a) + F(x) = b\}|$$

Advantages of CCZ-equivalence

If $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and $G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are **CCZ-equivalent**. Then

- ⋆ **Differential** properties are the same: $\delta_F = \delta_G$.

Differential uniformity

$$\delta_F = \max_{a \neq 0, b} |\{x \in \mathbb{F}_{2^n}, F(x+a) + F(x) = b\}|$$

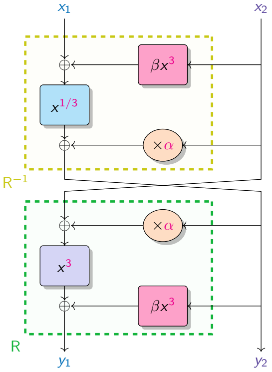
- ⋆ **Linear** properties are the same: $\mathcal{W}_F = \mathcal{W}_G$.

Linearity

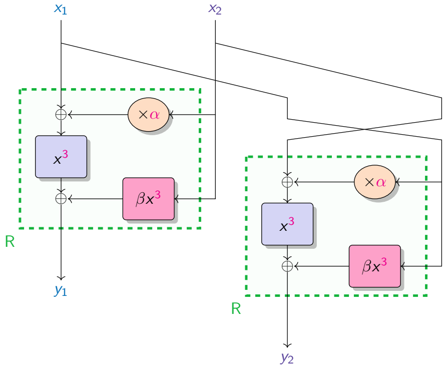
$$\mathcal{W}_F = \max_{u, v \neq 0} \left| \sum_{x \in \mathbb{F}_{2^n}} (-1)^{u \cdot x + v \cdot F(x)} \right|$$

Butterfly - Definition

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



Open variant.



Closed variant.

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

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

Take-away

- ⋆ Butterfly introduced over binary fields
- ⋆ Structure of APN permutations on an even number of bits
- ⋆ 2 variants of the construction: Open and Closed
- ⋆ An example of CCZ-equivalent functions
- ⋆ Same differential and linear properties for the 2 variants

Outline

From the original Butterfly in $\mathbb{F}_{2^n}^2$...

Preliminaries

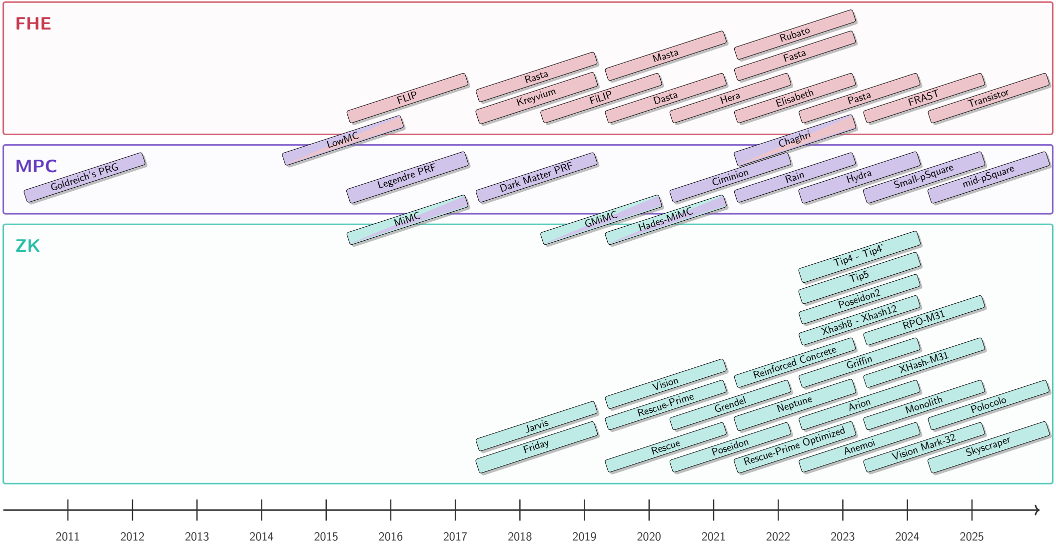
and definitions

... to new challenges in prime fields.

Context

and recents results

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

$\leq$ 8 years of cryptanalysis

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

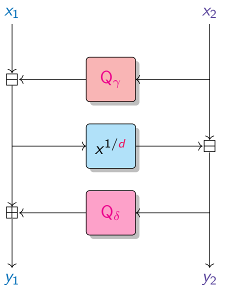
The Flystel in Anemoi

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

Butterfly + Feistel ⇒ Flystel

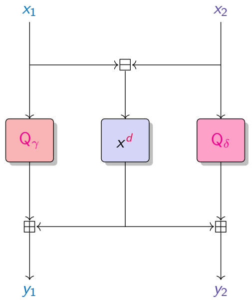
$Q_\gamma : \mathbb{F}_q \to \mathbb{F}_q$ and $Q_\delta : \mathbb{F}_q \to \mathbb{F}_q$ two quadratic functions, and $E : \mathbb{F}_q \to \mathbb{F}_q, x \mapsto x^d$ a permutation

High-Degree permutation



Open Flystel $\mathcal{H}$.

Low-Degree function



Closed Flystel $\mathcal{V}$.

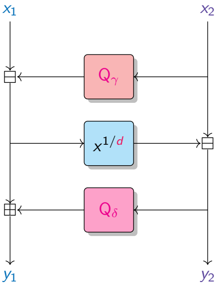
The Flystel in Anemoi

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

Butterfly + Feistel ⇒ Flystel

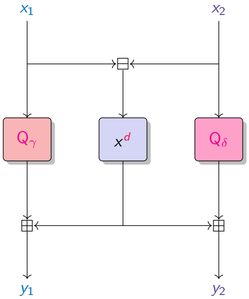
$Q_\gamma : \mathbb{F}_q \to \mathbb{F}_q$ and $Q_\delta : \mathbb{F}_q \to \mathbb{F}_q$ two quadratic functions, and $E : \mathbb{F}_q \to \mathbb{F}_q, x \mapsto x^d$ a permutation

High-Degree
permutation



Open Flystel $\mathcal{H}$.

Low-Degree
function



Closed Flystel $\mathcal{V}$.

$$\Gamma_{\mathcal{H}} = \mathcal{L}(\Gamma_{\mathcal{V}}) \quad \text{s.t.} \quad ((x_1, x_2), (y_1, y_2)) = \mathcal{L}\left(((y_2, x_2), (x_1, y_1)) \right)$$

How to adapt definitions

Differential uniformity

In binary fields

$$\delta_F = \max_{a \neq 0, b} \left| \{ x \in \mathbb{F}_{2^n}, F(x+a) + F(x) = b \} \right|$$

In prime fields

$$\delta_F = \max_{a \neq 0, b} \left| \{ x \in \mathbb{F}_p, F(x+a) - F(x) = b \} \right|$$

How to adapt definitions

Differential uniformity

In binary fields

$$\delta_F = \max_{a \neq 0, b} |\{x \in \mathbb{F}_{2^n}, F(x+a) + F(x) = b\}|$$

In prime fields

$$\delta_F = \max_{a \neq 0, b} |\{x \in \mathbb{F}_p, F(x+a) - F(x) = b\}|$$

Linearity

In binary fields

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

Characters

Definition

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

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

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

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

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 $F : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^m$ 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

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

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

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

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

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

Definition

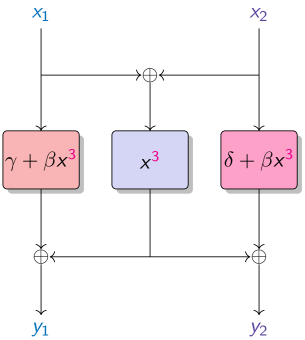
The **Linearity** $\mathcal{L}_F$ of $F : \mathbb{F}_q^n \to \mathbb{F}_q^m$ is the highest Walsh coefficient.

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

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

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

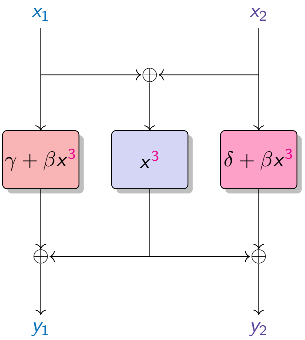
Degenerate case of Butterfly



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

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

Degenerate case of Butterfly



If $\beta \neq 0$, then [Li et al., 2018] stated that

Differential uniformity

$$\delta_F = \max_{a \neq 0, b} \left| \{x \in \mathbb{F}_{2^n}^2, F(x+a) + F(x) = b\} \right|$$

Bound:

$$\delta_F \leq 4$$

Linearity

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

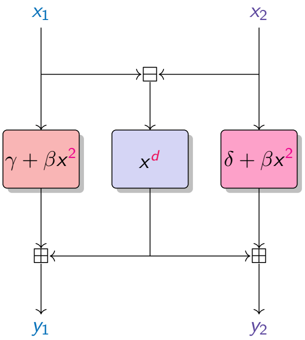
Bound:

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

Closed Flystel in $\mathbb{F}_p$

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

$x \mapsto x^d$ a perm. (usually $d = 3, 5$)



Differential uniformity

$$\delta_F = \max_{a \neq 0, b} |\{x \in \mathbb{F}_p^2, F(x + a) - F(x) = b\}|$$

Bound:

$$\delta_F \leq d - 1$$

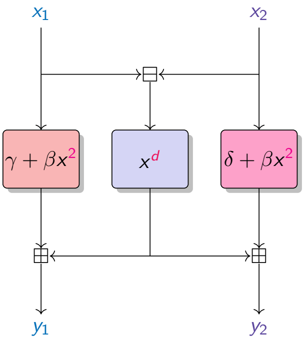
Solving an open problem

Finding APN permutations over $\mathbb{F}_p^2$.

Closed Flystel in $\mathbb{F}_p$

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

$x \mapsto x^d$ a perm. (usually $d = 3, 5$)



Differential uniformity

$$\delta_F = \max_{a \neq 0, b} |\{x \in \mathbb{F}_p^2, F(x+a) - F(x) = b\}|$$

Bound:

$$\delta_F \leq d - 1$$

Solving an open problem

Finding APN permutations over $\mathbb{F}_p^2$.

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

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

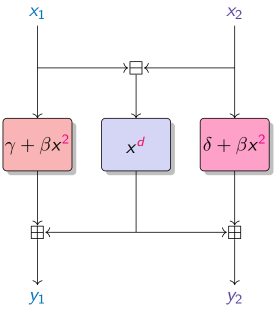
$$\mathcal{L}_f \leq (d-1)\sqrt{p}$$

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.

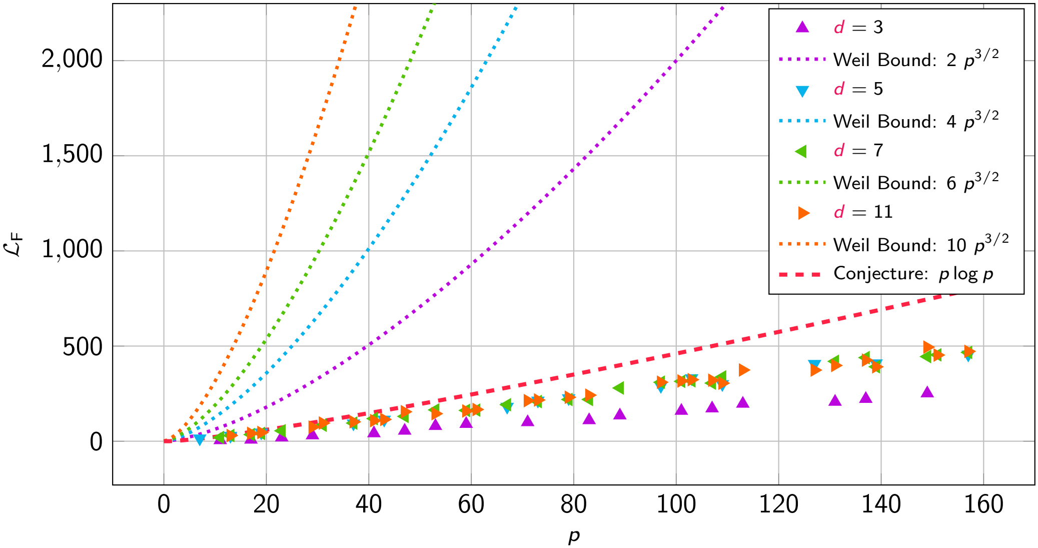
$$\mathcal{L}_F \leq (d-1)p\sqrt{p} \ ?$$

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

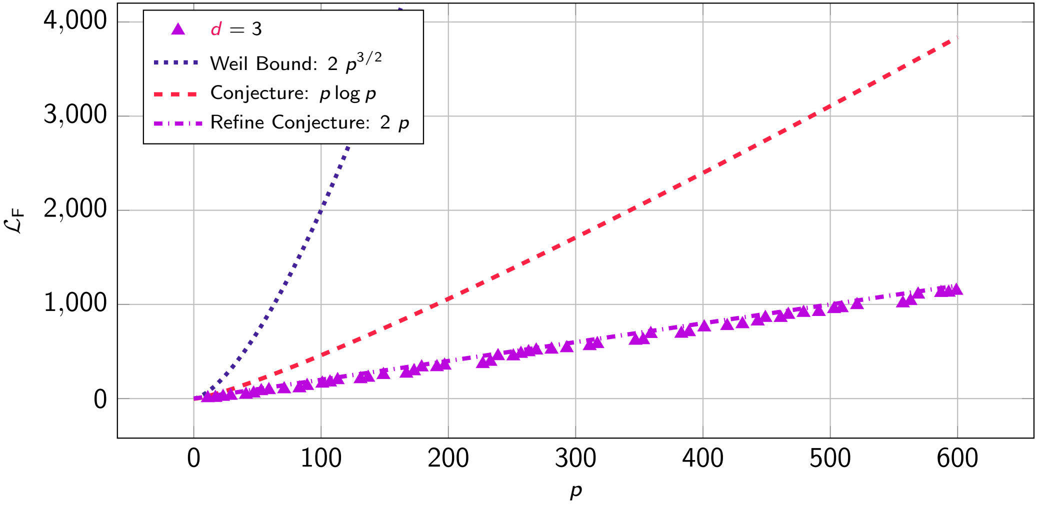
Conjecture

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

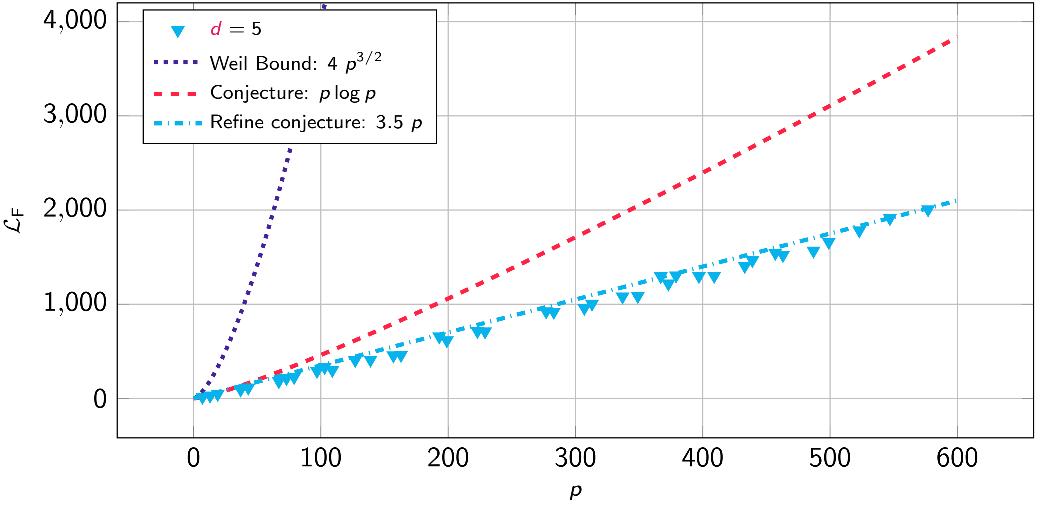
Experimental results



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:

- ⋆ 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

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.

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

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

  so that

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

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

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

  so that

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

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.

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

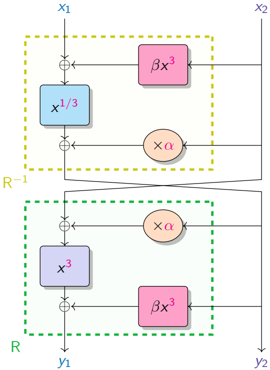
If the hypersurface defined by $f_d = 0$ is **smooth**, then, we have

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

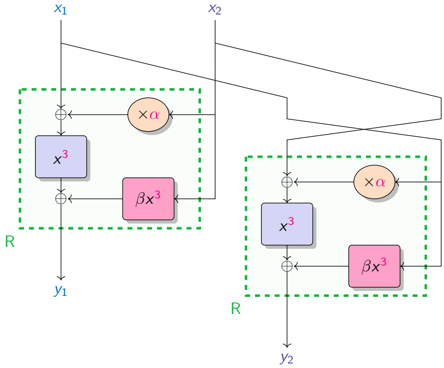
Linearity bound for $n = 2$: $\mathcal{L}_F \leq (d-1)^2 \cdot q$.

Butterfly - Definition

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



Open variant.



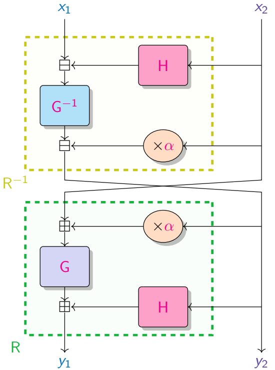
Closed variant.

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

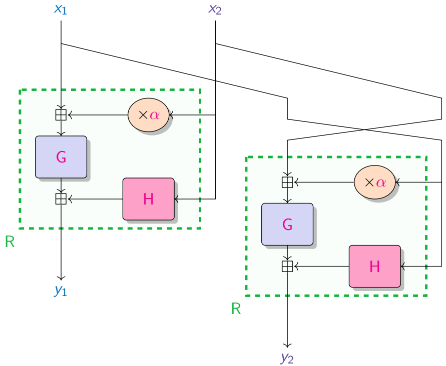
$$\begin{cases} y_1 &= (x_1 + \alpha x_2)^3 + (\beta x_2)^3 \\ y_2 &= (x_2 + \alpha x_1)^3 + (\beta x_1)^3 \,. \end{cases}$$

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.

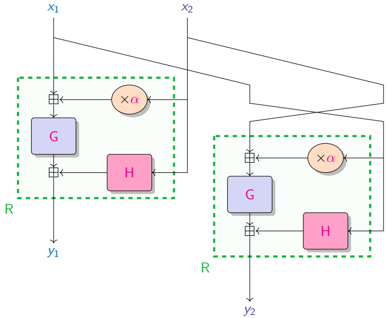
$$\begin{cases} y_1 &= G(x_2 + \alpha y_2) + H(y_2) \\ y_2 &= G^{-1}(x_1 - H(x_2)) - \alpha x_2 \,. \end{cases}$$

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

Generalized Butterfly - Bound

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

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

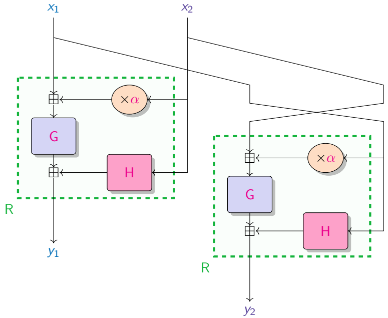


$$\begin{cases} y_1 &= \mathsf{G}(x_1 + \alpha x_2) + \mathsf{H}(x_2) \\ y_2 &= \mathsf{G}(x_2 + \alpha x_1) + \mathsf{H}(x_1) \, . \end{cases}$$

Generalized Butterfly - Bound

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

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



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

Linearity Bound

- ⋆ If $d = \deg \mathsf{G} > \deg \mathsf{H} > 1$, 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.

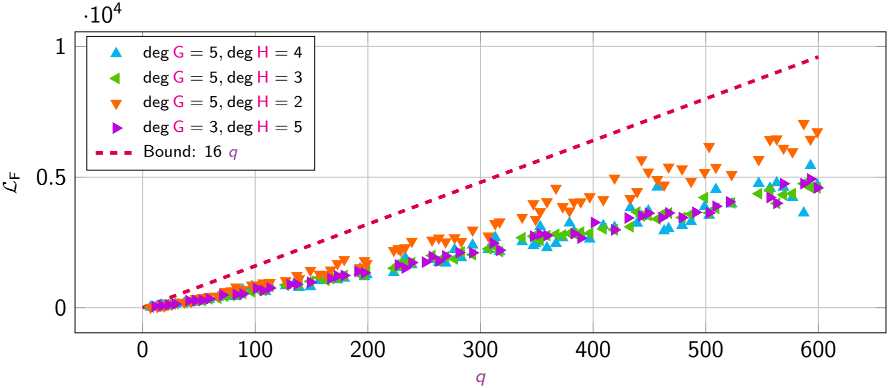
- ⋆ If $d = \deg \mathsf{H} > \deg \mathsf{G} > 1$, then

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

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

Generalized Butterfly - Results

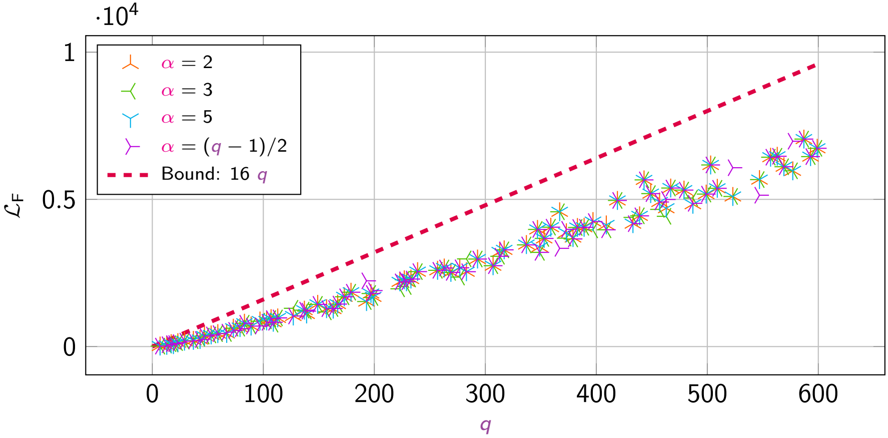
Let $\mathsf{F} = \textsc{Butterfly}[\mathsf{G}, \mathsf{H}, \alpha]$ with G and H monomial functions.



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

Generalized Butterfly - Results

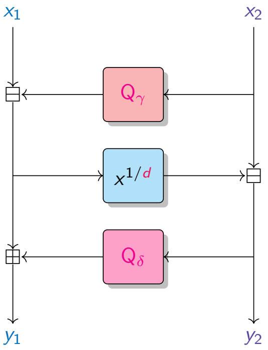
Let $F = \textsc{Butterfly}[G, H, \alpha]$ with G and H monomial functions.



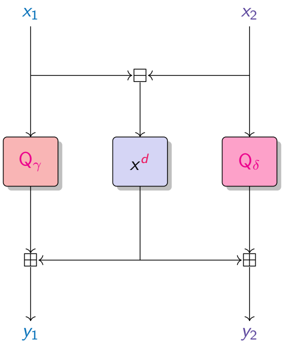
Influence of α (deg G = 5 and deg H = 2).

Flystel - Definition

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



Open variant.



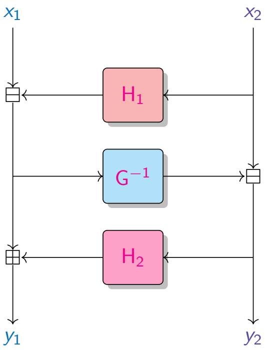
Closed variant.

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

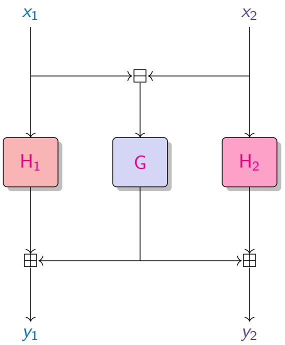
$$\begin{cases} y_1 & = (x_1 - x_2)^d + Q_\gamma(x_1) \\ y_2 & = (x_1 - x_2)^d + Q_\delta(x_2) . \end{cases}$$

Generalized Flystel - Definition

$F = \textsc{Flystel}[H_1, G, H_2]$, 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.

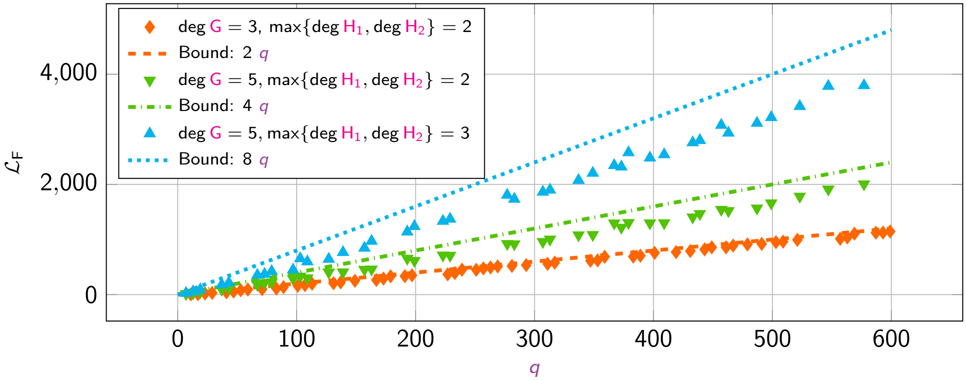
$$\begin{cases} y_1 & = x_1 - H_1(x_2) + H_2(x_2 - G^{-1}(x_1 - H_1(x_2))) \\ y_2 & = x_2 - G^{-1}(x_1 - H_1(x_2)) \,. \end{cases}$$

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

Generalized Flystel - Results

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

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

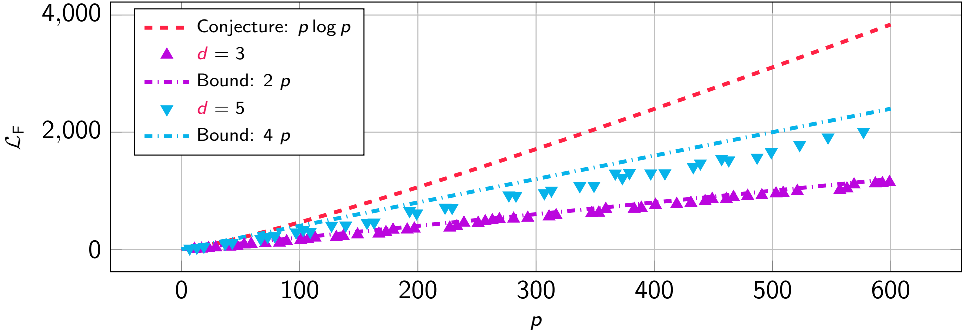


Solving conjecture

Proposition

Let $F = \text{Flystel}[H_1, G, H_2]$ 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

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



Conclusions

⋆ Butterfly construction found interest over prime fields

Conclusions

- ⋆ Butterfly construction found interest over prime fields
- ⋆ Solving the open problem of finding APN permutations over $\mathbb{F}_p^2$

Conclusions

- ⋆ Butterfly construction found interest over prime fields
- ⋆ Solving the open problem of finding APN permutations over $\mathbb{F}_p^2$
- ⋆ 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

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

Conclusions

- ⋆ Butterfly construction found interest over prime fields
- ⋆ Solving the open problem of finding APN permutations over $\mathbb{F}_p^2$
- ⋆ 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

- Butterfly construction found interest over prime fields

- Solving the open problem of finding APN permutations over $\mathbb{F}_p^2$

- 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

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

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

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

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

$$\Downarrow$$

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

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

$$\Downarrow$$

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.

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?

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

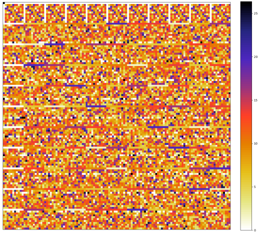
(on-going work with Christophe Levrat)

Perspectives

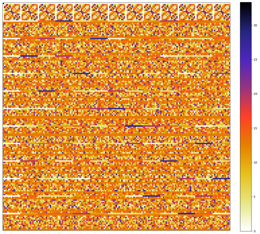
Can we provide detailed calculations of the cohomological spaces to refine bounds?

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

(on-going work with Christophe Levrat)



Closed Butterfly ($q = 11$)



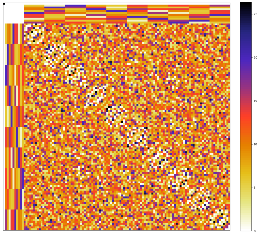
Closed Butterfly ($q = 13$)

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 ($q = 11$)

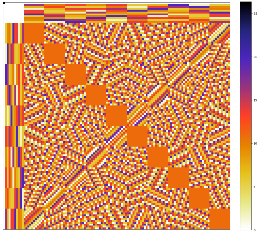
Open Butterfly ($q = 13$)

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 ($q = 11$)

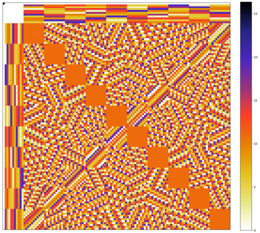
Open Flystel ($q = 13$)

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