A Guided Tour through the Jungle of Arithmetization-Oriented Primitives

PART 2

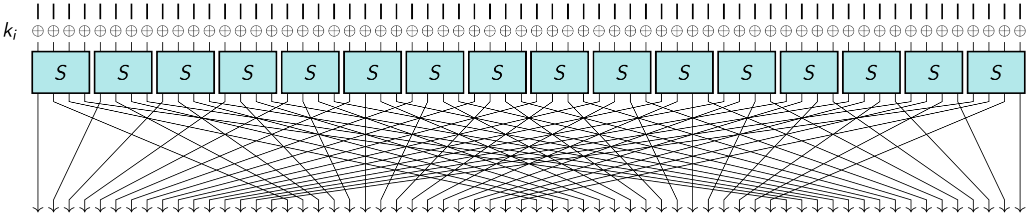
Clémence Bouvier

Université de Lorraine, CNRS, Inria, LORIA

SAC Summer School, Toronto, Canada
August 12th, 2025

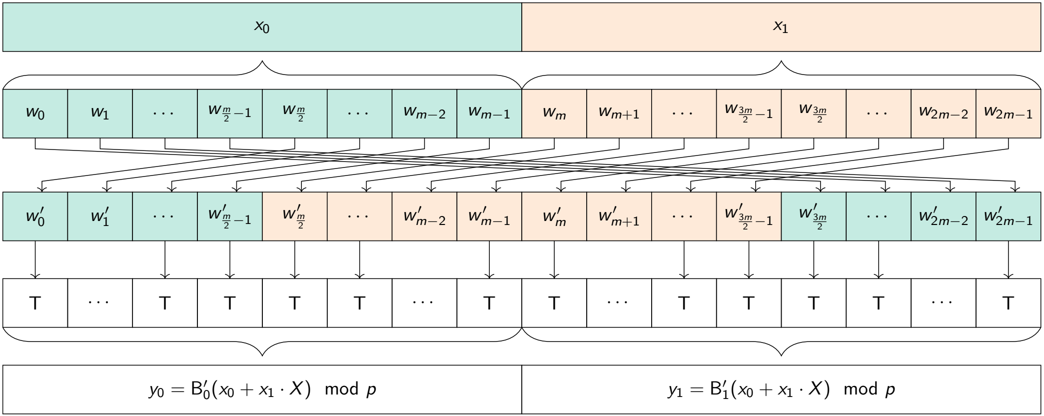
Classical design

Present round function



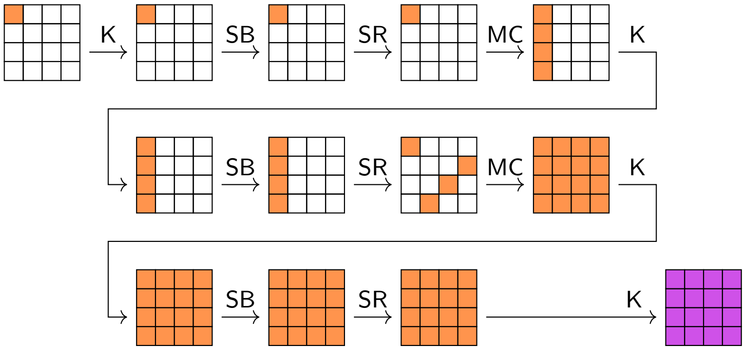
Design of AOPs

Skyscraper Bar layer



Classical cryptanalysis

AES square attack



Cryptanalysis of AOPs

Anemoi linear analysis

Theorem [Rojas-León, 2006]

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

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

If the following conditions are satisfied

- ⋆ the hypersurface defined by $f_d = 0$ has at worst **quasi-homogeneous isolated singularities** of degrees prime to p with **Milnor numbers** $\mu_1, \ldots, \mu_s$,
- ⋆ the hypersurface defined by $f_{d'} = 0$ contains none of these singularities,

then we have

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

Outline

PART 1

- ⋆ General Introduction

- ⋆ Advanced Protocols

- ⋆ New AOPs

- ⋆ Computing constraints

PART 2

- ⋆ Design of AOPs

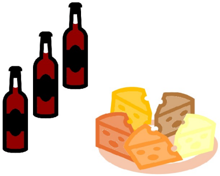
- ⋆ Algebraic Cryptanalysis

- ⋆ Other attacks

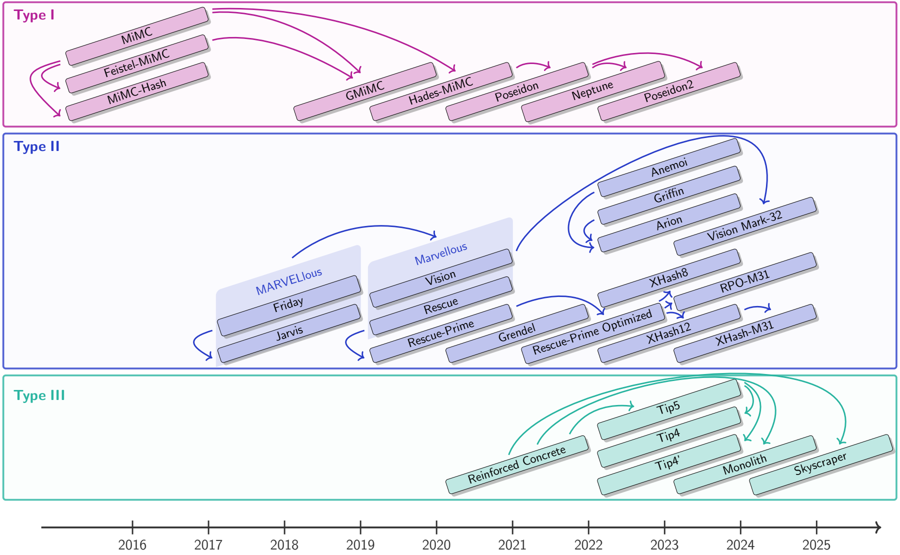
New AOPs

Many (many) designs

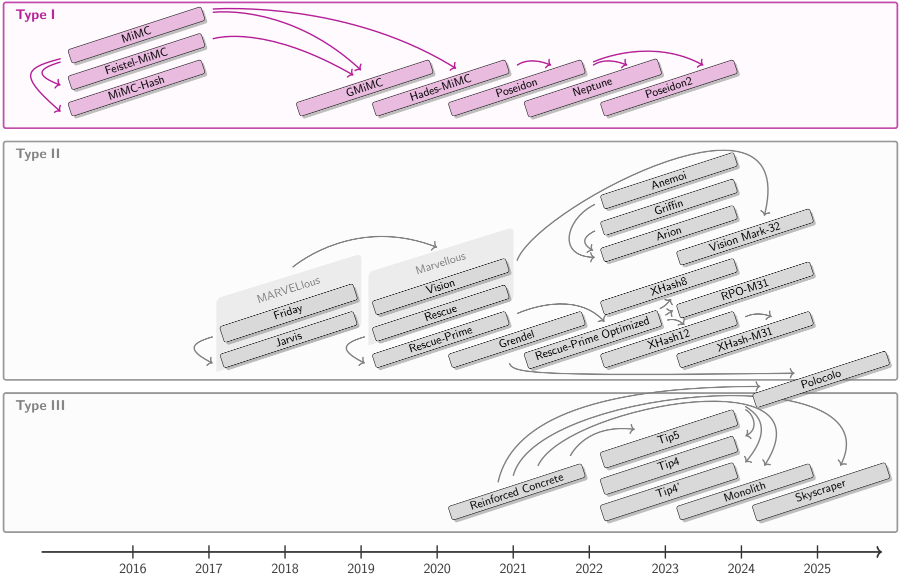
How to classify them ?



ZKP Primitives overview

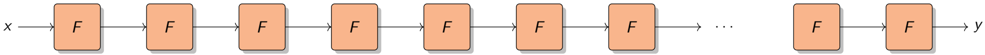


ZKP Primitives overview



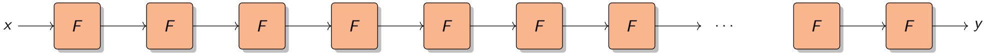
Type I

Low-Degree Primitives



Type I

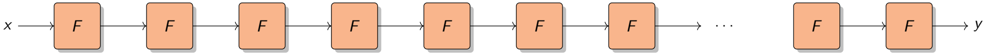
Low-Degree Primitives



Degree	5	5^2	5^3	5^4	5^5	5^6	5^7	5^{79}	5^{80}

Type I

Low-Degree Primitives

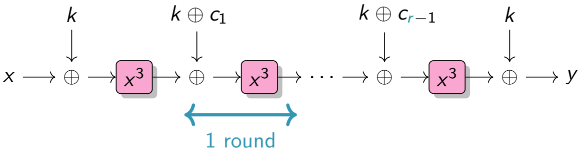


Degree	5	5^2	5^3	5^4	5^5	5^6	5^7	5^{79}	5^{80}
Constraints	3	3×2	3×3	3×4	3×5	3×6	3×7	3×79	3×80

MiMC / Feistel-MiMC

M. Albrecht, L. Grassi, C. Rechberger, A. Roy and T. Tiessen, 2016

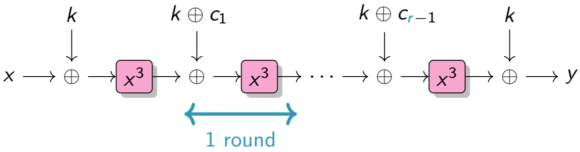
- ⋆ n-bit blocks (n odd ≈ 129) : $x \in \mathbb{F}_{2^n}$
- ⋆ n-bit key : $k \in \mathbb{F}_{2^n}$
- ⋆ 82 rounds when $n = 129$

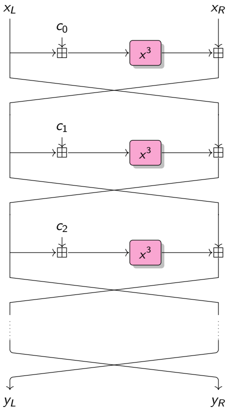


MiMC / Feistel-MiMC

M. Albrecht, L. Grassi, C. Rechberger, A. Roy and T. Tiessen, 2016

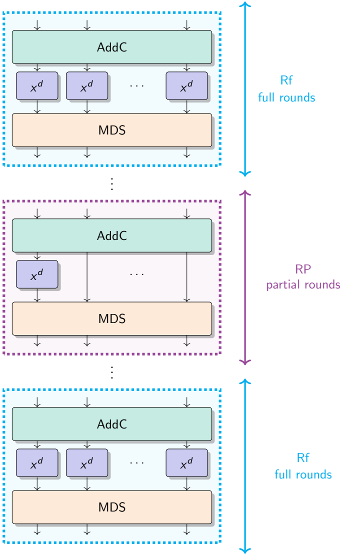
- n-bit blocks (n odd ≈ 129) : $x \in \mathbb{F}_{2^n}$
- n-bit key : $k \in \mathbb{F}_{2^n}$
- 82 rounds when $n = 129$





Feistel-MiMC

Poseidon



L. Grassi, D. Khovratovich, C. Rechberger, A. Roy and M. Schofnegger, 2021

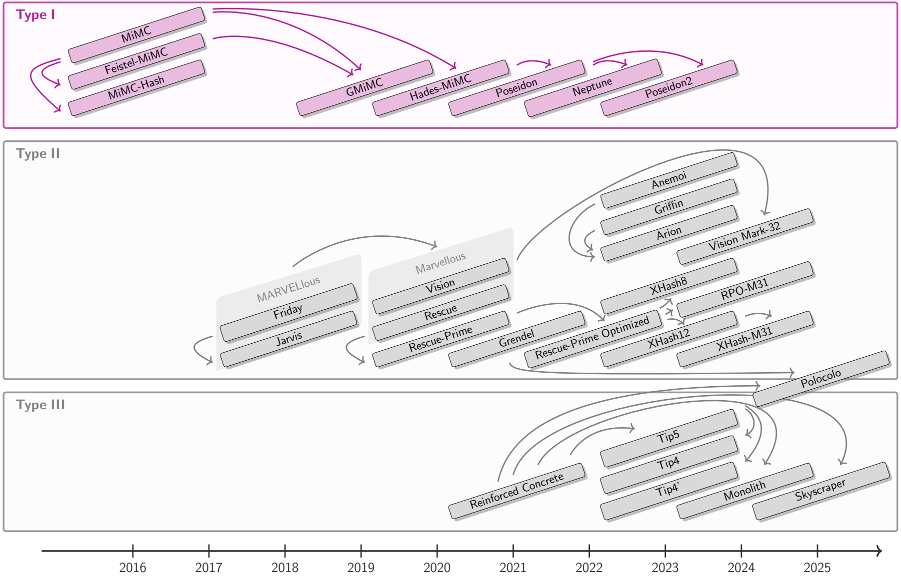
- ⋆ S-box :

$$x \mapsto x^3$$

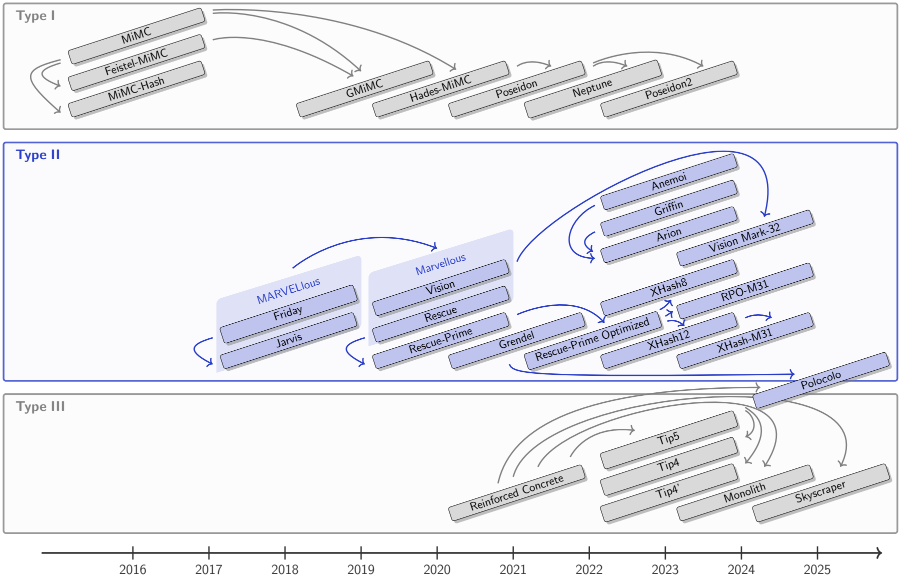
- ⋆ Nb rounds :

$$\begin{aligned} R &= 2 \times Rf + RP \\ &= 8 + (\text{from } 56 \text{ to } 84) \end{aligned}$$

ZKP Primitives overview

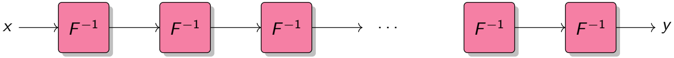


ZKP Primitives overview



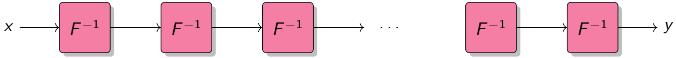
Type II

Primitives based on Equivalence



Type II

Primitives based on Equivalence



Degree	5^{-1}	5^{-2}	5^{-3}		5^{-19}	5^{-20}

Example

In $\mathbb{F}_p$ with

$$p = \texttt{0x73eda753299d7d483339d80809a1d80553bda402fffe5bfeffffffff00000001}$$

If $F(x) = x^5$ then $F^{-1}(x) = x^{5^{-1}}$ with

$$5^{-1} = \texttt{0x2e5f0fbadd72321ce14a56699d73f002217f0e679998f19933333332cccccccd}$$

Type II

Primitives based on Equivalence

$$x \longrightarrow \boxed{F^{-1}} \longrightarrow \boxed{F^{-1}} \longrightarrow \boxed{F^{-1}} \longrightarrow \cdots \quad \boxed{F^{-1}} \longrightarrow \boxed{F^{-1}} \longrightarrow y$$

Degree	5^{-1}	5^{-2}	5^{-3}	5^{-19}	5^{-20}
Constraints	3×20	3×19	3×18	3×2	3

Example

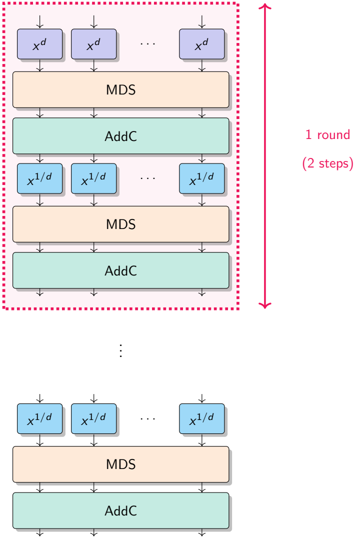
In $\mathbb{F}_p$ with

$$p = \texttt{0x73eda753299d7d483339d80809a1d80553bda402fffe5bfeffffffff00000001}$$

If $F(x) = x^5$ then $F^{-1}(x) = x^{5^{-1}}$ with

$$5^{-1} = \texttt{0x2e5f0fbadd72321ce14a56699d73f002217f0e679998f19933333332cccccccd}$$

Rescue / Rescue-Prime



A. Aly, T. Ashur, E. Ben-Sasson, S. Dhooghe and A. Szepieniec, 2020

- ⋆ S-box :

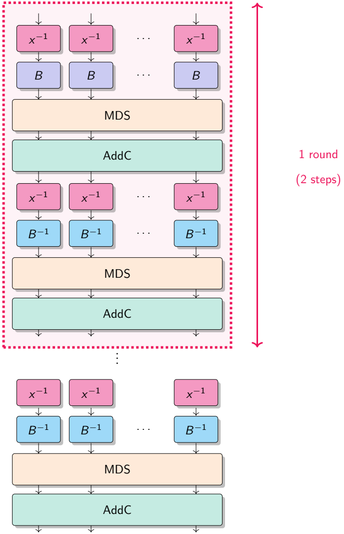
$$x \mapsto x^3 \quad \text{and} \quad x \mapsto x^{1/3}$$

- ⋆ Nb rounds :

$$R = \text{from 8 to 26}$$

(2 S-boxes per round)

Vision



A. Aly, T. Ashur, E. Ben-Sasson, S. Dhooghe and A. Szepieniec, 2020

⋆ S-box :

$$x \mapsto B(x^{-1}) \quad \text{and} \quad x \mapsto B^{-1}(x^{-1})$$

where B is an $\mathbb{F}_2$-linearized affine polynomial

$$B(x) = b_{-1} + \sum_{i=0}^{n-1} b_i x^{2^i}$$

of univariate degree 4.

Anemoi

Need : verification using few multiplications.

⋆ **First approach :** evaluation using few multiplications, e.g. Poseidon [GKRRS21]

$\boxed{y \leftarrow E(x)}$ $\rightsquigarrow E$: low degree

$\boxed{y == E(x)}$ $\rightsquigarrow E$: low degree

Anemoi

Need : verification using few multiplications.

⋆ **First approach :** evaluation using few multiplications, e.g. Poseidon [GKRRS21]

$\boxed{y \leftarrow E(x)}$ $\rightsquigarrow E$: low degree

$\boxed{y == E(x)}$ $\rightsquigarrow E$: low degree

⋆ **Rescue breakthrough :** using inversion, e.g. Rescue [AABDS20]

$\boxed{y \leftarrow E(x)}$ $\rightsquigarrow E$: high degree

$\boxed{x == E^{-1}(y)}$ $\rightsquigarrow E^{-1}$: low degree

Anemoi

Need : verification using few multiplications.

- ⋆ **First approach :** evaluation using few multiplications, e.g. Poseidon [GKRRS21]

$\boxed{y \leftarrow E(x)}$ $\rightsquigarrow E$: low degree $\boxed{y == E(x)}$ $\rightsquigarrow E$: low degree

- ⋆ **Rescue breakthrough :** using inversion, e.g. Rescue [AABDS20]

$\boxed{y \leftarrow E(x)}$ $\rightsquigarrow E$: high degree $\boxed{x == E^{-1}(y)}$ $\rightsquigarrow E^{-1}$: low degree

- ⋆ **Anemoi approach :** using $(u, v) = \mathcal{L}(x, y)$, where $\mathcal{L}$ is linear

$\boxed{y \leftarrow F(x)}$ $\rightsquigarrow F$: high degree $\boxed{v == G(u)}$ $\rightsquigarrow G$: low degree

CCZ-equivalence

Inversion

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

Noting that

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

then, we have :

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

CCZ-equivalence

Inversion

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

Noting that

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

then, we have :

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

Definition [Carlet, Charpin and Zinoviev, DCC98]

$F : \mathbb{F}_q \to \mathbb{F}_q$ and $G : \mathbb{F}_q \to \mathbb{F}_q$ are **CCZ-equivalent** if

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

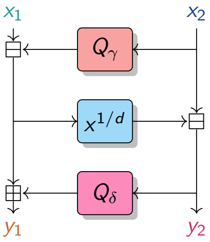
The Flystel

C. Bouvier, P. Briaud, P. Chaidos, L. Perrin, R. Salen, V. Velichkov and D. Willems, 2023

Butterfly + Feistel $\Rightarrow$ Flystel

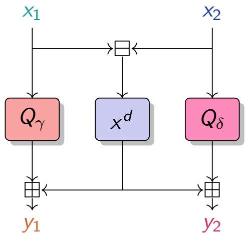
A 3-round Feistel-network with
$Q_\gamma : \mathbb{F}_q \rightarrow \mathbb{F}_q$ and $Q_\delta : \mathbb{F}_q \rightarrow \mathbb{F}_q$ two quadratic functions, and $E : \mathbb{F}_q \rightarrow \mathbb{F}_q$ a permutation

High-Degree permutation



Open Flystel $\mathcal{H}$.

Low-Degree function



Closed Flystel $\mathcal{V}$.

The Flystel

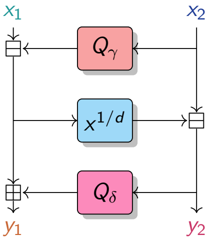
C. Bouvier, P. Briaud, P. Chaidos, L. Perrin, R. Salen, V. Velichkov and D. Willems, 2023

$\boxed{\text{Butterfly} + \text{Feistel} \Rightarrow \text{Flystel}}$

A 3-round Feistel-network with

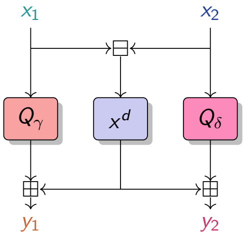
$Q_\gamma : \mathbb{F}_q \rightarrow \mathbb{F}_q$ and $Q_\delta : \mathbb{F}_q \rightarrow \mathbb{F}_q$ two quadratic functions, and $E : \mathbb{F}_q \rightarrow \mathbb{F}_q$ a permutation

High-Degree permutation



Open Flystel $\mathcal{H}$.

Low-Degree function



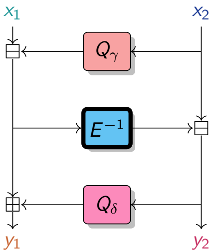
Closed Flystel $\mathcal{V}$.

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

Advantage of CCZ-equivalence

⋆ High-Degree Evaluation.

High-Degree
permutation



Open Flystel $\mathcal{H}$.

Example

if $E : x \mapsto x^5$ in $\mathbb{F}_p$ where

$$p = \texttt{0x73eda753299d7d483339d80809a1d805}$$
$$\texttt{53bda402fffe5bfeffffffff00000001}$$

then $E^{-1} : x \mapsto x^{5^{-1}}$ where

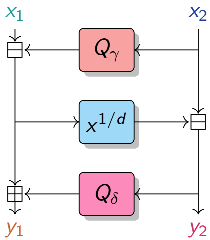
$$5^{-1} = \texttt{0x2e5f0fbadd72321ce14a56699d73f002}$$
$$\texttt{217f0e679998f19933333332cccccccd}$$

Advantage of CCZ-equivalence

- ⋆ High-Degree Evaluation.
- ⋆ Low-Degree Verification.

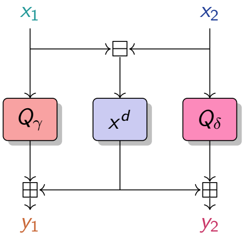
$$\boxed{(y_1, y_2) == \mathcal{H}(x_1, x_2) \Leftrightarrow (x_1, y_1) == \mathcal{V}(x_2, y_2)}$$

High-Degree permutation



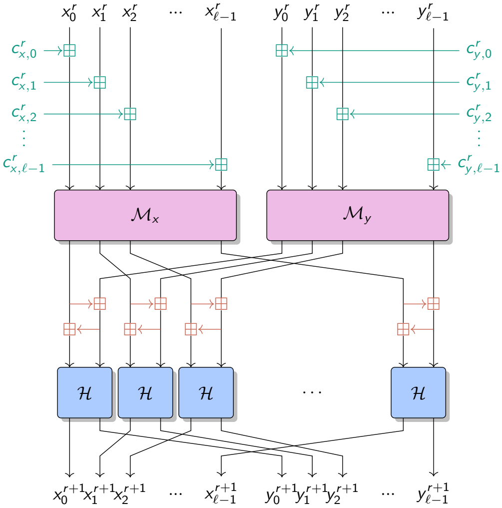
Open Flystel $\mathcal{H}$.

Low-Degree function

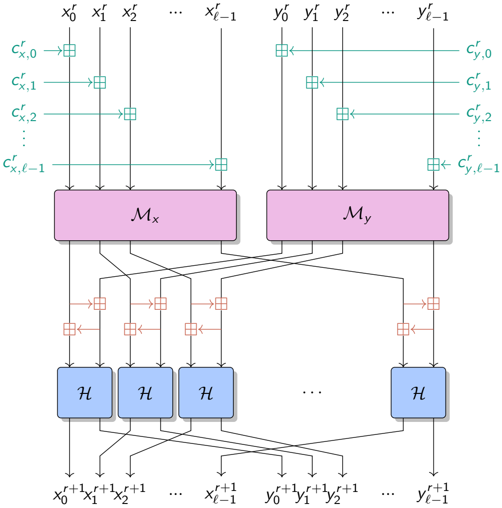


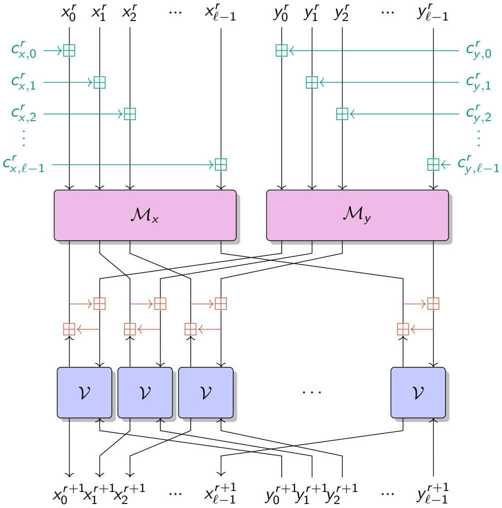
Closed Flystel $\mathcal{V}$.

The SPN Structure

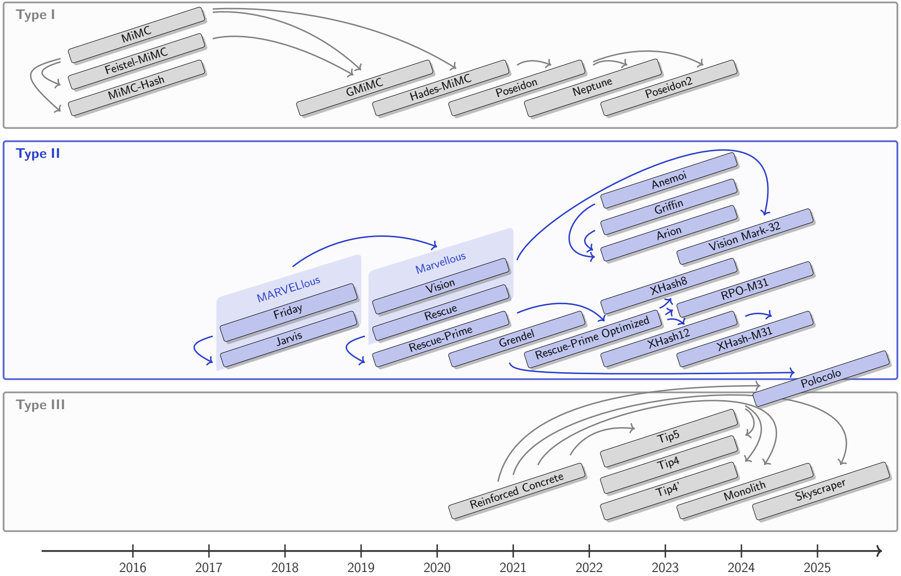


The SPN Structure

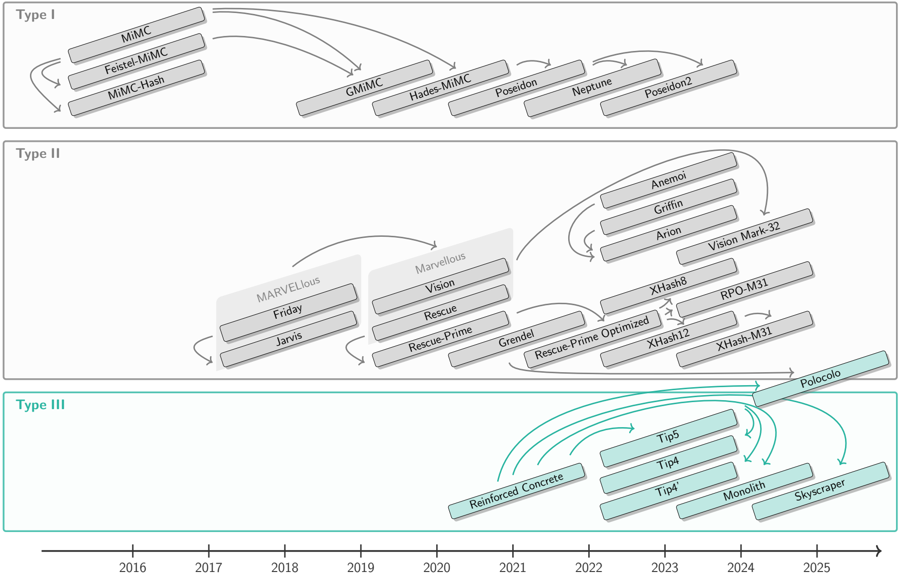




ZKP Primitives overview

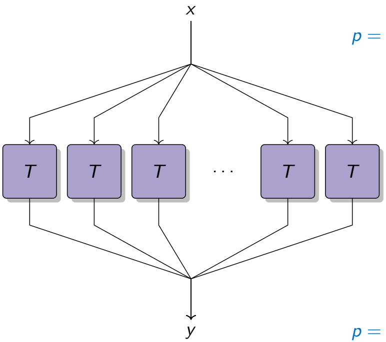


ZKP Primitives overview



Type III

Primitives using Look-up-Tables

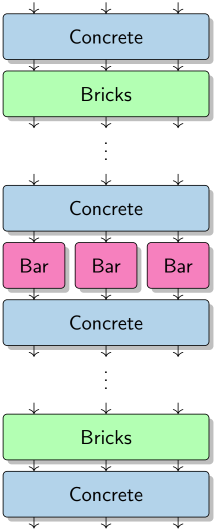


$\mathbb{F}_p$ with
$p =$ `0x73eda753299d7d483339d80809a1d80553bda402fffe5bfeffffffff00000001`

$\mathbb{F}_2^8$
$(0,0,0,0,0,0,0,0) \ \dots \ (1,1,1,1,1,1,1,1)$

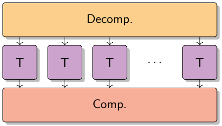
$\mathbb{F}_p$ with
$p =$ `0x73eda753299d7d483339d80809a1d80553bda402fffe5bfeffffffff00000001`

Reinforced Concrete



L. Grassi, D. Khovratovich, R. Lüftenegger, C. Rechberger, M. Schofnegger and R. Walch, 2022

⋆ S-box :

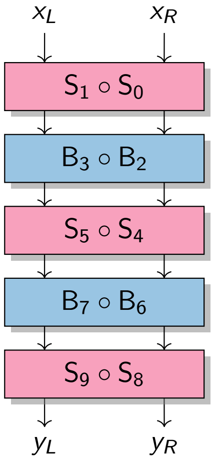


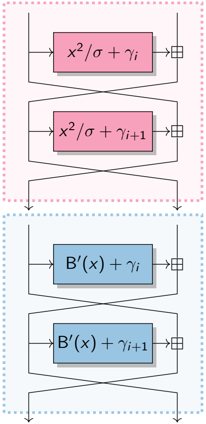
⋆ Nb rounds :

$$R = 7$$

Skyscraper

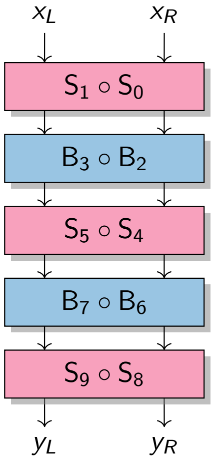
C. Bouvier, L. Grassi, D. Khovratovich, K. Koschatko, C. Rechberger, F. Schmid and M. Schofnegger, 2025

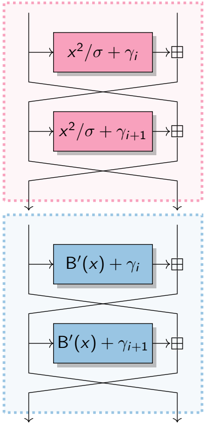


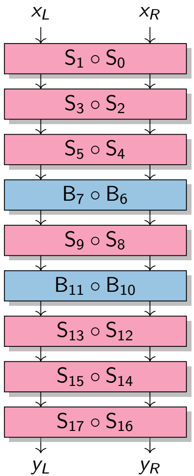


Skyscraper

C. Bouvier, L. Grassi, D. Khovratovich, K. Koschatko, C. Rechberger, F. Schmid and M. Schofnegger, 2025







Summary

	Type I Low-degree primitives	Type II Equivalence relation	Type III Look-up tables
Alphabet	$\mathbb{F}_q^m$ for various q and m	$\mathbb{F}_q^m$ for various q and m	specific fields
Nb of rounds	many	few	fewer
Plain performance	fast	slow	faster
Nb of constraints	often more	fewer	it depends on the proof system
Examples	Feistel-MiMC Poseidon	Rescue Anemoi	Reinforced Concrete Skyscraper

QUIZ ! !

- To which type of primitives (I, II, or III) does AES belong ?
- A look-up table is a form of CCZ equivalence. True or False ?
- Low degree primitives are the ones for which we have less cryptanalysis. True or False ?

Take-away

Design techniques of AOPs

- ⋆ Type I : low degree primitives
- ⋆ Type II : primitives based on equivalence relations
- ⋆ Type III : look-up tables based primitives

"N'en faisons pas tout un fromage !"

Algebraic Attacks

Some definitions

Tricks to reduce complexity

Importance of the modelisation

CICO Problem

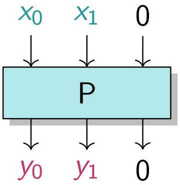
CICO : Constrained Input Constrained Output

Definition

Let $P : \mathbb{F}_q^t \rightarrow \mathbb{F}_q^t$ and $u < t$.

The **CICO** problem is :

$$\text{Finding } X, Y \in \mathbb{F}_q^{t-u} \text{ s.t. } P(X, 0^u) = (Y, 0^u).$$



when $t = 3,\ u = 1.$

Need to solve polynomial systems

Solving polynomial systems

⋆ **Univariate** solving : find the roots of $\mathcal{P}_j \in \mathbb{F}_q[X]$

$$\begin{cases} \mathcal{P}_0(X) & = 0 \\ & \vdots \\ \mathcal{P}_{m-1}(X) & = 0 \ . \end{cases}$$

Solving polynomial systems

⋆ **Univariate** solving : find the roots of $\mathcal{P}_j \in \mathbb{F}_q[X]$

$$\begin{cases} \mathcal{P}_0(X) & = 0 \\ & \vdots \\ \mathcal{P}_{m-1}(X) & = 0 \ . \end{cases}$$

⋆ **Multivariate** solving : find the roots of $\mathcal{P}_j \in \mathbb{F}_q[X_0, \ldots, X_{n-1}]$

$$\begin{cases} \mathcal{P}_0(X_0, \ldots, X_{n-1}) & = 0 \\ & \vdots \\ \mathcal{P}_{m-1}(X_0, \ldots, X_{n-1}) & = 0 \ . \end{cases}$$

Euclidean division

⋆ Integers

$$a = q \times b + r,\ 0 \leq r < b$$

Example : division of 2025 by 100

$$2025 = 20 \times 100 + 25$$

Euclidean division

⋆ Integers

$$a = q \times b + r,\ 0 \leq r < b$$

Example : division of 2025 by 100

$$2025 = 20 \times 100 + 25$$

⋆ Univariate polynomials

$$A = Q \times B + R,\ 0 \leq \deg(R) < \deg(B)$$

Example : division of $X^5 + 2X^3 + 3X$ by X^2

$$X^5 + 2X^3 + 3X = (X^3 + 2X) \times X^2 + 3X$$

Euclidean division

⋆ Integers

$$a = q \times b + r,\ 0 \leq r < b$$

Example : division of 2025 by 100

$$2025 = 20 \times 100 + 25$$

⋆ Univariate polynomials

$$A = Q \times B + R,\ 0 \leq \deg(R) < \deg(B)$$

Example : division of $X^5 + 2X^3 + 3X$ by X^2

$$X^5 + 2X^3 + 3X = (X^3 + 2X) \times X^2 + 3X$$

⋆ Multivariate polynomials

Euclidean division

⋆ Integers

$$a = q \times b + r, \; 0 \leq r < b$$

Example : division of 2025 by 100

$$2025 = 20 \times 100 + 25$$

⋆ Univariate polynomials

$$A = Q \times B + R, \; 0 \leq \deg(R) < \deg(B)$$

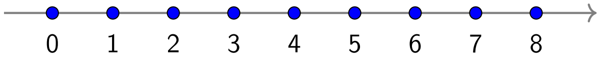
Example : division of $X^5 + 2X^3 + 3X$ by X^2

$$X^5 + 2X^3 + 3X = (X^3 + 2X) \times X^2 + 3X$$

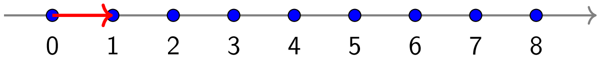
⋆ Multivariate polynomials

$$\boxed{\text{Need monomial ordering}}$$

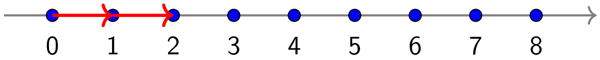
Monomial ordering



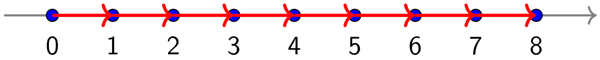
Monomial ordering



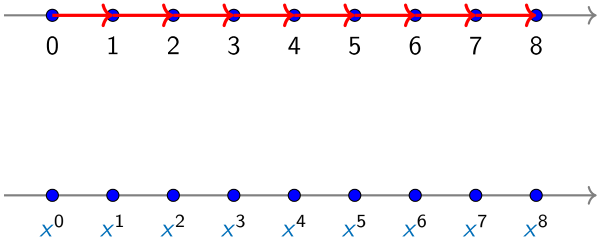
Monomial ordering



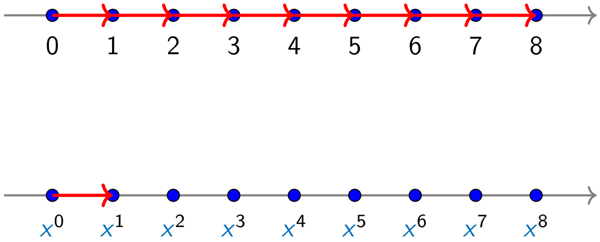
Monomial ordering



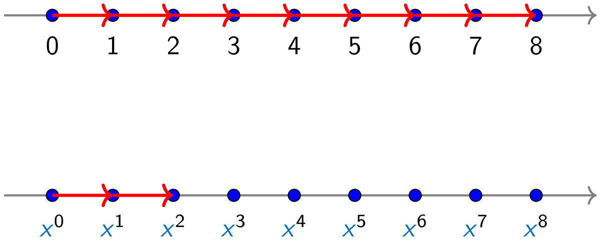
Monomial ordering



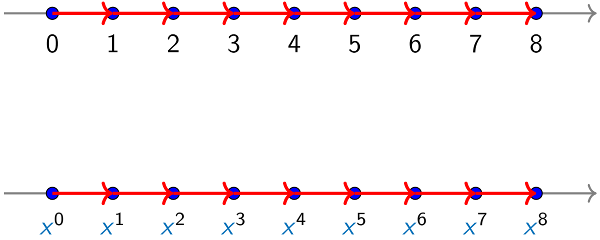
Monomial ordering



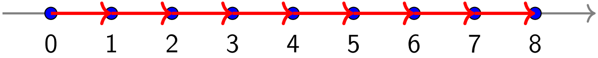
Monomial ordering

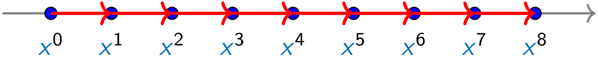


Monomial ordering



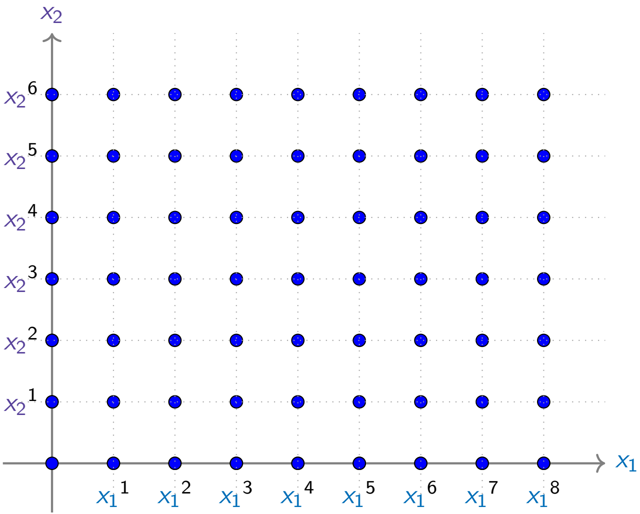
Monomial ordering





What about the multivariate case ?

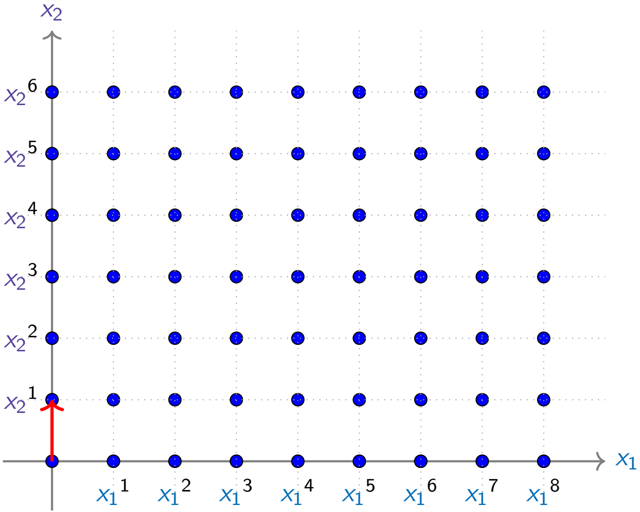
Lexicographical ordering



Order : x_1 is greater than any power of x_2.

$$x_1 > {x_2}^n$$

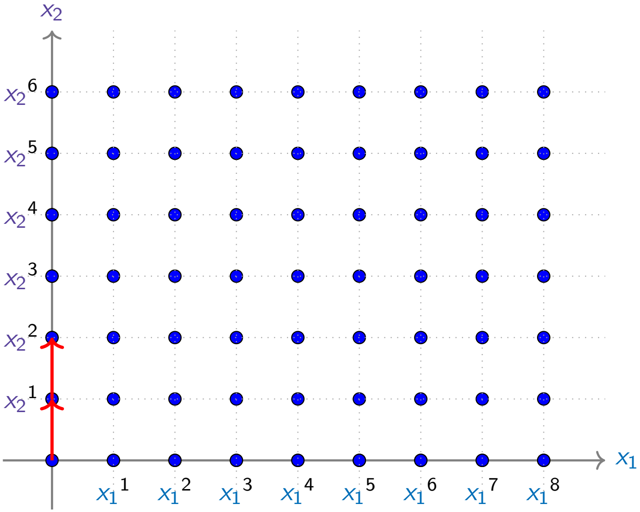
Lexicographical ordering



Order : x_1 is greater than any power of x_2.

$$x_1 > {x_2}^n$$

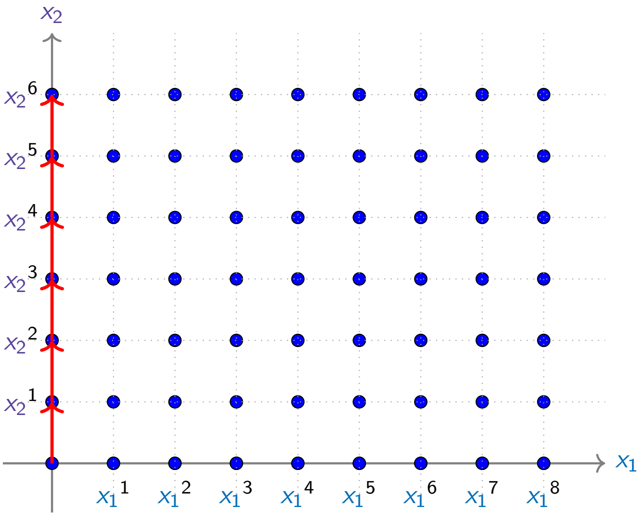
Lexicographical ordering



Order : x_1 is greater than any power of x_2.

$$x_1 > x_2{}^n$$

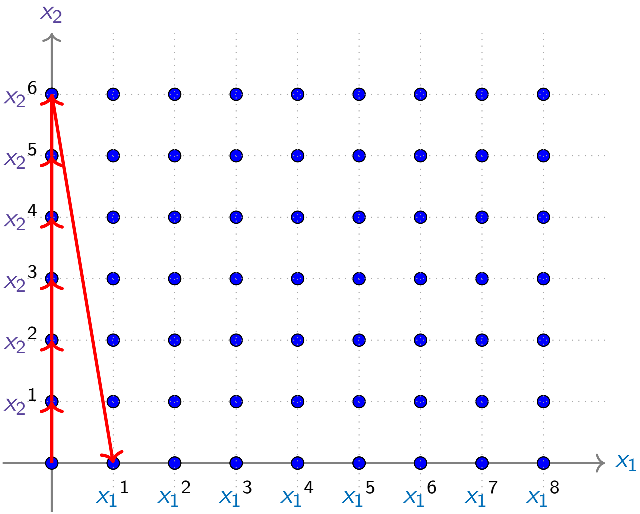
Lexicographical ordering



Order : x_1 is greater than any power of x_2.

$$x_1 > x_2{}^n$$

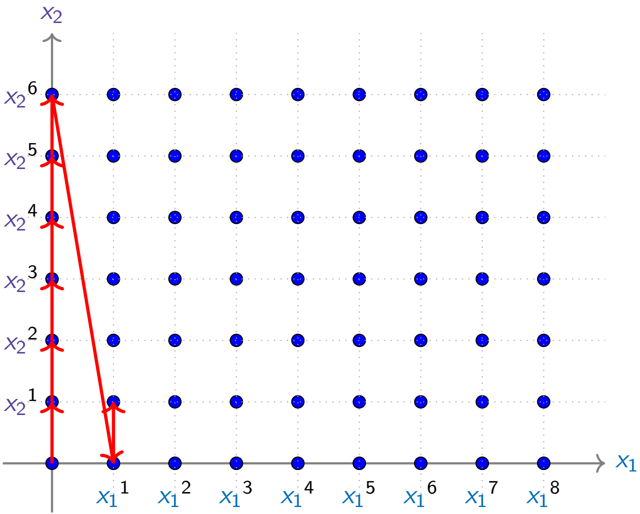
Lexicographical ordering



Order : x_1 is greater than any power of x_2.

$$x_1 > x_2{}^n$$

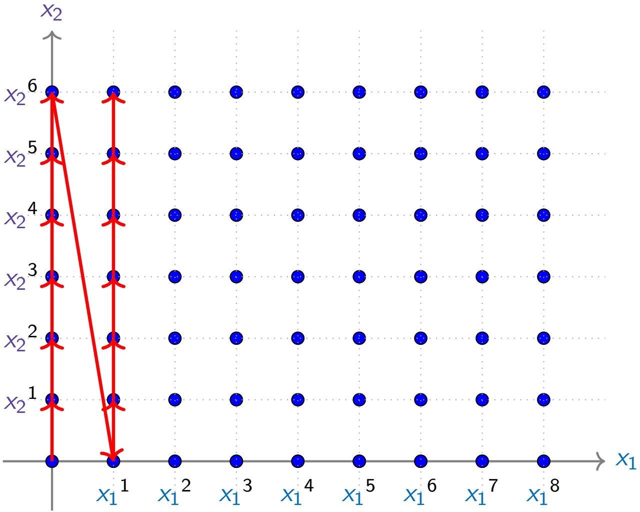
Lexicographical ordering



Order : x_1 is greater than any power of x_2.

$$x_1 > {x_2}^n$$

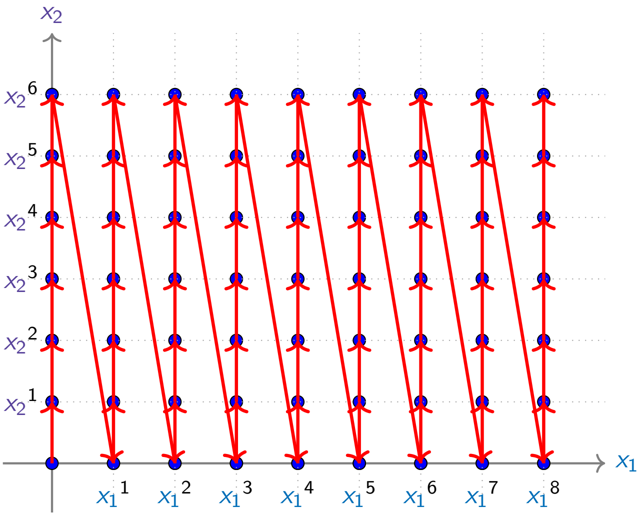
Lexicographical ordering



Order : x_1 is greater than any power of x_2.

$$x_1 > x_2{}^n$$

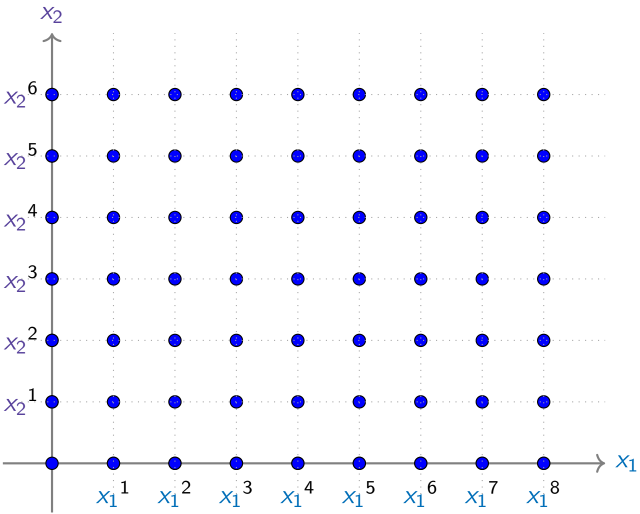
Lexicographical ordering



Order : x_1 is greater than any power of x_2.

$$x_1 > {x_2}^n$$

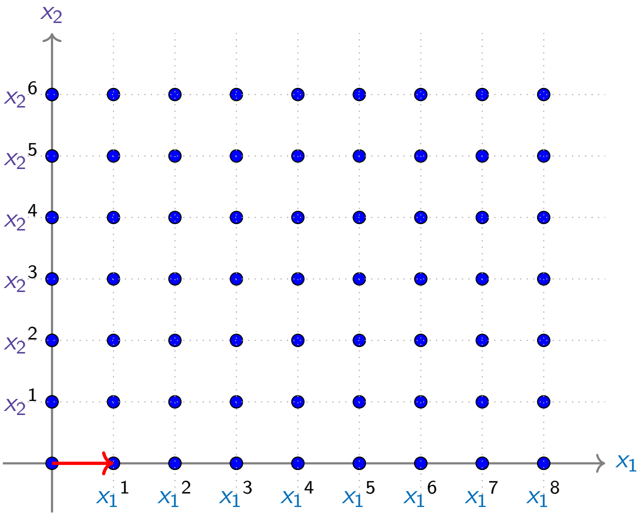
Reverse lex. ordering



Order : x_2 is greater than any power of x_1.

$$x_2 > {x_1}^n$$

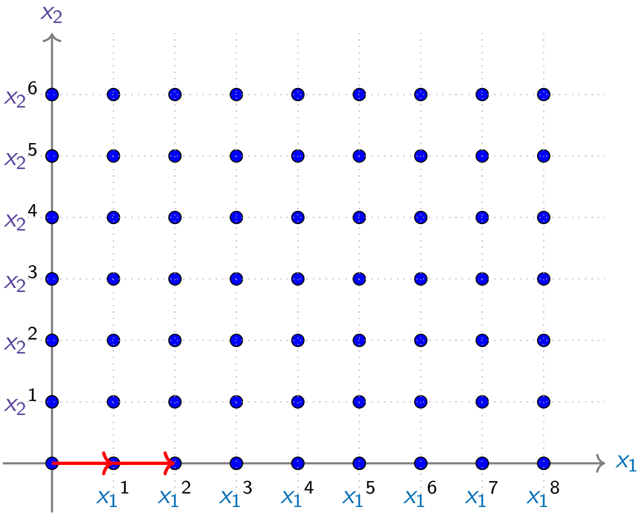
Reverse lex. ordering



Order : x_2 is greater than any power of x_1.

$$x_2 > x_1{}^n$$

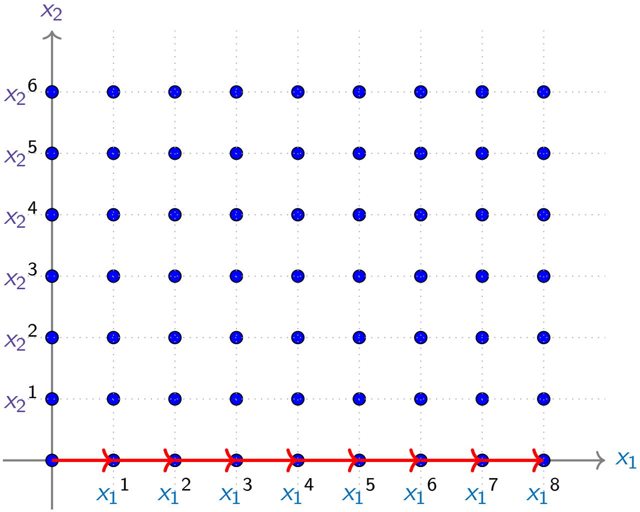
Reverse lex. ordering



Order : x_2 is greater than any power of x_1.

$$x_2 > {x_1}^n$$

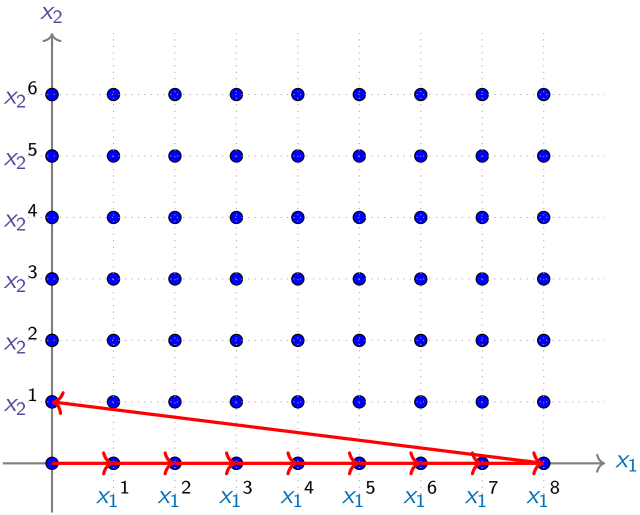
Reverse lex. ordering



Order : x_2 is greater than any power of x_1.

$$x_2 > x_1{}^n$$

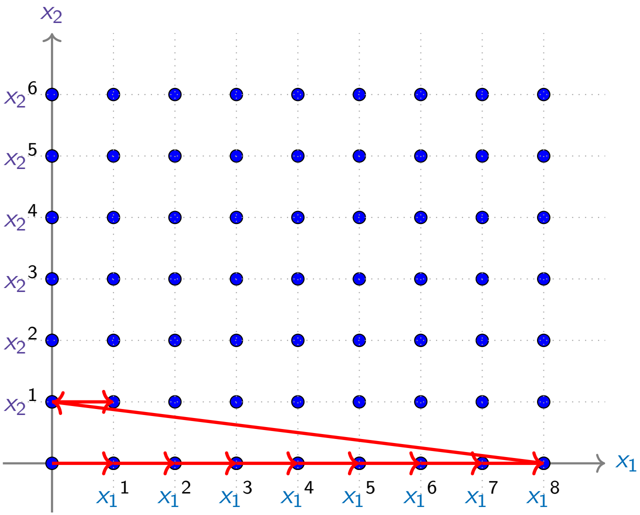
Reverse lex. ordering



Order : x_2 is greater than any power of x_1.

$$x_2 > x_1{}^n$$

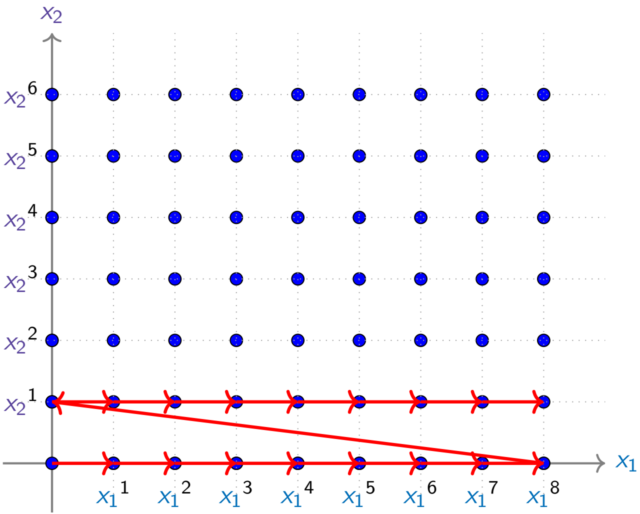
Reverse lex. ordering



Order : x_2 is greater than any power of x_1.

$$x_2 > x_1{}^n$$

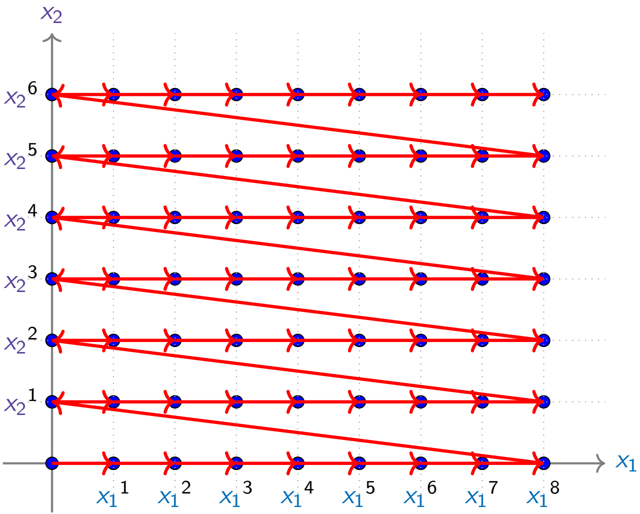
Reverse lex. ordering



Order : x_2 is greater than any power of x_1.

$$x_2 > {x_1}^n$$

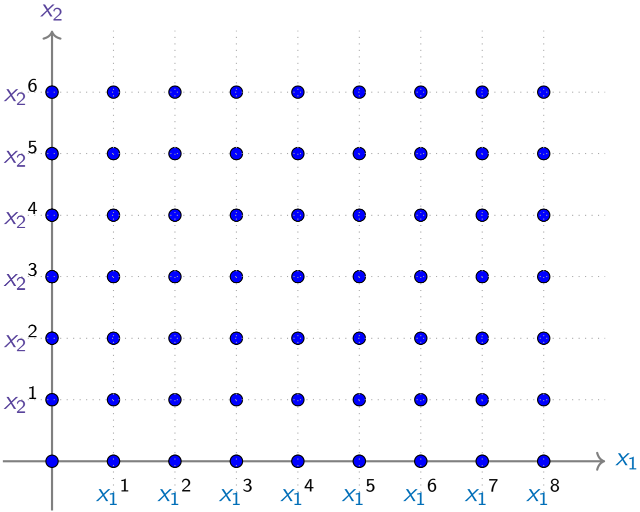
Reverse lex. ordering



Order : x_2 is greater than any power of x_1.

$$x_2 > x_1{}^n$$

Graded lex. ordering



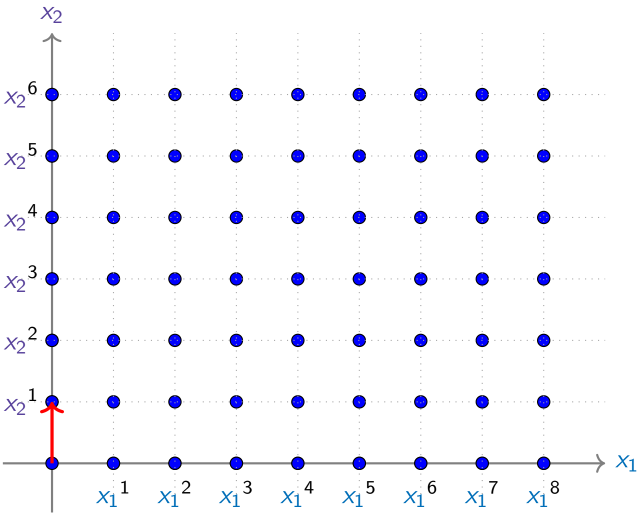
Order : The element with the highest degree is the largest.

$$\begin{cases} x_1{}^{n_1} x_2{}^{n_2} & > x_1{}^{m_1} x_2{}^{m_2} \\ n_1 + n_2 & > m_1 + m_2 \end{cases}$$

If equality holds, x_1 is greater than x_2.

$$x_1 > x_2$$

Graded lex. ordering



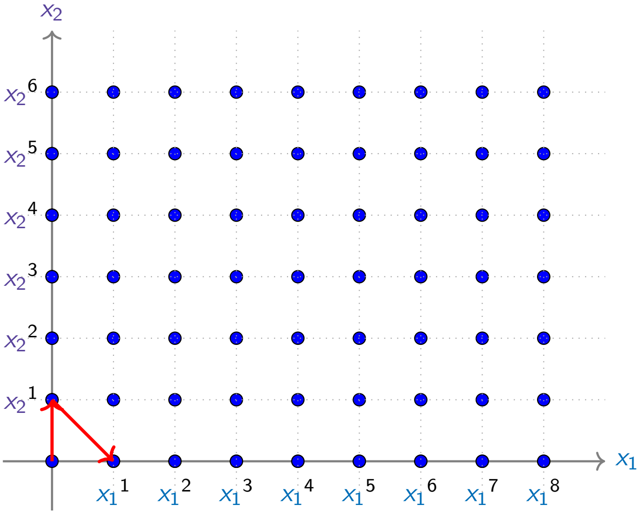
Order : The element with the highest degree is the largest.

$$\begin{cases} {x_1}^{n_1}{x_2}^{n_2} & > {x_1}^{m_1}{x_2}^{m_2} \\ n_1 + n_2 & > m_1 + m_2 \end{cases}$$

If equality holds, x_1 is greater than x_2.

$$x_1 > x_2$$

Graded lex. ordering



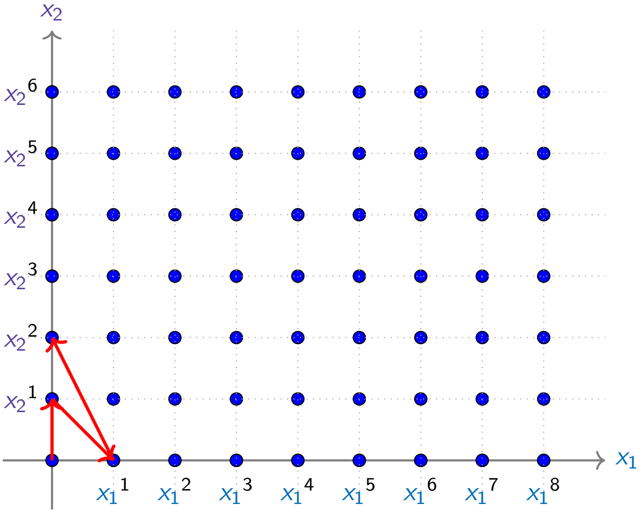
Order : The element with the highest degree is the largest.

$$\begin{cases} x_1^{n_1} x_2^{n_2} & > x_1^{m_1} x_2^{m_2} \\ n_1 + n_2 & > m_1 + m_2 \end{cases}$$

If equality holds, x_1 is greater than x_2.

$$x_1 > x_2$$

Graded lex. ordering



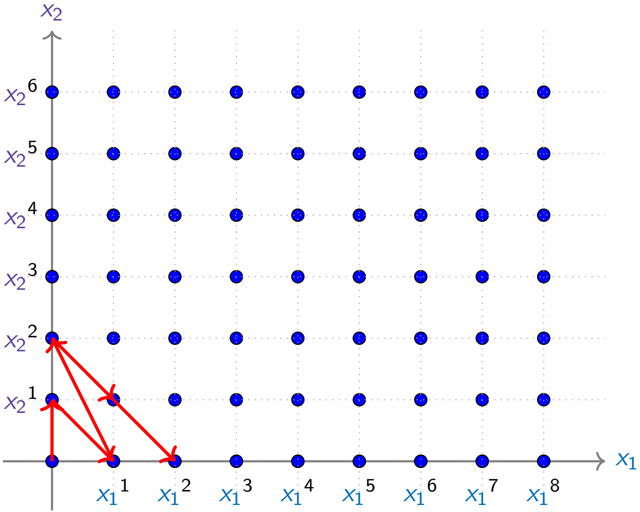
Order : The element with the highest degree is the largest.

$$\begin{cases} x_1{}^{n_1} x_2{}^{n_2} & > x_1{}^{m_1} x_2{}^{m_2} \\ n_1 + n_2 & > m_1 + m_2 \end{cases}$$

If equality holds, x_1 is greater than x_2.

$$x_1 > x_2$$

Graded lex. ordering



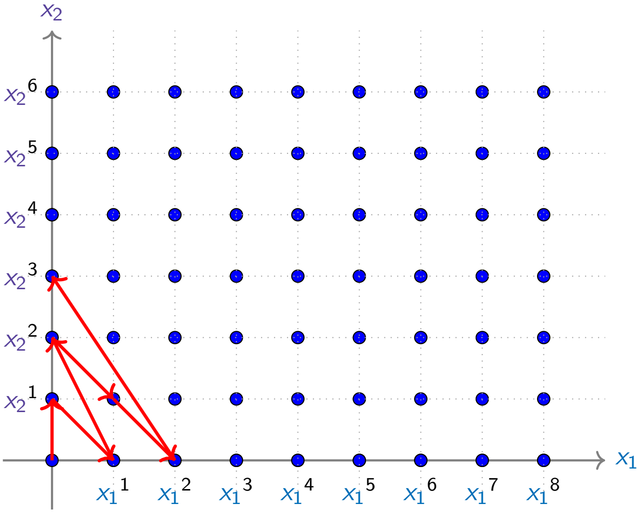
Order : The element with the highest degree is the largest.

$$\begin{cases} {x_1}^{n_1}{x_2}^{n_2} & > {x_1}^{m_1}{x_2}^{m_2} \\ n_1 + n_2 & > m_1 + m_2 \end{cases}$$

If equality holds, x_1 is greater than x_2.

$$x_1 > x_2$$

Graded lex. ordering



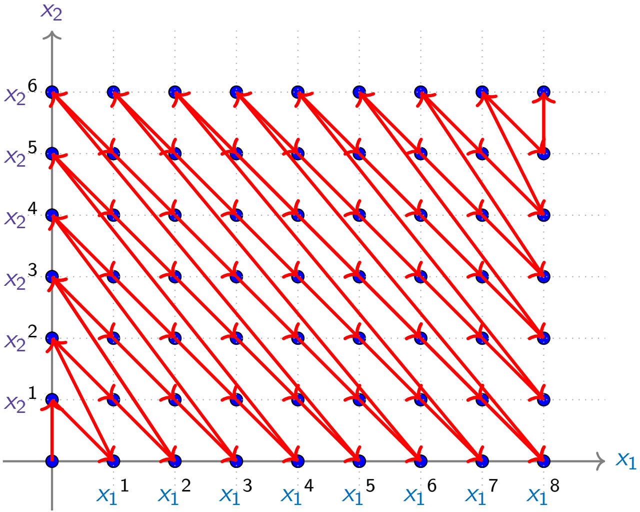
Order : The element with the highest degree is the largest.

$$\begin{cases} x_1{}^{n_1} x_2{}^{n_2} & > x_1{}^{m_1} x_2{}^{m_2} \\ n_1 + n_2 & > m_1 + m_2 \end{cases}$$

If equality holds, x_1 is greater than x_2.

$$x_1 > x_2$$

Graded lex. ordering



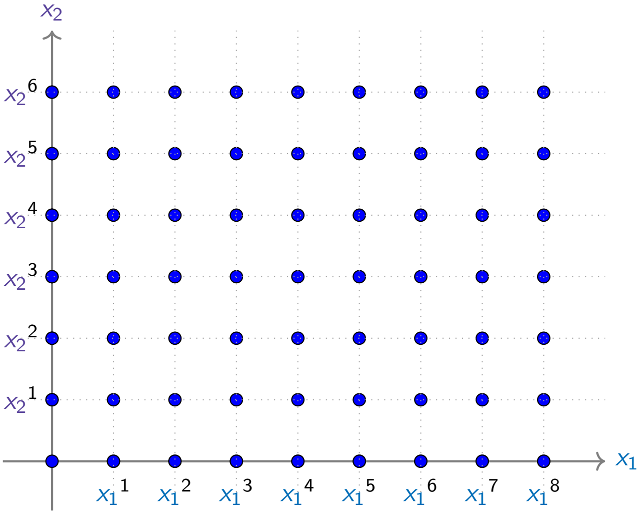
Order : The element with the highest degree is the largest.

$$\begin{cases} {x_1}^{n_1}{x_2}^{n_2} & > {x_1}^{m_1}{x_2}^{m_2} \\ n_1 + n_2 & > m_1 + m_2 \end{cases}$$

If equality holds, x_1 is greater than x_2.

$$x_1 > x_2$$

Graded reverse lex. ordering



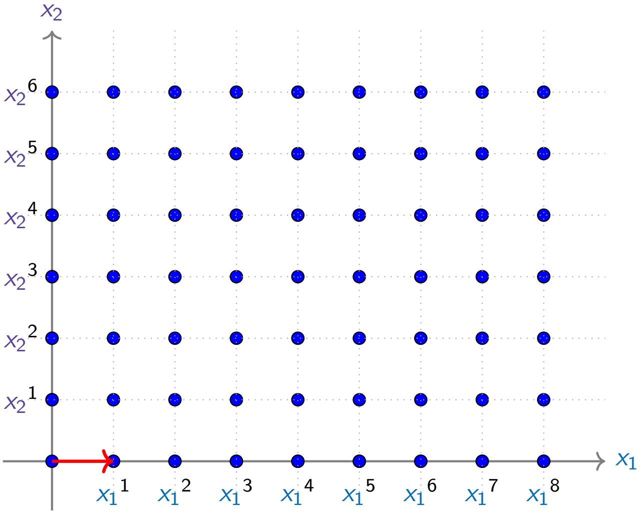
Order : The element with the highest degree is the largest.

$$\begin{cases} {x_1}^{n_1}{x_2}^{n_2} & > {x_1}^{m_1}{x_2}^{m_2} \\ n_1 + n_2 & > m_1 + m_2 \end{cases}$$

If equality holds, x_2 is greater than x_1.

$$x_2 > x_1$$

Graded reverse lex. ordering



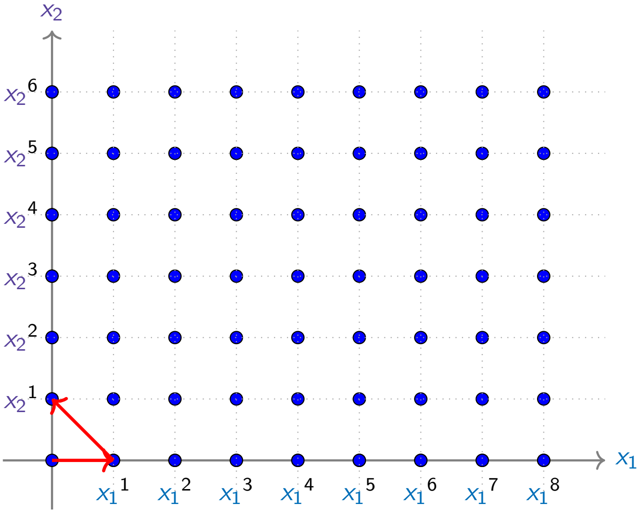
Order : The element with the highest degree is the largest.

$$\begin{cases} {x_1}^{n_1} {x_2}^{n_2} & > {x_1}^{m_1} {x_2}^{m_2} \\ n_1 + n_2 & > m_1 + m_2 \end{cases}$$

If equality holds, x_2 is greater than x_1.

$$x_2 > x_1$$

Graded reverse lex. ordering



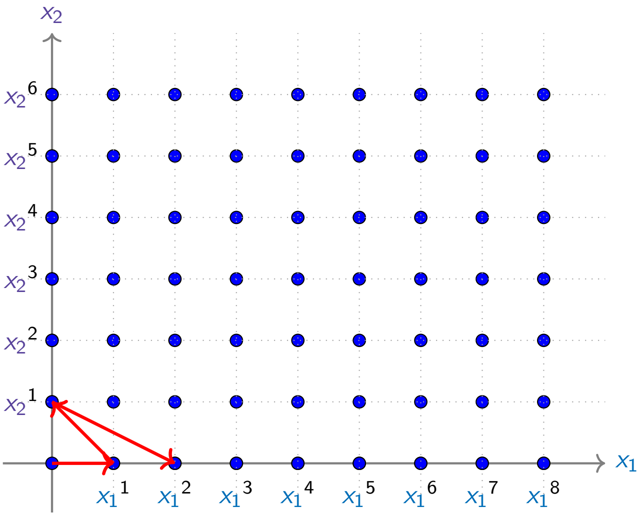
Order : The element with the highest degree is the largest.

$$\begin{cases} {x_1}^{n_1}{x_2}^{n_2} & > {x_1}^{m_1}{x_2}^{m_2} \\ n_1 + n_2 & > m_1 + m_2 \end{cases}$$

If equality holds, x_2 is greater than x_1.

$$x_2 > x_1$$

Graded reverse lex. ordering



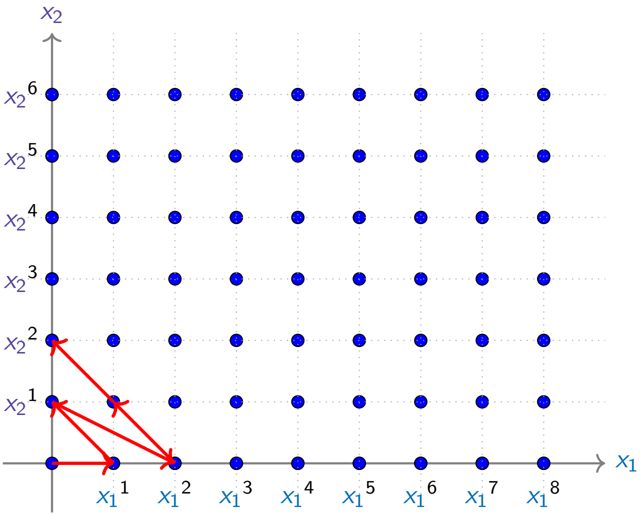
Order : The element with the highest degree is the largest.

$$\begin{cases} x_1{}^{n_1} x_2{}^{n_2} & > x_1{}^{m_1} x_2{}^{m_2} \\ n_1 + n_2 & > m_1 + m_2 \end{cases}$$

If equality holds, x_2 is greater than x_1.

$$x_2 > x_1$$

Graded reverse lex. ordering



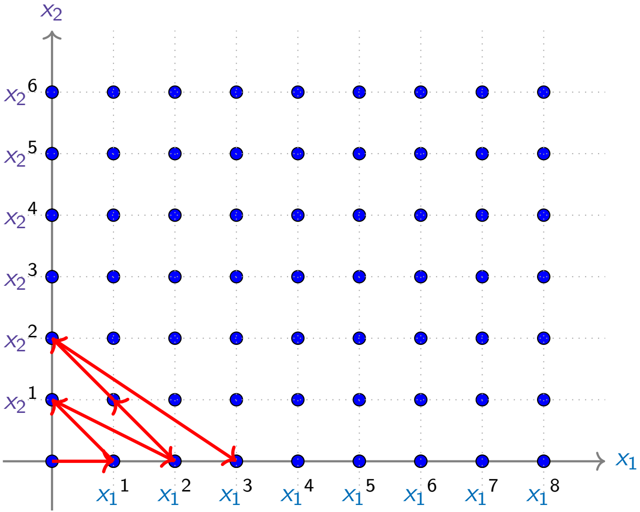
Order : The element with the highest degree is the largest.

$$\begin{cases} {x_1}^{n_1} {x_2}^{n_2} & > {x_1}^{m_1} {x_2}^{m_2} \\ n_1 + n_2 & > m_1 + m_2 \end{cases}$$

If equality holds, x_2 is greater than x_1.

$$x_2 > x_1$$

Graded reverse lex. ordering



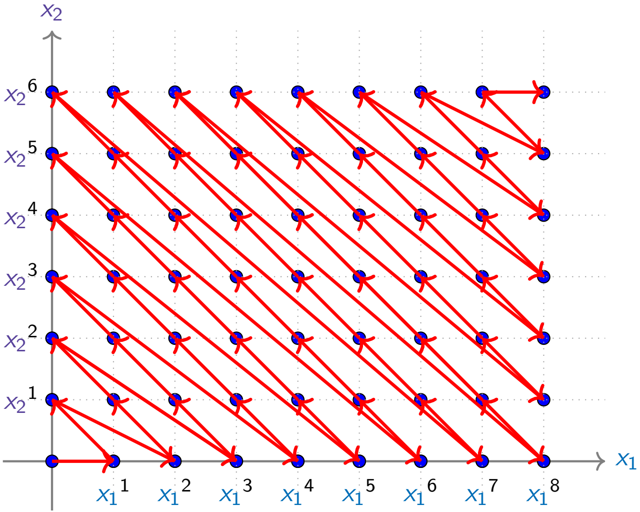
Order : The element with the highest degree is the largest.

$$\begin{cases} x_1{}^{n_1} x_2{}^{n_2} & > x_1{}^{m_1} x_2{}^{m_2} \\ n_1 + n_2 & > m_1 + m_2 \end{cases}$$

If equality holds, x_2 is greater than x_1.

$$x_2 > x_1$$

Graded reverse lex. ordering



Order : The element with the highest degree is the largest.

$$\begin{cases} x_1{}^{n_1} x_2{}^{n_2} & > x_1{}^{m_1} x_2{}^{m_2} \\ n_1 + n_2 & > m_1 + m_2 \end{cases}$$

If equality holds, x_2 is greater than x_1.

$$x_2 > x_1$$

Monomial ordering

Some orderings in $\mathbb{F}_q[x_1, x_2, \dots, x_n]$.

Lexicographical order (lex)

First, compare degrees of highest variable, then second variable, ...

$$x_1 > x_2 > \ldots > x_n, \qquad x_1 > {x_2}^2,$$

$$ {x_1}^2 x_2 > {x_1}^2 x_n$$

Monomial ordering

Some orderings in $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$.

Lexicographical order (lex)

First, compare degrees of highest variable, then second variable, ...

$$x_1 > x_2 > \ldots > x_n, \qquad x_1 > {x_2}^2,$$

$$ {x_1}^2 x_2 > {x_1}^2 x_n$$

Graded lex. order (grlex)

First, compare total degree, then lex. order if equality.

$$x_1 > x_2 > \ldots > x_n, \qquad x_1 < {x_2}^2,$$

$$ {x_1}^2 x_2 > {x_1}^2 x_n$$

Monomial ordering

Some orderings in $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$.

Lexicographical order (lex)

First, compare degrees of highest variable, then second variable, ...

$$x_1 > x_2 > \ldots > x_n, \qquad x_1 > {x_2}^2,$$

$$ {x_1}^2 x_2 > {x_1}^2 x_n$$

Graded lex. order (grlex)

First, compare total degree, then lex. order if equality.

$$x_1 > x_2 > \ldots > x_n, \qquad x_1 < {x_2}^2,$$

$$ {x_1}^2 x_2 > {x_1}^2 x_n$$

Graded reverse lex. order (grevlex)

First, compare total degree, then inverse lex. order if equality.

$$x_1 < x_2 < \ldots < x_n, \qquad x_1 < {x_2}^2,$$

$$ {x_1}^2 x_2 < {x_1}^2 x_n$$

Monomial ordering

Some orderings in $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$.

Lexicographical order (lex)

First, compare degrees of highest variable, then second variable, ...

$$x_1 > x_2 > \ldots > x_n, \qquad x_1 > {x_2}^2,$$
$$ {x_1}^2 x_2 > {x_1}^2 x_n$$

Graded lex. order (grlex)

First, compare total degree, then lex. order if equality.

$$x_1 > x_2 > \ldots > x_n, \qquad x_1 < {x_2}^2,$$
$$ {x_1}^2 x_2 > {x_1}^2 x_n$$

Graded reverse lex. order (grevlex)

First, compare total degree, then inverse lex. order if equality.

$$x_1 < x_2 < \ldots < x_n, \qquad x_1 < {x_2}^2,$$
$$ {x_1}^2 x_2 < {x_1}^2 x_n$$

Weighted graded lex. order

First, compare weighted sum of degrees, then graded lex. order.

If $\mathrm{wt}(x_1) = 3$, $\mathrm{wt}(x_2) = 1$ and $\mathrm{wt}(x_n) = 4$, then

$$x_1 < {x_2}^2 x_n$$

Solving polynomial systems

- **Univariate** solving : find the roots of $\mathcal{P}_j \in \mathbb{F}_q[X]$

$$\begin{cases} \mathcal{P}_0(X) & = 0 \\ & \vdots \\ \mathcal{P}_{m-1}(X) & = 0 \,. \end{cases}$$

- **Multivariate** solving : find the roots of $\mathcal{P}_j \in \mathbb{F}_q[X_0, \ldots, X_{n-1}]$

$$\begin{cases} \mathcal{P}_0(X_0, \ldots, X_{n-1}) & = 0 \\ & \vdots \\ \mathcal{P}_{m-1}(X_0, \ldots, X_{n-1}) & = 0 \,. \end{cases}$$

  - Compute a grevlex order GB (**F5** algorithm)
  - Convert it into lex order GB (**FGLM** algorithm)
  - Find the roots in $\mathbb{F}_q^n$ of the GB polynomials using univariate system resolution.

Strategies

How to efficiency solve polynomial systems to build algebraic attacks ?

Strategies

How to efficiency solve polynomial systems to build algebraic attacks ?

- $\star$ by bypassing some rounds of iterated constructions
- $\star$ by changing the modeling
- $\star$ by changing the ordering

Strategies

How to efficiency solve polynomial systems to build algebraic attacks ?

- ⋆ by bypassing some rounds of iterated constructions
- ⋆ by changing the modeling
- ⋆ by changing the ordering
- ⋆ .... by doing nothing ? ?

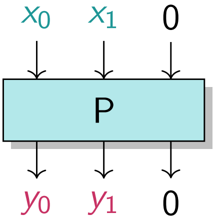
Ethereum Foundation Challenges

https://www.zkhashbounties.info/

(November 2021)

Solving CICO Problem

- ⋆ Feistel–MiMC [Albrecht et al., 2016]
- ⋆ Poseidon [Grassi et al., 2021]
- ⋆ Rescue–Prime [Aly et al., 2020]
- ⋆ Reinforced Concrete [Grassi et al., 2022]



Ethereum Challenges : solving CICO problem for AO primitives with $q \sim 2^{64}$ prime

A. Bariant, C. Bouvier, G. Leurent, L. Perrin, 2022

Cryptanalysis Challenge

Category	Parameters	Security level	Bounty
Easy	$r = 6$	9	$\$2,000$
Easy	$r = 10$	15	$\$4,000$
Medium	$r = 14$	22	$\$6,000$
Hard	$r = 18$	28	$\$12,000$
Hard	$r = 22$	34	$\$26,000$

(a) *Feistel–MiMC*

Category	Parameters	Security level	Bounty
Easy	$N = 4, m = 3$	25	$\$2,000$
Easy	$N = 6, m = 2$	25	$\$4,000$
Medium	$N = 7, m = 2$	29	$\$6,000$
Hard	$N = 5, m = 3$	30	$\$12,000$
Hard	$N = 8, m = 2$	33	$\$26,000$

(b) *Rescue–Prime*

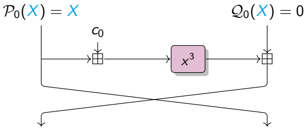
Category	Parameters	Security level	Bounty
Easy	$\mathrm{RP} = 3$	8	$\$2,000$
Easy	$\mathrm{RP} = 8$	16	$\$4,000$
Medium	$\mathrm{RP} = 13$	24	$\$6,000$
Hard	$\mathrm{RP} = 19$	32	$\$12,000$
Hard	$\mathrm{RP} = 24$	40	$\$26,000$

(c) *Poseidon*

Category	Parameters	Security level	Bounty
Easy	$p = 281474976710597$	24	$\$4,000$
Medium	$p = 72057594037926839$	28	$\$6,000$
Hard	$p = 18446744073709551557$	32	$\$12,000$

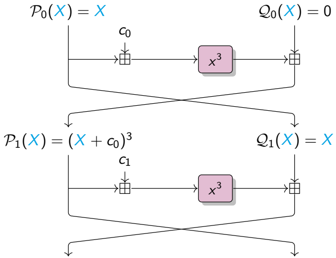
(d) *Reinforced Concrete*

Feistel-MiMC



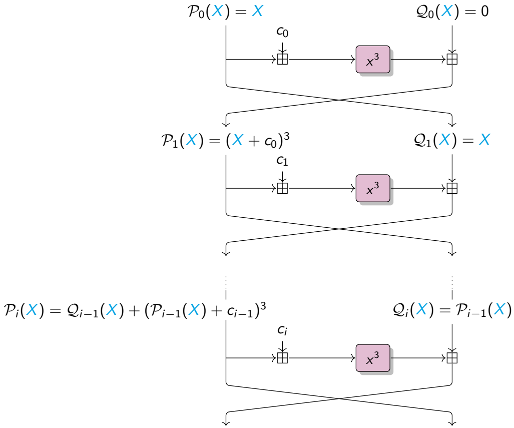
$$\begin{cases} \mathcal{P}_0(X) & = X \\ \mathcal{Q}_0(X) & = 0 \end{cases}$$

Feistel-MiMC



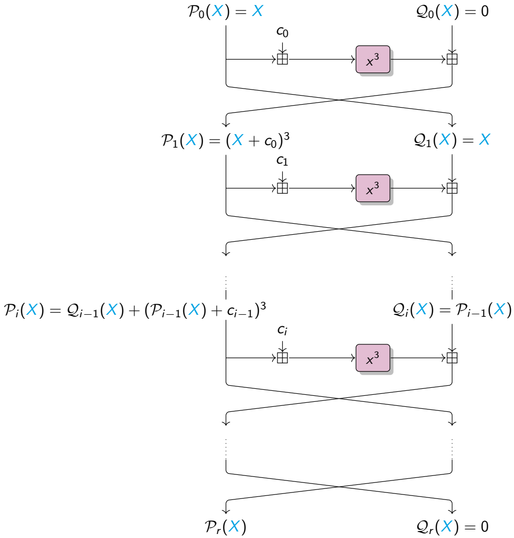
$$\begin{cases} \mathcal{P}_0(X) & = X \\ \mathcal{Q}_0(X) & = 0 \\ \mathcal{P}_1(X) & = (X + c_0)^3 \\ \mathcal{Q}_1(X) & = X \end{cases}$$

Feistel-MiMC



$$\begin{cases} \mathcal{P}_0(X) &= X \\ \mathcal{Q}_0(X) &= 0 \\ \mathcal{P}_1(X) &= (X + c_0)^3 \\ \mathcal{Q}_1(X) &= X \\ \dots & \\ \mathcal{P}_i(X) &= \mathcal{Q}_{i-1}(X) + (\mathcal{P}_{i-1}(X) + c_{i-1})^3 \\ \mathcal{Q}_i(X) &= \mathcal{P}_{i-1}(X) \end{cases}$$

Feistel-MiMC



$$
\begin{cases}
\mathcal{P}_0(X) & = X \\
\mathcal{Q}_0(X) & = 0 \\
\mathcal{P}_1(X) & = (X + c_0)^3 \\
\mathcal{Q}_1(X) & = X \\
\dots & \\
\mathcal{P}_i(X) & = \mathcal{Q}_{i-1}(X) + (\mathcal{P}_{i-1}(X) + c_{i-1})^3 \\
\mathcal{Q}_i(X) & = \mathcal{P}_{i-1}(X) \\
\dots & \\
\mathcal{Q}_r(X) & = 0
\end{cases}
$$

1 variable + $(2r + 1)$ equations

Cryptanalysis Challenge

Category	Parameters	Security level	Bounty
~~Easy~~	~~$r = 6$~~	~~9~~	~~$2,000~~
~~Easy~~	~~$r = 10$~~	~~15~~	~~$4,000~~
~~Medium~~	~~$r = 14$~~	~~22~~	~~$6,000~~
~~Hard~~	~~$r = 18$~~	~~28~~	$12,000
~~Hard~~	~~$r = 22$~~	~~34~~	$26,000

(a) *Feistel–MiMC*

$12,000

Category	Parameters	Security level	Bounty
Easy	$N = 4, m = 3$	25	$2,000
Easy	$N = 6, m = 2$	25	$4,000
Medium	$N = 7, m = 2$	29	$6,000
Hard	$N = 5, m = 3$	30	$12,000
Hard	$N = 8, m = 2$	33	$26,000

(b) *Rescue–Prime*

Category	Parameters	Security level	Bounty
Easy	RP $= 3$	8	$2,000
Easy	RP $= 8$	16	$4,000
Medium	RP $= 13$	24	$6,000
Hard	RP $= 19$	32	$12,000
Hard	RP $= 24$	40	$26,000

(c) *Poseidon*

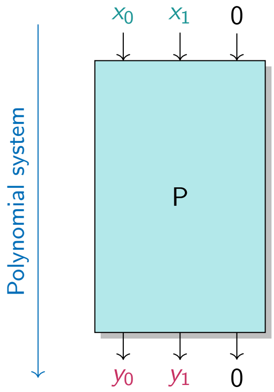
Category	Parameters	Security level	Bounty
Easy	$p = 281474976710597$	24	$4,000
Medium	$p = 72057594037926839$	28	$6,000
Hard	$p = 18446744073709551557$	32	$12,000

(d) *Reinforced Concrete*

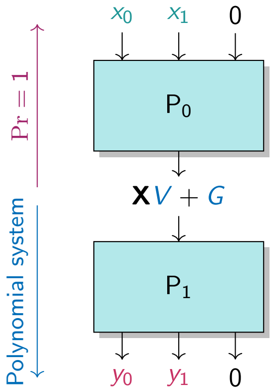
Trick for SPN

Let $P = P_0 \circ P_1$ be a permutation of $\mathbb{F}_p^3$ and suppose

$$\exists\ V, G \in \mathbb{F}_p^3, \quad \text{s.t. } \forall\ \mathbf{X} \in \mathbb{F}_p, \quad P_0^{-1}(\mathbf{X}V + G) = (*, *, 0)\ .$$

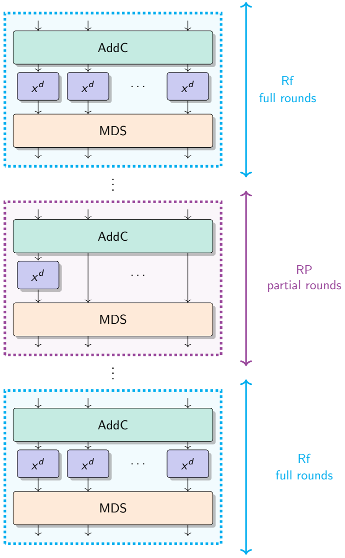


(a) *R-round system.*



(b) $(R-2)$*-round system.*

Poseidon

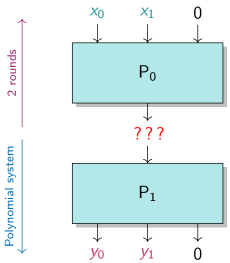


- ⋆ S-box :

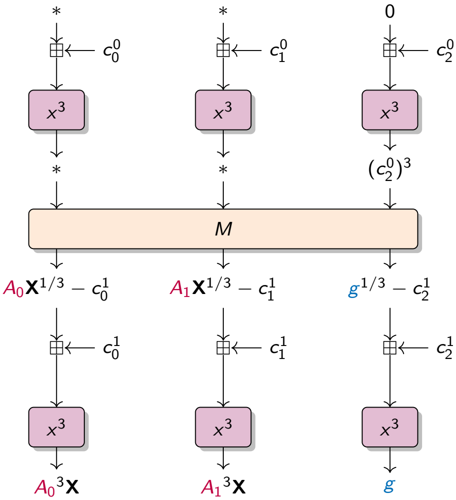
$$x \mapsto x^3$$

- ⋆ Nb rounds :

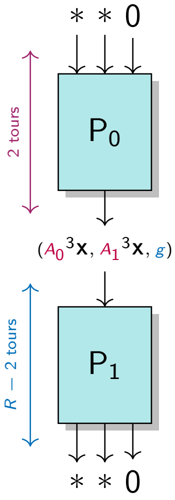
$$R = 2 \times Rf + RP$$
$$= 8 + (\text{from } 3 \text{ to } 24)$$



Trick for Poseidon

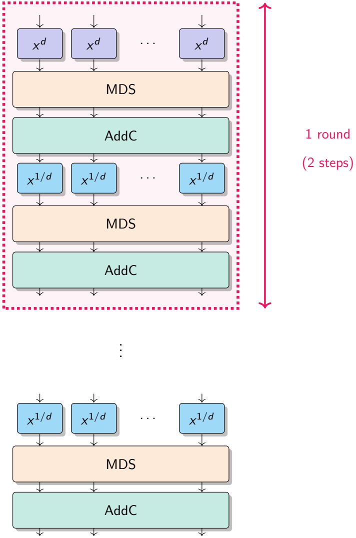


(a) *First two rounds.*



(b) *Overview.*

Rescue–Prime



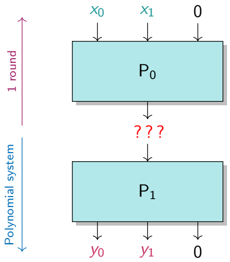
- ⋆ S-box :

$$x \mapsto x^3 \quad \text{and} \quad x \mapsto x^{1/3}$$

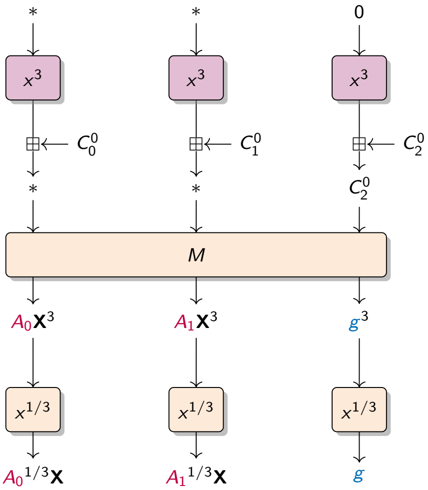
- ⋆ Nb rounds :

$$R = \text{from 4 to 8}$$

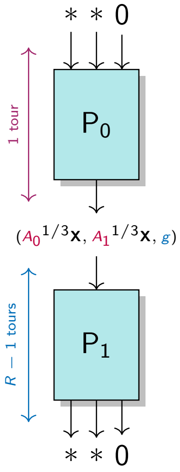
(2 S-boxes per round)



Trick for Rescue–Prime



(a) *First round.*



(b) *Overview.*

Cryptanalysis Challenge

Category	Parameters	Security level	Bounty
~~Easy~~	~~$r = 6$~~	~~9~~	~~\$2, 000~~
~~Easy~~	~~$r = 10$~~	~~15~~	~~\$4, 000~~
~~Medium~~	~~$r = 14$~~	~~22~~	~~\$6, 000~~
~~Hard~~	~~$r = 18$~~	~~28~~	\$12, 000
~~Hard~~	~~$r = 22$~~	~~34~~	\$26, 000

(a) *Feistel–MiMC*

\$26, 000

Category	Parameters	Security level	Bounty
~~Easy~~	~~$N = 4, m = 3$~~	~~25~~	~~\$2, 000~~
Easy	$N = 6, m = 2$	25	\$4, 000
Medium	$N = 7, m = 2$	29	\$6, 000
Hard	$N = 5, m = 3$	30	\$12, 000
Hard	$N = 8, m = 2$	33	\$26, 000

(b) *Rescue–Prime*

Category	Parameters	Security level	Bounty
~~Easy~~	~~RP = 3~~	~~8~~	~~\$2, 000~~
~~Easy~~	~~RP = 8~~	~~16~~	~~\$4, 000~~
~~Medium~~	~~RP = 13~~	~~24~~	~~\$6, 000~~
Hard	RP $= 19$	32	\$12, 000
Hard	RP $= 24$	40	\$26, 000

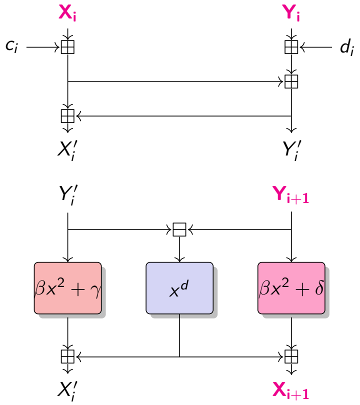
(c) *Poseidon*

Category	Parameters	Security level	Bounty
Easy	$p = 281474976710597$	24	\$4, 000
Medium	$p = 72057594037926839$	28	\$6, 000
Hard	$p = 18446744073709551557$	32	\$12, 000

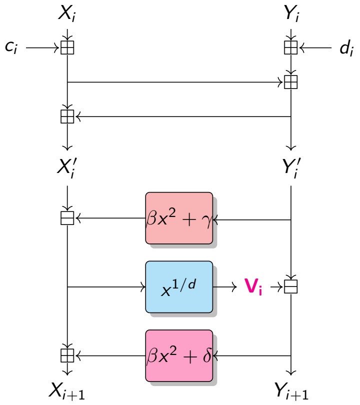
(d) *Reinforced Concrete*

Modeling of Anemoi

C. Bouvier, P. Briaud, P. Chaidos, L. Perrin, R. Salen, V. Velichkov and D. Willems, 2023

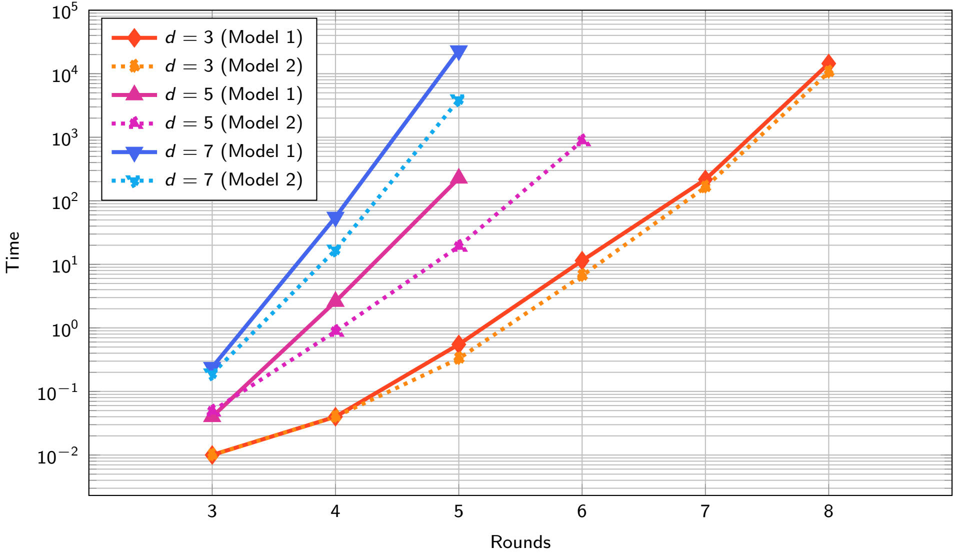


Model 1.



Model 2.

Importance of modeling



FreeLunch attack

A. Bariant, A. Boeuf, A. Lemoine, I. Manterola Ayala, M. Øygarden, L. Perrin, and H. Raddum, 2024

Multivariate solving :

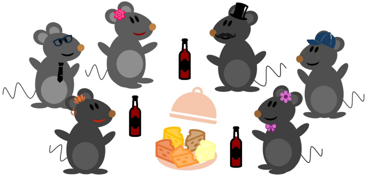
- ⋆ Define the system
- ⋆ Compute a grevlex order GB (**F5** algorithm)
- ⋆ Convert it into lex order GB (**FGLM** algorithm)
- ⋆ Find the roots in $\mathbb{F}_q^n$ of the GB polynomials using univariate system resolution.

FreeLunch attack

A. Bariant, A. Boeuf, A. Lemoine, I. Manterola Ayala, M. Øygarden, L. Perrin, and H. Raddum, 2024

Multivariate solving :

- ⋆ Define the system
- ⋆ Compute a grevlex order GB (**F5** algorithm) $\rightsquigarrow$ **can be skipped**
- ⋆ Convert it into lex order GB (**FGLM** algorithm)
- ⋆ Find the roots in $\mathbb{F}_q^n$ of the GB polynomials using univariate system resolution.



New Challenges

https://www.poseidon-initiative.info/

(November 2024)

New winners

- Poseidon-256:
- ~~24 bit estimated security: RF=6, RP=8.~~ $4000 **claimed 9 Dec 2024**
- ~~28 bit estimated security: RF=6, RP=9~~. $6000 **claimed 2 Jan 2025**
- 32-bit estimated security: RF=6, RP=11. $10000
- 40-bit estimated security: RF=6, RP=16. $15000
- Poseidon-64:
- 24-bit estimated security: RF=6, RP=7 $4000
- 28-bit estimated security: RF=6, RP=8. $6000
- 32-bit estimated security: RF=6, RP=10. $10000
- 40-bit estimated security: RF=6, RP=13. $15000
- Poseidon-31:
- 24-bit estimated security: ~~RF=4, RP=0 (M31)~~ **claimed 29 Nov 2025** ~~and RP=1 (KoalaBear). $4000~~ **claimed 30 Nov 2025**
- 28-bit estimated security: ~~RF=4, RP=1 (M31) and RP=3 (KoalaBear). $6000~~ **claimed 29 Nov 2025**
- 32-bit estimated security: ~~RF=6, RP=1 (M31)~~ **claimed 2 Dec 2025** ~~and RP=4 (KoalaBear)~~. ~~$10000~~ **claimed 5 Dec 2025**
- 40-bit estimated security: RF=6, RP=4 (M31 only). $15000

QUIZ ! !

- With respect to lexicographical ordering, $x_1 x_2 < x_2 x_3$? $x_3 > x_1^3$? $x_1 > x_2^3$?
- With respect to graded reverse lexicographical ordering, $x_1 x_2 x_3 > x_4 x_5$?
- Could we use the tricks for SPN on Reinforced Concrete ?
- Is the FreeLunch attack usefull for Feistel-MiMC ?

Take-away

How to prevent algebraic attacks ?

- ⋆ Try as many modelings as possible
- ⋆ Prefer univariate systems instead of multivariate systems
- ⋆ Be careful with tricks that allow to bypass rounds

$\boxed{\text{AOPs : a new lucrative business ?}}$

Other attacks

HO attacks and music

Differential attacks and morse code

Linear attacks and cohomology

Algebraic degree

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$. Using the isomorphism $\mathbb{F}_2^n \simeq \mathbb{F}_{2^n}$,
there is **a unique univariate polynomial representation** on $\mathbb{F}_{2^n}$ of degree at most $2^n - 1$:

$$F(x) = \sum_{i=0}^{2^n-1} b_i x^i ; b_i \in \mathbb{F}_{2^n}$$

Algebraic degree

$$\deg^a(F) = \max\{\mathrm{wt}(i),\ 0 \leq i < 2^n,\ \text{and}\ \ b_i \neq 0\}$$

Algebraic degree

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$. Using the isomorphism $\mathbb{F}_2^n \simeq \mathbb{F}_{2^n}$,
there is **a unique univariate polynomial representation** on $\mathbb{F}_{2^n}$ of degree at most $2^n - 1$:

$$F(x) = \sum_{i=0}^{2^n-1} b_i x^i ; b_i \in \mathbb{F}_{2^n}$$

Algebraic degree

$$\deg^a(F) = \max\{\mathrm{wt}(i),\ 0 \le i < 2^n,\ \text{and}\ \ b_i \neq 0\}$$

Example : $\deg^u(x \mapsto x^3) = 3$ and $\deg^a(x \mapsto x^3) = 2.$

Algebraic degree

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$. Using the isomorphism $\mathbb{F}_2^n \simeq \mathbb{F}_{2^n}$,
there is **a unique univariate polynomial representation** on $\mathbb{F}_{2^n}$ of degree at most $2^n - 1$:

$$F(x) = \sum_{i=0}^{2^n-1} b_i x^i ; b_i \in \mathbb{F}_{2^n}$$

Algebraic degree

$$\deg^a(F) = \max\{\mathrm{wt}(i),\ 0 \leq i < 2^n,\ \text{and}\ \ b_i \neq 0\}$$

Example : $\deg^u(x \mapsto x^3) = 3$ and $\deg^a(x \mapsto x^3) = 2$.

If $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is a permutation, then

$$\boxed{\deg^a(F) \leq n - 1}$$

Higher-Order differential attacks

Exploiting a low algebraic degree

For any affine subspace $\mathcal{V} \subset \mathbb{F}_2^n$ with $\dim \mathcal{V} \geq \deg^a(F) + 1$, we have a 0-sum distinguisher :

$$\bigoplus_{x \in \mathcal{V}} F(x) = 0.$$

Random permutation : degree $= n - 1$

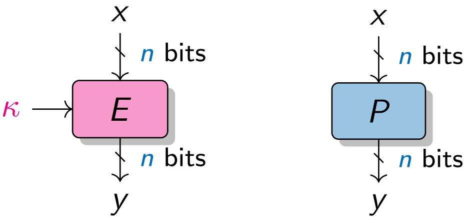
Higher-Order differential attacks

Exploiting a low algebraic degree

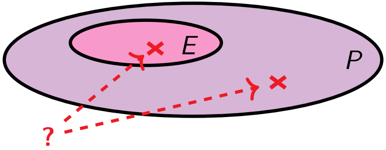
For any affine subspace $\mathcal{V} \subset \mathbb{F}_2^n$ with $\dim \mathcal{V} \geq \deg^a(F) + 1$, we have a 0-sum distinguisher :

$$\bigoplus_{x \in \mathcal{V}} F(x) = 0.$$

Random permutation : degree $= n - 1$



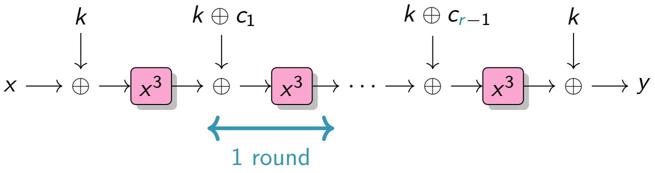
(a) *Block cipher* **(b)** *Random permutation*



MiMC

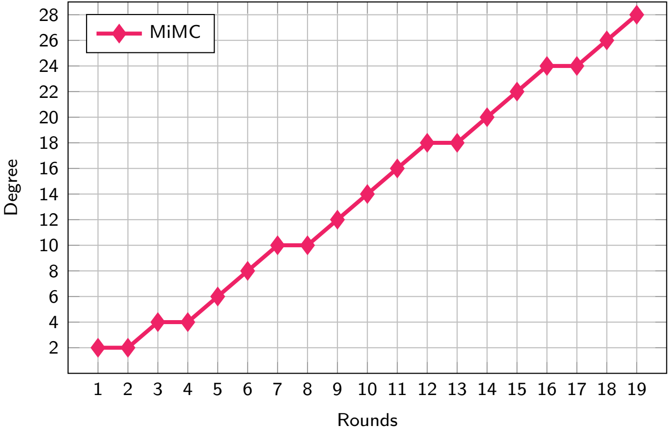
M. Albrecht, L. Grassi, C. Rechberger, A. Roy and T. Tiessen, 2016

- n-bit blocks (n odd ≈ 129) : $x \in \mathbb{F}_{2^n}$
- n-bit key : $k \in \mathbb{F}_{2^n}$
- 82 rounds when $n = 129$



Plateau

C. Bouvier, A. Canteaut and L. Perrin, 2023



Proposition

There is a plateau when

$$k_r = \lfloor r \log_2 3 \rfloor = 1 \bmod 2$$

and

$$k_{r+1} = \lfloor (r+1) \log_2 3 \rfloor = 0 \bmod 2$$

Music in MiMC

- Patterns in sequence $(\lfloor r \log_2 3 \rfloor)_{r>0}$: denominators of semiconvergents of

$$\log_2(3) \simeq 1.5849625$$

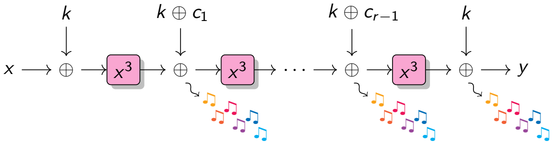
$$\mathfrak{D} = \{\boxed{1}, \boxed{2}, 3, 5, \boxed{7}, \boxed{12}, 17, 29, 41, \boxed{53}, 94, 147, 200, 253, 306, \boxed{359}, \ldots\} ,$$

$$\log_2(3) \simeq \frac{a}{b} \quad \Leftrightarrow \quad 2^a \simeq 3^b$$

- **Music theory :**
  - perfect octave 2 :1
  - perfect fifth 3 :2

$$2^{19} \simeq 3^{12} \quad \Leftrightarrow \quad 2^7 \simeq \left(\frac{3}{2}\right)^{12}$$

$$\Leftrightarrow \quad \text{7 octaves} \sim \text{12 fifths}$$



Statistical attacks

⋆ Differential attacks

Definition

Let $F : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^m$ be a function. The **Differential uniformity** δ_F is given by

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

⋆ Linear attacks

Statistical attacks

- Differential attacks

Definition

Let $F : \mathbb{F}_q^n \to \mathbb{F}_q^m$ be a function. The **Differential uniformity** δ_F is given by

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

- Linear attacks

Definition

Let $F : \mathbb{F}_q^n \to \mathbb{F}_q^m$ be a function and ω a primitive element.
The **Linearity** $\mathcal{L}_F$ is the highest Walsh coefficient.

$$\mathcal{L}_F = \max_{u, v \neq 0} \left| \sum_{x \in \mathbb{F}_2^n} (-1)^{(\langle v, F(x) \rangle \oplus \langle u, x \rangle)} \right|$$

Statistical attacks

⋆ Differential attacks

Definition

Let $F : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^m$ be a function. The **Differential uniformity** δ_F is given by

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

⋆ Linear attacks

Definition

Let $F : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^m$ be a function and ω a primitive element.
The **Linearity** $\mathcal{L}_F$ is the highest Walsh coefficient.

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

Statistical attacks

⋆ Differential attacks — Example : **Rescue**

Definition

Let $F : \mathbb{F}_q^n \to \mathbb{F}_q^m$ be a function. The **Differential uniformity** δ_F is given by

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

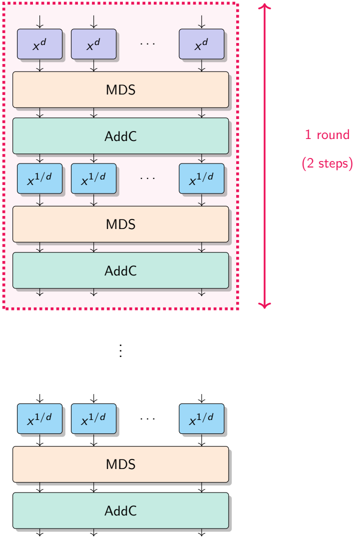
⋆ Linear attacks — Example : **Anemoi** (Flystel)

Definition

Let $F : \mathbb{F}_q^n \to \mathbb{F}_q^m$ be a function and ω a primitive element.
The **Linearity** $\mathcal{L}_F$ is the highest Walsh coefficient.

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

Rescue



A. Aly, T. Ashur, E. Ben-Sasson, S. Dhooghe and A. Szepieniec, 2020

- S-box :

$$x \mapsto x^3 \quad \text{and} \quad x \mapsto x^{1/3}$$

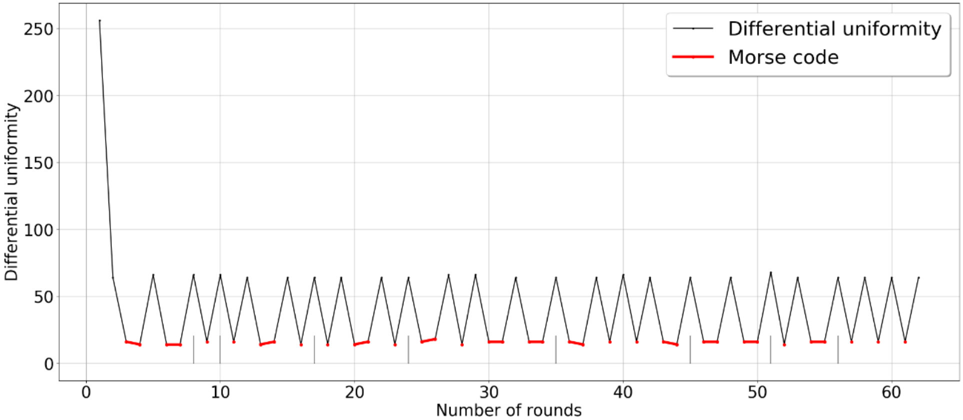
- Nb rounds :

$$R = \text{from 8 to 26}$$

(2 S-boxes per round)

Morse Code

A. Boeuf, A. Canteaut and L. Perrin, 2024



– . .-. .-. -.– -..— .- ... (MERRYXMAS)

Weil bound for the Linearity

Proposition [Weil, 1948]

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

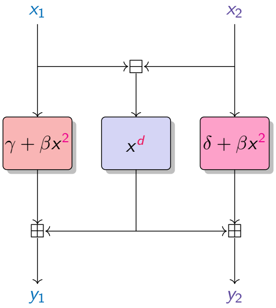
$$\mathcal{L}_f \leq (d-1)\sqrt{p}$$

Weil bound for the Linearity

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.

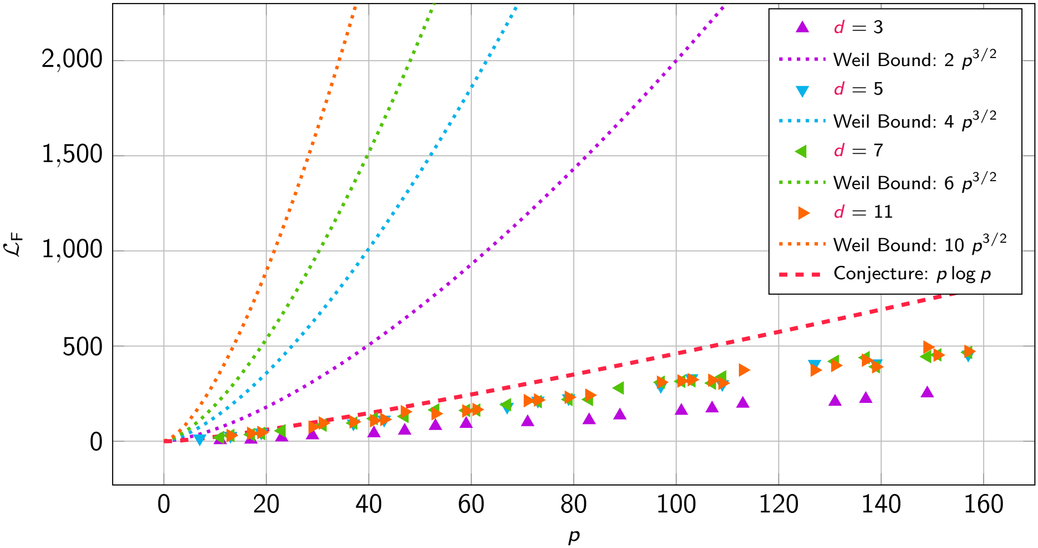
$$\mathcal{L}_{\mathsf{F}} \leq (d-1)p\sqrt{p} \ ?$$

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

Conjecture

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

Experimental results



Exponential sums

T. Beyne and C. Bouvier, 2024

⋆ Direct applications of results for exponential sums (generalization of Weil bound)

Exponential sums

T. Beyne and C. Bouvier, 2024

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

Functions with 2 variables

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

Exponential sums

T. Beyne and C. Bouvier, 2024

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

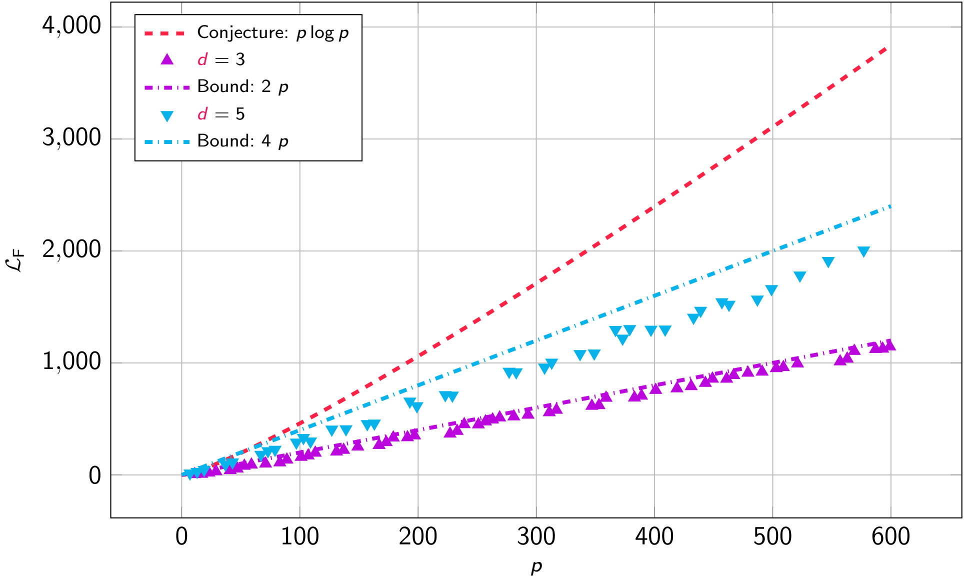
Functions with 2 variables

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

- ⋆ Solving conjecture on the linearity of the Flystel construction (for $d \leq \log p$)

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

Solving conjecture



Take-away

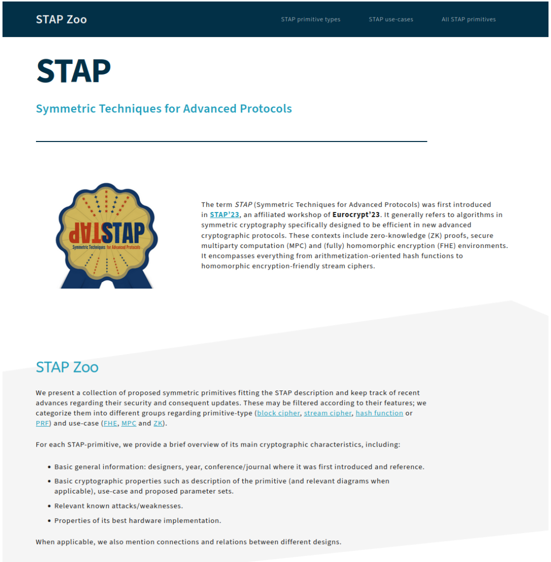
Progress in cryptanalysis

⋆ Some results have links with other fields.

⋆ Some results require very complex maths

$\boxed{\text{AOPs are full of unexpected resources !}}$

STAP Zoo



STAP Zoo | STAP primitive types | STAP use-cases | All STAP primitives

STAP

Symmetric Techniques for Advanced Protocols

The term *STAP* (Symmetric Techniques for Advanced Protocols) was first introduced in STAP'23, an affiliated workshop of **Eurocrypt'23**. It generally refers to algorithms in symmetric cryptography specifically designed to be efficient in new advanced cryptographic protocols. These contexts include zero-knowledge (ZK) proofs, secure multiparty computation (MPC) and (fully) homomorphic encryption (FHE) environments. It encompasses everything from arithmetization-oriented hash functions to homomorphic encryption-friendly stream ciphers.

STAP Zoo

We present a collection of proposed symmetric primitives fitting the STAP description and keep track of recent advances regarding their security and consequent updates. These may be filtered according to their features; we categorize them into different groups regarding primitive-type (block cipher, stream cipher, hash function or PRF) and use-case (FHE, MPC and ZK).

For each STAP-primitive, we provide a brief overview of its main cryptographic characteristics, including:

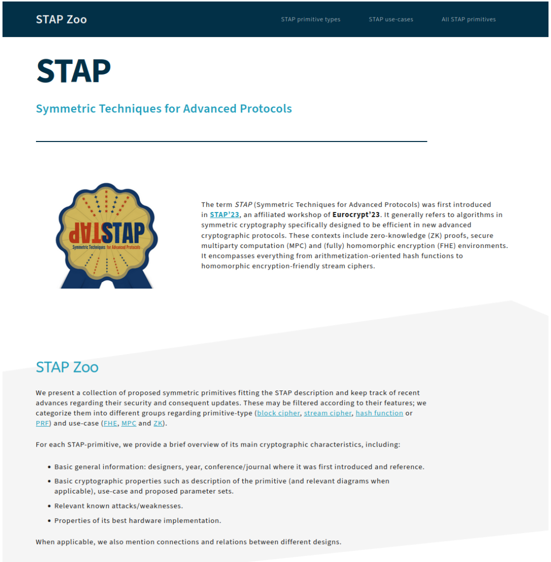
- Basic general information: designers, year, conference/journal where it was first introduced and reference.
- Basic cryptographic properties such as description of the primitive (and relevant diagrams when applicable), use-case and proposed parameter sets.
- Relevant known attacks/weaknesses.
- Properties of its best hardware implementation.

When applicable, we also mention connections and relations between different designs.

Check our website

`stap-zoo.com`

STAP Zoo


STAP Zoo STAP primitive types STAP use-cases All STAP primitives

STAP

Symmetric Techniques for Advanced Protocols

The term *STAP* (Symmetric Techniques for Advanced Protocols) was first introduced in STAP'23, an affiliated workshop of **Eurocrypt'23**. It generally refers to algorithms in symmetric cryptography specifically designed to be efficient in new advanced cryptographic protocols. These contexts include zero-knowledge (ZK) proofs, secure multiparty computation (MPC) and (fully) homomorphic encryption (FHE) environments. It encompasses everything from arithmetization-oriented hash functions to homomorphic encryption-friendly stream ciphers.

STAP Zoo

We present a collection of proposed symmetric primitives fitting the STAP description and keep track of recent advances regarding their security and consequent updates. These may be filtered according to their features; we categorize them into different groups regarding primitive-type (block cipher, stream cipher, hash function or PRF) and use-case (FHE, MPC and ZK).

For each STAP-primitive, we provide a brief overview of its main cryptographic characteristics, including:

- Basic general information: designers, year, conference/journal where it was first introduced and reference.
- Basic cryptographic properties such as description of the primitive (and relevant diagrams when applicable), use-case and proposed parameter sets.
- Relevant known attacks/weaknesses.
- Properties of its best hardware implementation.

When applicable, we also mention connections and relations between different designs.

Check our website

stap-zoo.com

Thank you !