From Algebraic Geometry to Linear Cryptanalysis

Application to Anemoi

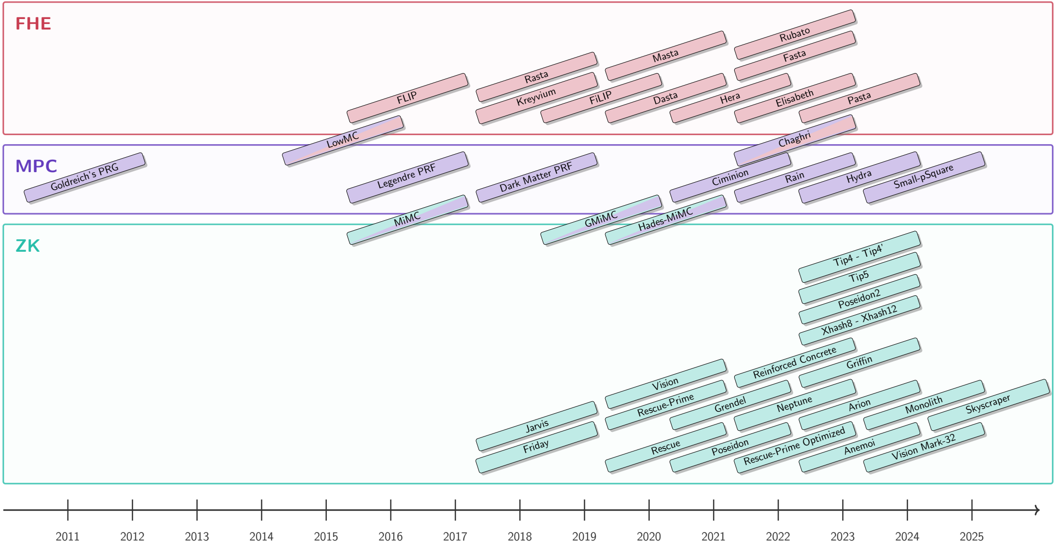
Clémence Bouvier

Université de Lorraine, CNRS, Inria, LORIA

(joint work with Tim Beyne)

ALPSY Workshop, Obergurgl, Austria
January 26th, 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 ✗
- ...

Linearity

Definition

Let $\mathrm{F} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ be a function and ω a primitive character. The **Walsh transform** for the character ω of the linear approximation (u, v) of F is given by

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

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

Linearity

Definition

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

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

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

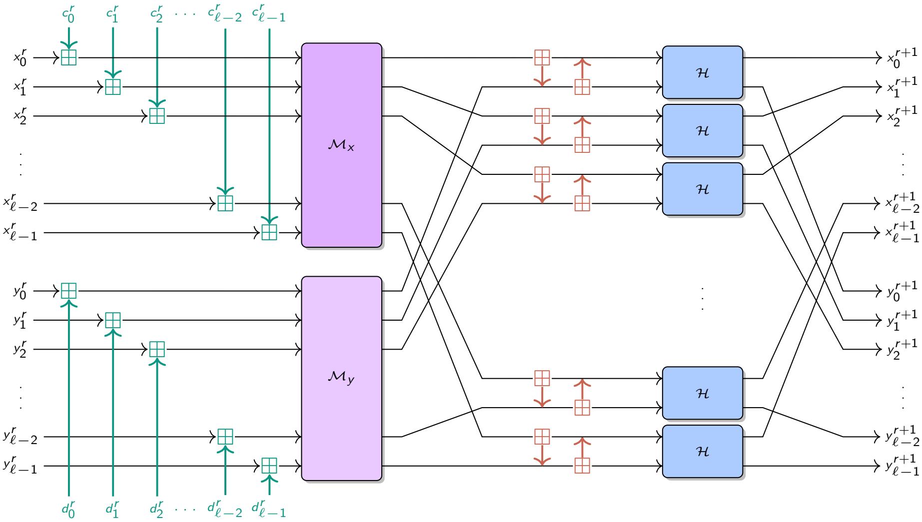
Definition

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

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

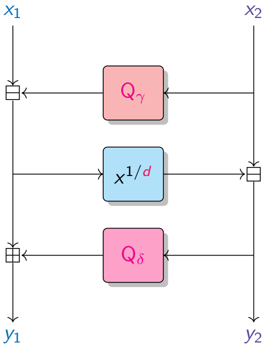
Anemoi round function

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

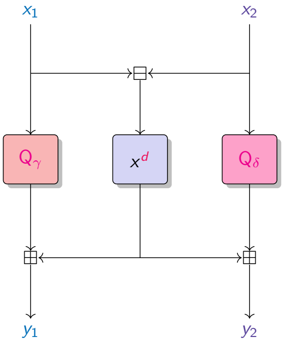


Flystel - Definition

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



Open variant.



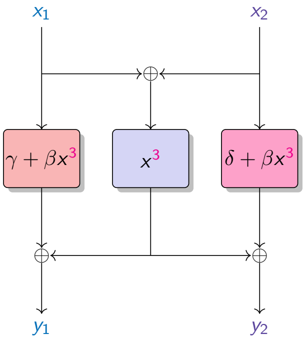
Closed variant.

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

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

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

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



Closed Flystel.

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

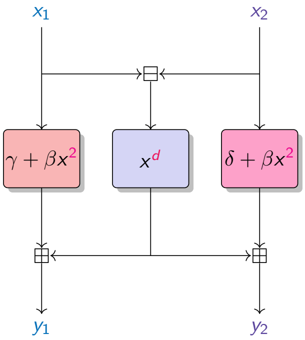
Bound

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].



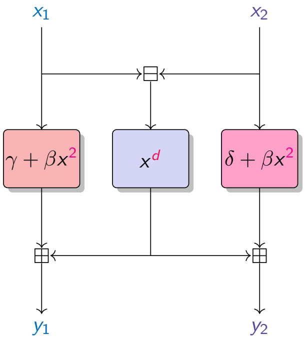
Closed Flystel.

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

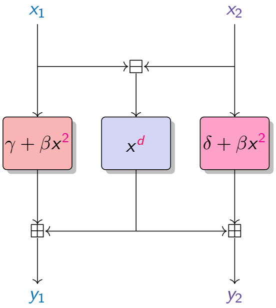
$$\mathcal{L}_f \leq (d-1)\sqrt{p}$$

Weil bound

Proposition [Weil, 1948]

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

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



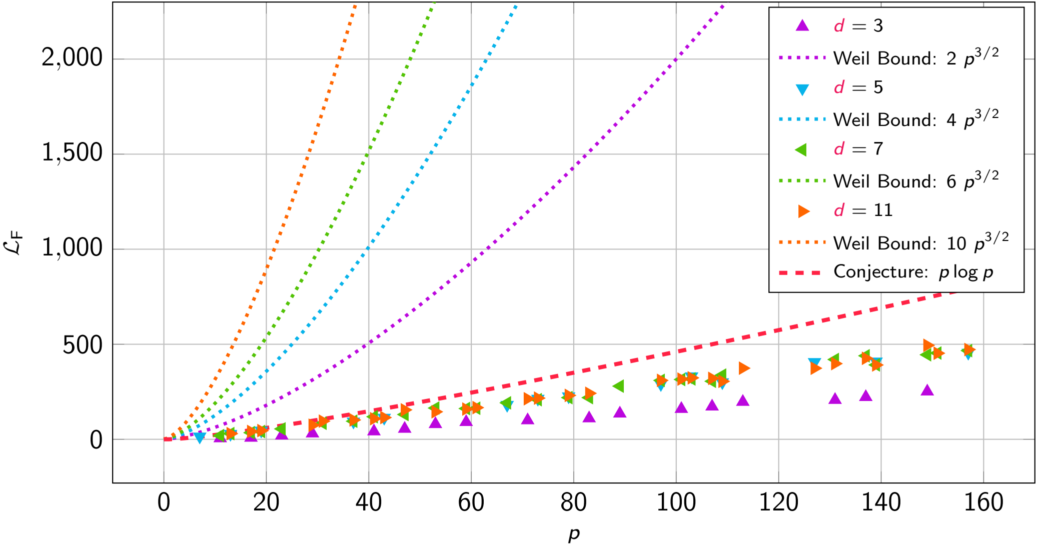
Closed Flystel.

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

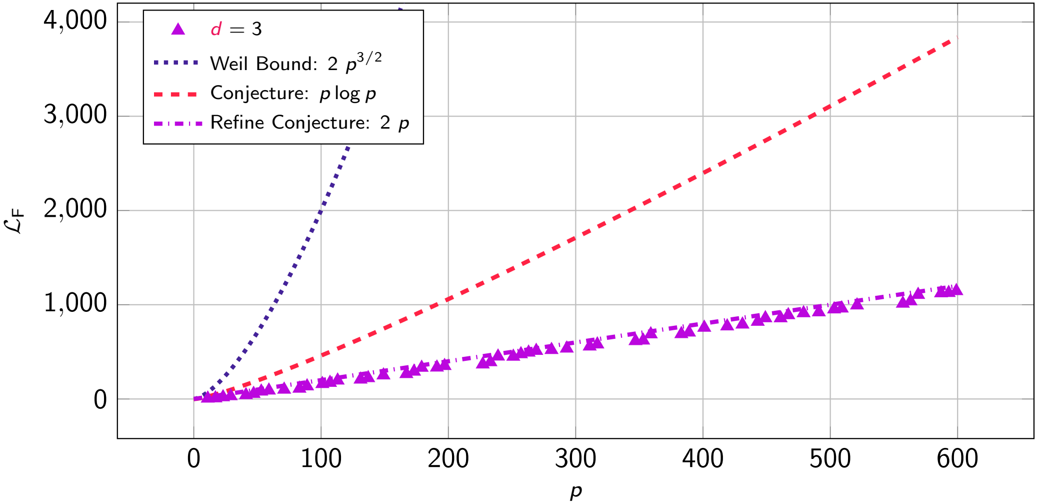
Conjecture

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

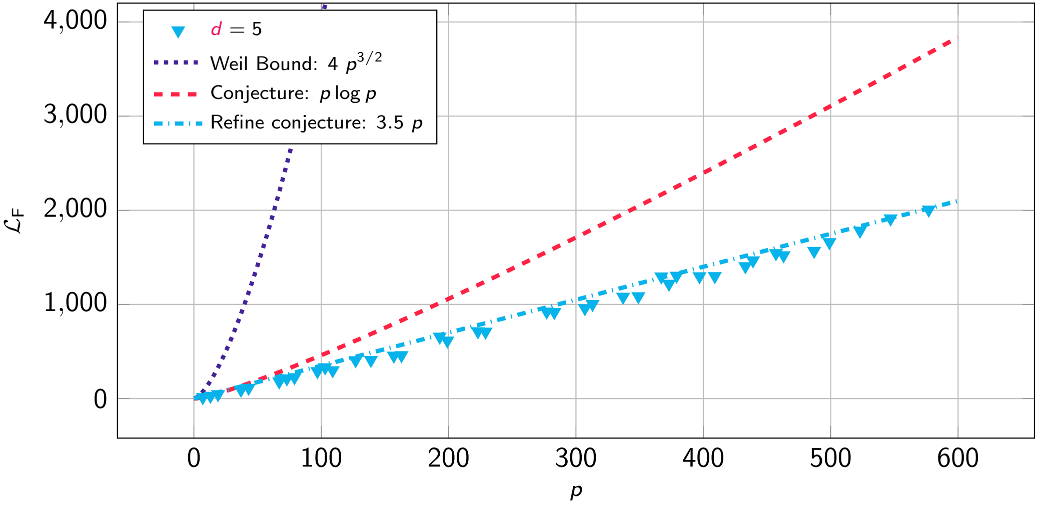
Experimental results



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.

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

This Talk:

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

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

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

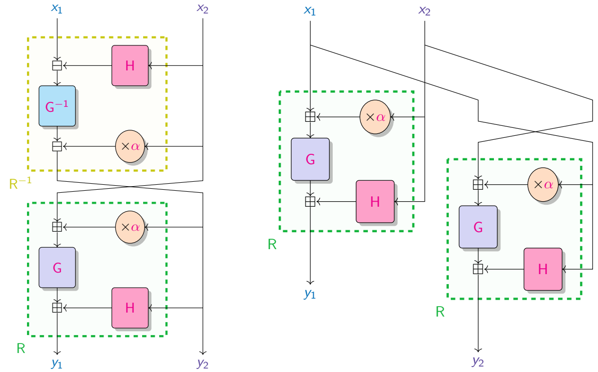
Generalizations of Weil bound

- ⋆ 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

Generalized Butterfly

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

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



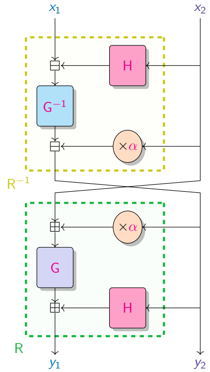
Open variant. *Closed variant.*

Generalized Butterfly

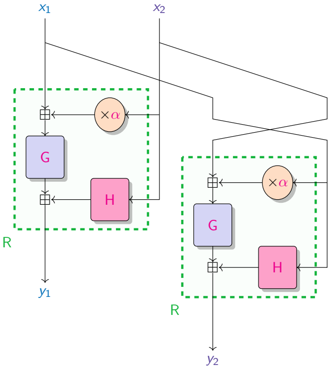
Originally introduced by [Perrin, Udovenko and Biryukov, 2016] over binary fields, $\mathbb{F}_{2^n}^2$, n odd.

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

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



Open variant.



Closed variant.

Deligne Bound

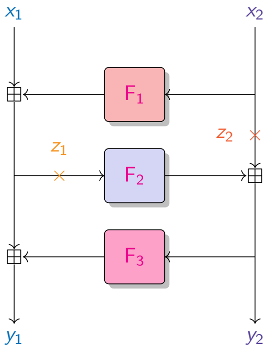
The hypersurface defined by $f_d = 0$ (the degree-d homogeneous component of f) is smooth so that

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

3-round Feistel

Let $\textsc{Feistel}[F_1, F_2, F_3]$ be a 3-round Feistel network with F_2 a permutation and $d_1 \geq d_3$ where

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



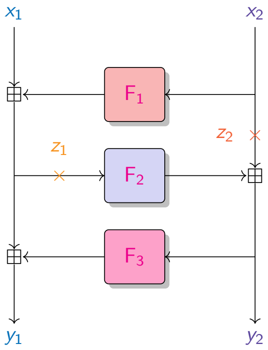
A 3-round Feistel.

3-round Feistel

Let $\textsc{Feistel}[F_1, F_2, F_3]$ be a 3-round Feistel network with F_2 a permutation and $d_1 \geq d_3$ where

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

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

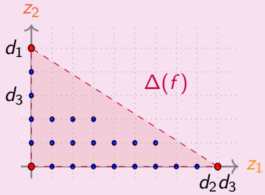


A 3-round Feistel.

Denef-Loeser Bound

f is commode and non-degenerate, with Newton number:

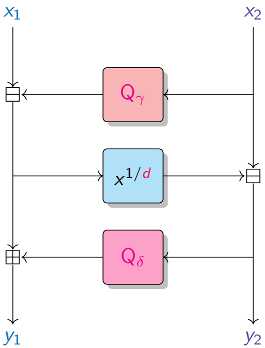
$$\nu(f) = (d_1 - 1)(d_2 d_3 - 1) \ .$$



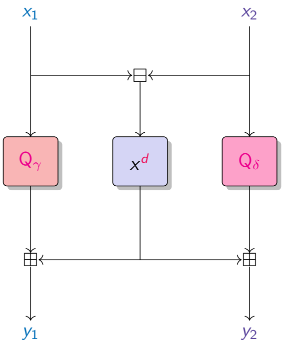
$$\boxed{\mathcal{L}_F \leq (d_1 - 1)(d_2 d_3 - 1) \cdot q}$$

Flystel - Definition

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



Open variant.



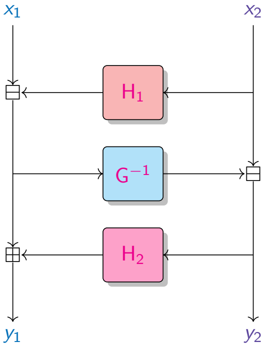
Closed variant.

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

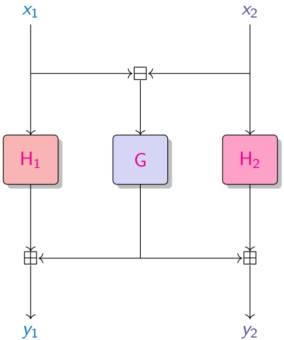
$$\begin{cases} y_1 &= (x_1 - x_2)^d + Q_\gamma(x_1) \\ y_2 &= (x_1 - x_2)^d + Q_\delta(x_2)\,. \end{cases}$$

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.

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

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

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 $\prod_{i=1}^{n} (\delta / w_i - 1)$

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 $f \in \mathbb{F}_q[x_1, \dots, x_n]$, 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** $\mu_1, \dots, \mu_s$,
- ⋆ 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 $f \in \mathbb{F}_q[x_1, \dots, x_n]$, 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** $\mu_1, \dots, \mu_s$,
- ⋆ the hypersurface defined by $f_{d'} = 0$ contains none of these singularities,

then we have

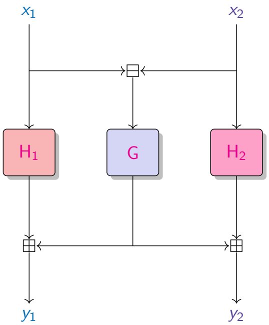
$$|S(f)| = \left| \sum_{x \in \mathbb{F}_q^n} \omega^{f(x)} \right| \leq \left((d-1)^n - (d-d') \sum_{i=1}^{s} \mu_i \right) \cdot q^{n/2} .$$

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

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 ($\deg \mathsf{G} > \deg \mathsf{H}_1, \deg \mathsf{H}_2$).

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

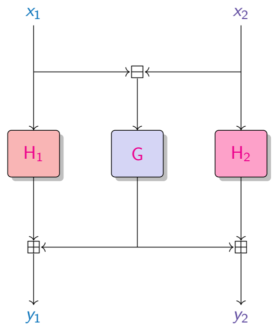


$$\begin{cases} y_1 &= \mathsf{G}(x_1 - x_2) + \mathsf{H}_1(x_1) \\ y_2 &= \mathsf{G}(x_1 - x_2) + \mathsf{H}_2(x_2)\,. \end{cases}$$

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 ($\deg \mathsf{G} > \deg \mathsf{H}_1, \deg \mathsf{H}_2$).

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



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

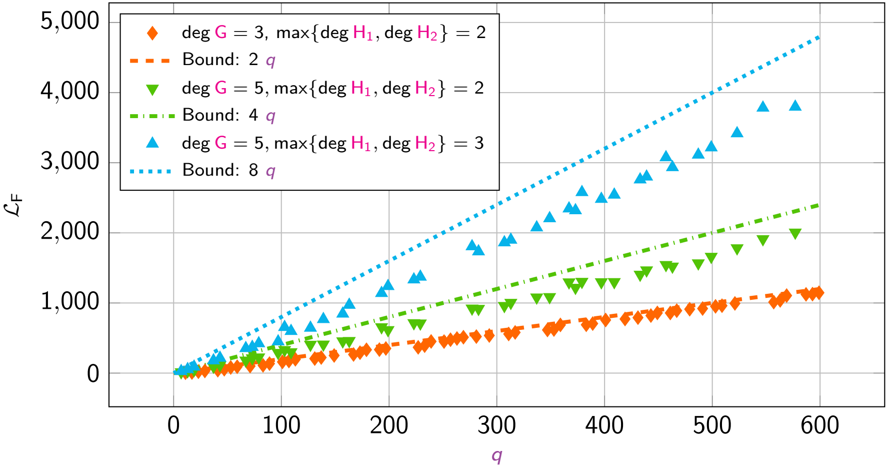
Linearity Bound

- ⋆ 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.

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

Generalized Flystel - Results

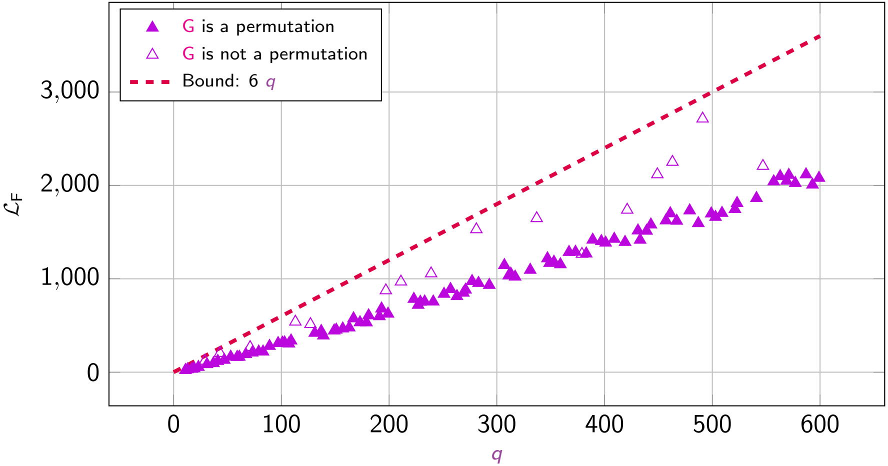
Let $F = \textsc{Flystel}[H_1, G, H_2]$ with H_1, G and H_2 monomials.



Low-degree permutations G, H_1 and H_2.

Generalized Flystel - Results

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

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

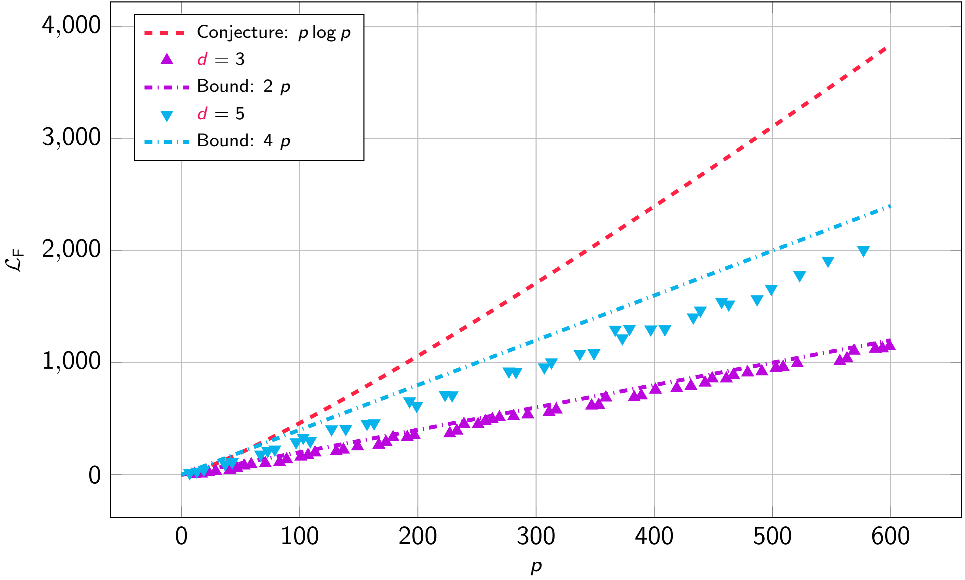
Conjecture proved for $d \leq \log p$

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

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

Solving conjecture



Cohomological framework

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

Cohomological framework

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

$$\Downarrow$$

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

$$\Downarrow$$

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

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

Cohomological framework

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

$$\Downarrow$$

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

$$\Downarrow$$

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

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

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

$$\Downarrow$$

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

$$\Downarrow$$

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

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.

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

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... for 3 important constructions
  - 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
- ⋆ 3 different results... for 3 important constructions
  - ⋆ 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

Conclusions

- Bounds on exponential sums have direct application to linear cryptanalysis
- 3 different results... for 3 important constructions
  - 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

Contribute to the cryptanalysis efforts for AOP.

Conclusions

- ⋆ Bounds on exponential sums have direct application to linear cryptanalysis
- ⋆ 3 different results... for 3 important constructions
  - ⋆ 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

Contribute to the cryptanalysis efforts for AOP.

Thank you