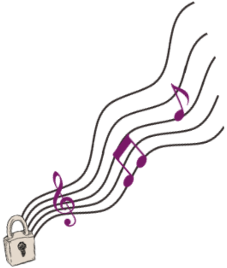
An Overview of Arithmetization-Oriented Primitives

Design and Security Insights

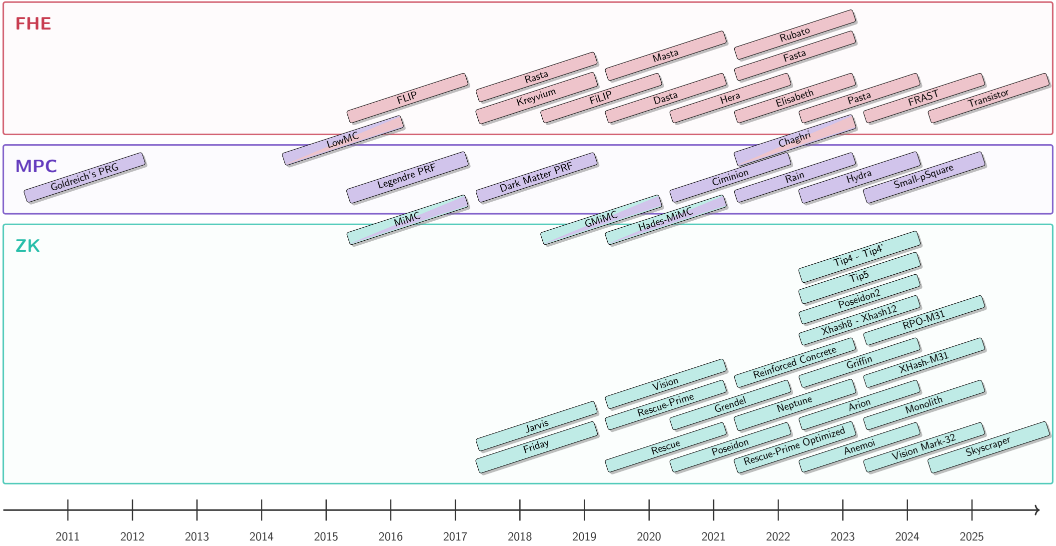


Clémence Bouvier

Université de Lorraine, CNRS, Inria, LORIA

APSIA Seminar, Esch-sur-Alzette, Luxembourg
February 21st, 2025

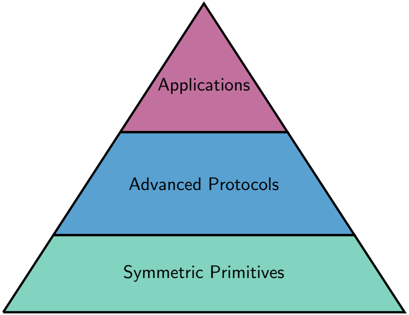
New symmetric primitives



A need for new primitives

Protocols requiring new primitives:

- ⋆ **FHE**: Fully Homomorphic Encryption
- ⋆ **MPC**: Multiparty Computation
- ⋆ **ZK**: Systems of Zero-Knowledge proofs
  Example: SNARKs, STARKs, Bulletproofs

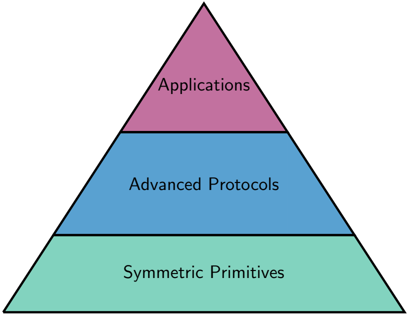


Problem: Designing new symmetric primitives

A need for new primitives

Protocols requiring new primitives:

- ⋆ **FHE**: Fully Homomorphic Encryption
- ⋆ **MPC**: Multiparty Computation
- ⋆ **ZK**: Systems of Zero-Knowledge proofs
  Example: SNARKs, STARKs, Bulletproofs



Problem: Designing new symmetric primitives

And analyse their security!

Block ciphers

⋆ input: n-bit block

$$x \in \mathbb{F}_2^n$$

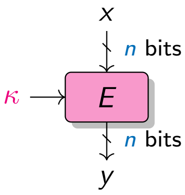
⋆ parameter: k-bit key

$$\kappa \in \mathbb{F}_2^k$$

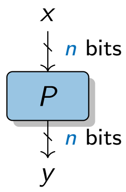
⋆ output: n-bit block

$$y = E_\kappa(x) \in \mathbb{F}_2^n$$

⋆ symmetry: E and E^{-1} use the same κ



(a) *Block cipher*



(b) *Random permutation*

Block ciphers

⋆ input: n-bit block

$$x \in \mathbb{F}_2^n$$

⋆ parameter: k-bit key

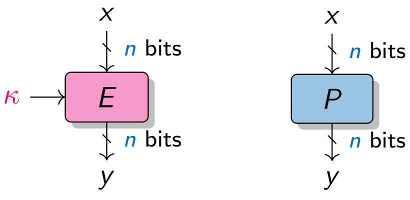
$$\kappa \in \mathbb{F}_2^k$$

⋆ output: n-bit block

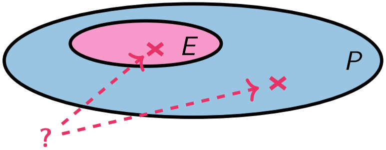
$$y = E_\kappa(x) \in \mathbb{F}_2^n$$

⋆ symmetry: E and E^{-1} use the same κ

A block cipher is a family of 2^k permutations of $\mathbb{F}_2^n$.



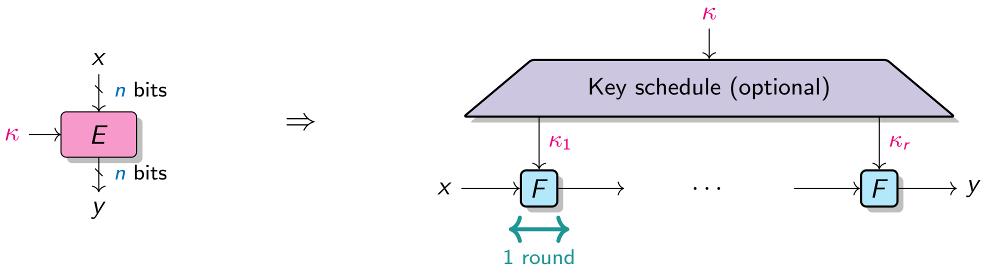
(a) *Block cipher* **(b)** *Random permutation*



Iterated constructions

How to build an efficient block cipher?

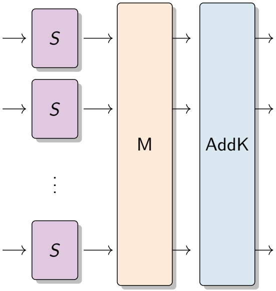
By iterating a round function.



Performance constraints! The primitive must be fast.

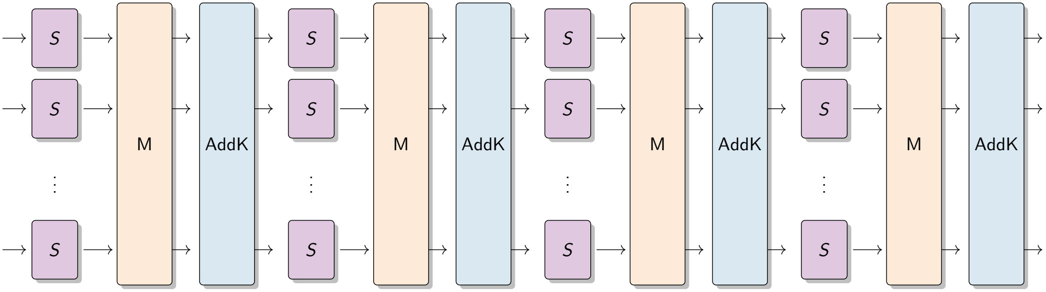
SPN construction

SPN = Substitution Permutation Networks



SPN construction

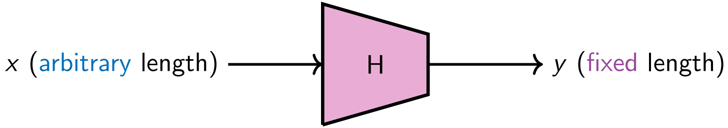
SPN = Substitution Permutation Networks



Hash functions

Definition

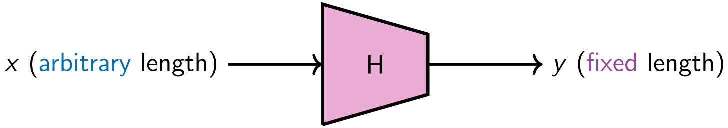
Hash function: $H : \mathbb{F}_q^\ell \to \mathbb{F}_q^h, x \mapsto y = H(x)$ where ℓ is arbitrary and h is fixed.



Hash functions

Definition

Hash function: $H : \mathbb{F}_q^{\ell} \to \mathbb{F}_q^{h}, x \mapsto y = H(x)$ where ℓ is arbitrary and h is fixed.



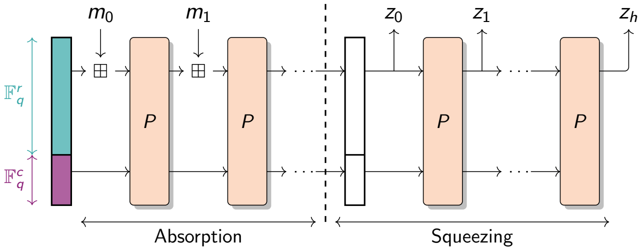
- ⋆ **Preimage resistance**: Given y it must be *infeasible* to find x s.t. $H(x) = y$.
- ⋆ **Collision resistance**: It must be *infeasible* to find $x \neq x'$ s.t. $H(x) = H(x')$.

Sponge construction

Sponge construction

Parameters:

- ⋆ rate $r > 0$
- ⋆ capacity $c > 0$
- ⋆ permutation of $\mathbb{F}_q^n$ $(n = r + c)$

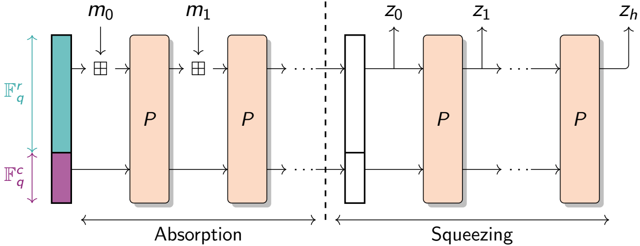


Sponge construction

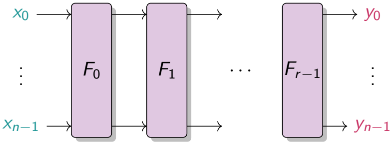
Sponge construction

Parameters:

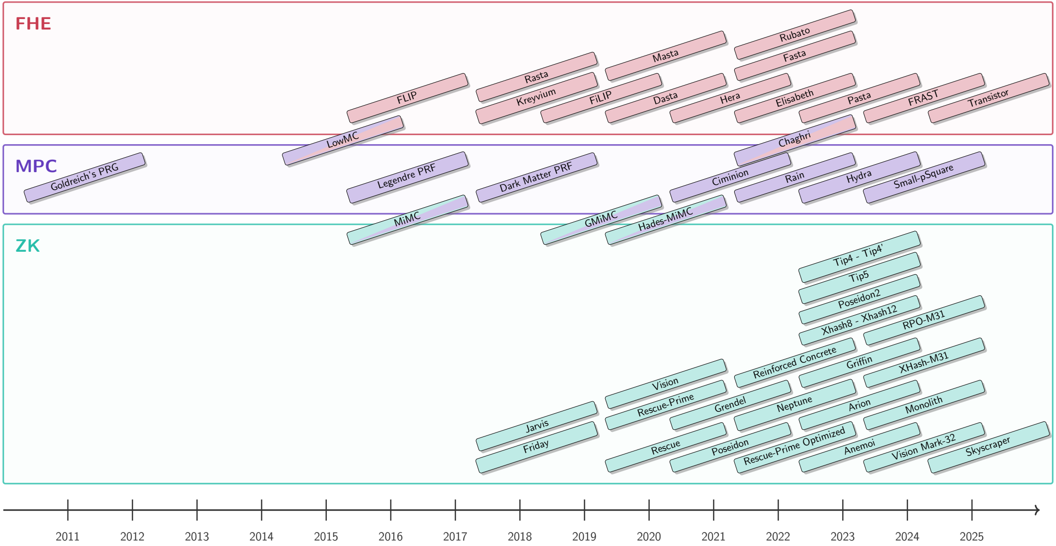
- ⋆ rate $r > 0$
- ⋆ capacity $c > 0$
- ⋆ permutation of $\mathbb{F}_q^n$ $(n = r + c)$



P is an iterated construction



New symmetric primitives



Performance metric

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

Performance metric

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

"It depends"

Performance metric

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

"It depends"

Example

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

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

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

Performance metric

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

"It depends"

Example

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

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

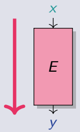
$t_0 = a \cdot x$
$t_1 = t_0 + b$
$t_2 = t_1 \times t_1$
$t_3 = t_2 \times t_1$
$t_4 = c \cdot x$
$t_5 = t_4 + d$
$t_6 = t_3 \times t_5$
$t_7 = e \cdot x$
$t_8 = t_6 + t_7$

3 constraints

Comparison with the traditional case

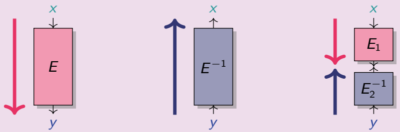
Traditional case

$$y \leftarrow E(x)$$



Arithmetization-oriented

$$y \leftarrow E(x) \quad \text{and} \quad y == E(x)$$



Comparison with the traditional case

Traditional case

$$y \leftarrow E(x)$$

- ⋆ Optimized for:
  implementation in software/hardware

Arithmetization-oriented

$$y \leftarrow E(x) \quad \text{and} \quad y == E(x)$$

- ⋆ Optimized for:
  integration within advanced protocols

Comparison with the traditional case

Traditional case

$$y \leftarrow E(x)$$

- Optimized for:
  implementation in software/hardware

- Alphabet size:
  $\mathbb{F}_2^n$, with $n \simeq 4, 8$

  Ex: Field of AES: $\mathbb{F}_{2^n}$ where $n = 8$

Arithmetization-oriented

$$y \leftarrow E(x) \quad \text{and} \quad y == E(x)$$

- Optimized for:
  integration within advanced protocols

- Alphabet size:
  $\mathbb{F}_q$, with $q \in \{2^n, p\}, p \simeq 2^n,\ n \geq 64$

  Ex: Scalar Field of Curve BLS12-381: $\mathbb{F}_p$ where

  $p =$ 0x73eda753299d7d483339d80809a1d805
  53bda402fffe5bfeffffffff00000001

Comparison with the traditional case

Traditional case

$$y \leftarrow E(x)$$

- ⋆ Optimized for:
  implementation in software/hardware
- ⋆ Alphabet size:
  $\mathbb{F}_2^n$, with $n \simeq 4, 8$
- ⋆ Operations:
  logical gates/CPU instructions

Arithmetization-oriented

$$y \leftarrow E(x) \quad \text{and} \quad y == E(x)$$

- ⋆ Optimized for:
  integration within advanced protocols
- ⋆ Alphabet size:
  $\mathbb{F}_q$, with $q \in \{2^n, p\}, p \simeq 2^n$, $n \geq 64$
- ⋆ Operations:
  large finite-field arithmetic

Comparison with the traditional case

Traditional case

$$y \leftarrow E(x)$$

- ⋆ Optimized for:
  implementation in software/hardware
- ⋆ Alphabet size:
  $\mathbb{F}_2^n$, with $n \simeq 4, 8$
- ⋆ Operations:
  logical gates/CPU instructions

Cryptanalysis

Decades of analysis

Arithmetization-oriented

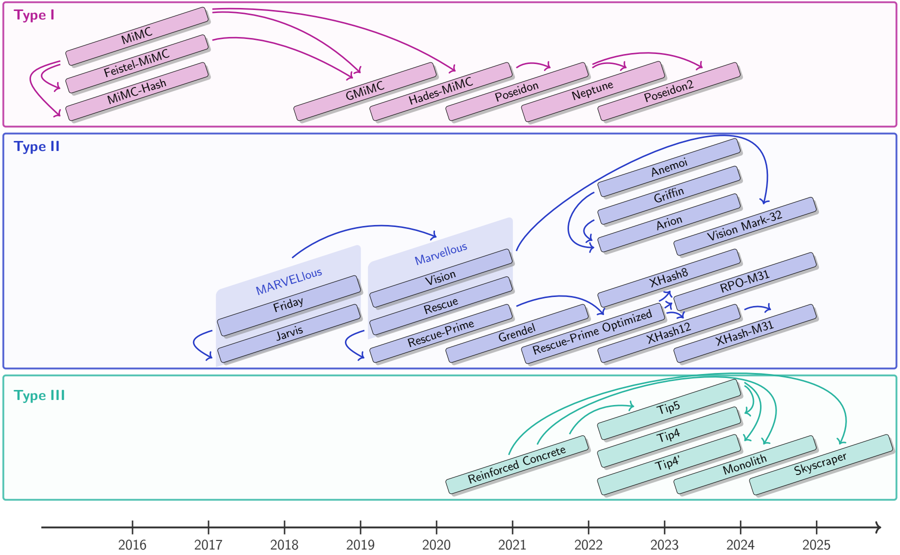
$$y \leftarrow E(x) \quad \text{and} \quad y == E(x)$$

- ⋆ Optimized for:
  integration within advanced protocols
- ⋆ Alphabet size:
  $\mathbb{F}_q$, with $q \in \{2^n, p\}, p \simeq 2^n,\ n \geq 64$
- ⋆ Operations:
  large finite-field arithmetic

Cryptanalysis

$\leq$ 8 years of analysis

ZKP Primitives overview



DESIGN

Design

Design

Cryptanalysis

Design

Design

Type I
- MiMC [AGRRT16] / Feistel-MiMC [AGRRT16]
- Poseidon [GKRRS21]

Type II
- Rescue [AABDS20] / Rescue-Prime [SAD20]
- Anemoi [BBCPSVW23]

Type III
- Reinforced-Concrete [GKLRSW22]
- Skyscraper [BGKKRSS25]

Cryptanalysis

Type I: Low-degree Primitives

Examples:

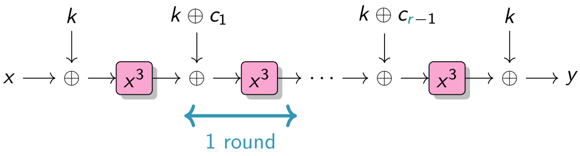
MiMC [AGRRT16] / Feistel-MiMC [AGRRT16]

Poseidon [GKRRS21]

MiMC / Feistel-MiMC

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

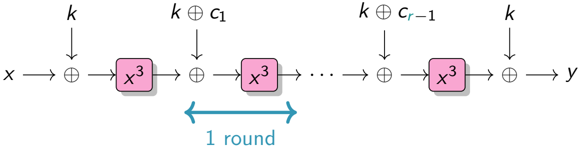
- ⋆ n-bit blocks (n odd ≈ 129): $x \in \mathbb{F}_{2^n}$
- ⋆ n-bit key: $k \in \mathbb{F}_{2^n}$
- ⋆ decryption : replacing x^3 by x^s where $s = (2^{n+1} - 1)/3$
- ⋆ 82 rounds when $n = 129$

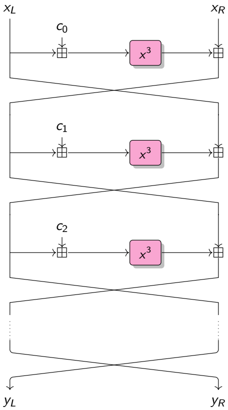


MiMC / Feistel-MiMC

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

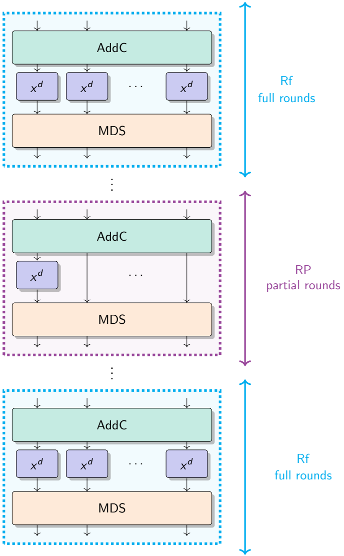
- n-bit blocks (n odd ≈ 129): $x \in \mathbb{F}_{2^n}$
- n-bit key: $k \in \mathbb{F}_{2^n}$
- decryption : replacing x^3 by x^s where $s = (2^{n+1} - 1)/3$
- 82 rounds when $n = 129$





Feistel-MiMC

Poseidon



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

- ⋆ S-box:

$$x \mapsto x^3$$

- ⋆ Nb rounds:

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

Type I: Low-degree Primitives

Fast in plain

Many rounds

Often more constraints

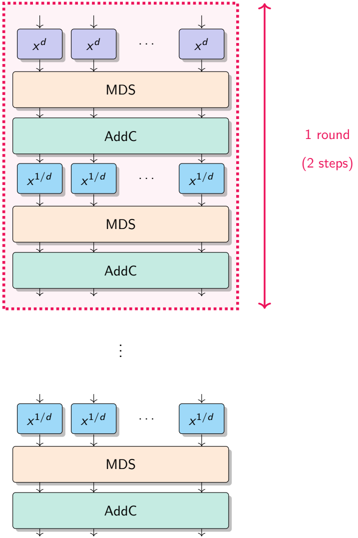
Type II: Primitives based on equivalence

Examples:

Rescue [AABDS20] / Rescue-Prime [SAD20]

Anemoi [BBCPSVW23]

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)

Our approach

Need: verification using few multiplications.

Our approach

Need: verification using few multiplications.

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

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

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

Our approach

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

⋆ **First 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

Our approach

Need: verification using few multiplications.

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

$y \leftarrow E(x)$ $\rightsquigarrow$ E: low degree $\qquad$ $y == E(x)$ $\rightsquigarrow$ E: low degree

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

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

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

$y \leftarrow F(x)$ $\rightsquigarrow$ F: high degree $\qquad$ $v == G(u)$ $\rightsquigarrow$ 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

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

Advantages of CCZ-equivalence

If $F : \mathbb{F}_q \rightarrow \mathbb{F}_q$ and $G : \mathbb{F}_q \rightarrow \mathbb{F}_q$ are **CCZ-equivalent**. Then

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

Differential uniformity

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

Advantages of CCZ-equivalence

If $F : \mathbb{F}_q \rightarrow \mathbb{F}_q$ and $G : \mathbb{F}_q \rightarrow \mathbb{F}_q$ are **CCZ-equivalent**. Then

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

Differential uniformity

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

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

Linearity

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

Advantages of CCZ-equivalence

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

- ⋆ Verification is the same: if $y \leftarrow F(x)$, $v \leftarrow G(u)$ and $(u, v) = \mathcal{L}(x, y)$

$$y == F(x)? \quad \iff \quad v == G(u)?$$

Advantages of CCZ-equivalence

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

- Verification is the same: if $y \leftarrow F(x)$, $v \leftarrow G(u)$ and $(u, v) = \mathcal{L}(x, y)$

$$y == F(x)? \iff v == G(u)?$$

- The degree is **not preserved**.

Example

in $\mathbb{F}_p$ where

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

if $F(x) = x^5$ then $F^{-1}(x) = x^{5^{-1}}$ where

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

Advantages of CCZ-equivalence

If $F : \mathbb{F}_q \rightarrow \mathbb{F}_q$ and $G : \mathbb{F}_q \rightarrow \mathbb{F}_q$ are **CCZ-equivalent**. Then

- ⋆ Verification is the same: if $y \leftarrow F(x)$, $v \leftarrow G(u)$ and $(u, v) = \mathcal{L}(x, y)$

$$y == F(x)? \iff v == G(u)?$$

- ⋆ The degree is **not preserved**.

Example

in $\mathbb{F}_p$ where

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

if $F(x) = x^5$ then $F^{-1}(x) = x^{5^{-1}}$ where

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

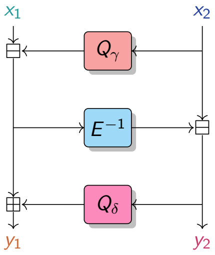
The Flystel

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

Butterfly + Feistel ⇒ Flystel

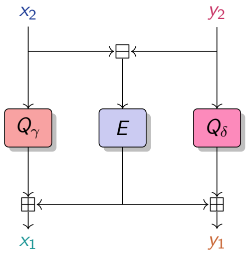
A 3-round Feistel-network with
$Q_\gamma : \mathbb{F}_q \rightarrow \mathbb{F}_q$ and $Q_\delta : \mathbb{F}_q \rightarrow \mathbb{F}_q$ two quadratic functions, and $E : \mathbb{F}_q \rightarrow \mathbb{F}_q$ a permutation

High-Degree permutation



Open Flystel $\mathcal{H}$.

Low-Degree function



Closed Flystel $\mathcal{V}$.

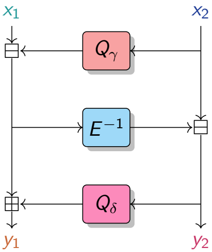
The Flystel

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

Butterfly + Feistel $\Rightarrow$ Flystel

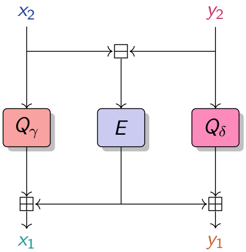
A 3-round Feistel-network with
$Q_\gamma : \mathbb{F}_q \rightarrow \mathbb{F}_q$ and $Q_\delta : \mathbb{F}_q \rightarrow \mathbb{F}_q$ two quadratic functions, and $E : \mathbb{F}_q \rightarrow \mathbb{F}_q$ a permutation

High-Degree permutation



Open Flystel $\mathcal{H}$.

Low-Degree function



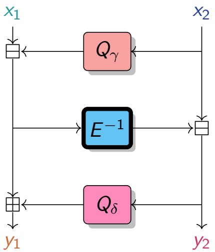
Closed Flystel $\mathcal{V}$.

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

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

$p =$ 0x73eda753299d7d483339d80809a1d805 53bda402fffe5bfeffffffff00000001

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

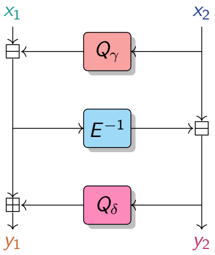
$5^{-1} =$ 0x2e5f0fbadd72321ce14a56699d73f002 217f0e679998f19933333332cccccccd

Advantage of CCZ-equivalence

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

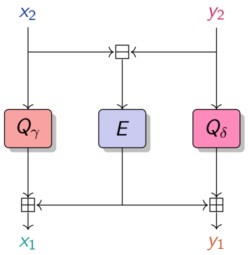
$$(y_1, y_2) == \mathcal{H}(x_1, x_2) \Leftrightarrow (x_1, y_1) == \mathcal{V}(x_2, y_2)$$

High-Degree permutation



Open Flystel $\mathcal{H}$.

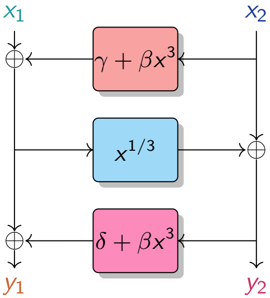
Low-Degree function



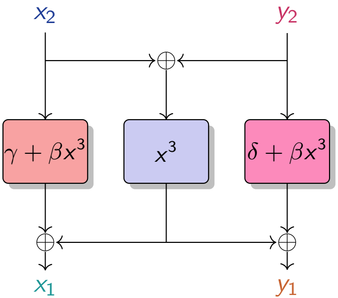
Closed Flystel $\mathcal{V}$.

FLYSTEL in $\mathbb{F}_{2^n}$, n odd

$$Q_\gamma(x) = \gamma + \beta x^3\,, \quad Q_\delta(x) = \delta + \beta x^3\,, \quad \text{and} \quad E(x) = x^3$$

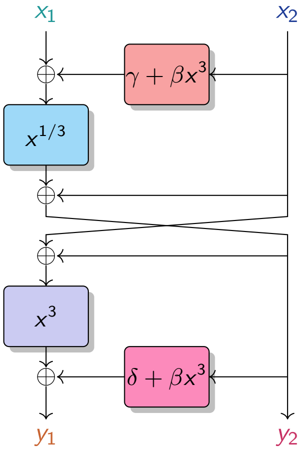


Open `Flystel`$_2$.



Closed `Flystel`$_2$.

Properties of Flystel in $\mathbb{F}_{2^n}$, n odd



Degenerated Butterfly.

Introduced by [PUB16].

Theorems in [LTYW18] state that if $\beta \neq 0$:

- ⋆ Differential properties

$$\delta_{\mathcal{H}} = \delta_{\mathcal{V}} = 4$$

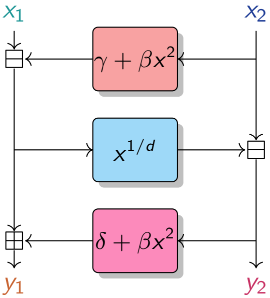
- ⋆ Linear properties

$$\mathcal{W}_{\mathcal{H}} = \mathcal{W}_{\mathcal{V}} = 2^{n+1}$$

- ⋆ Algebraic degree
  - ⋆ Open $\texttt{Flystel}_2$: $\deg_{\mathcal{H}} = n$
  - ⋆ Closed $\texttt{Flystel}_2$: $\deg_{\mathcal{V}} = 2$

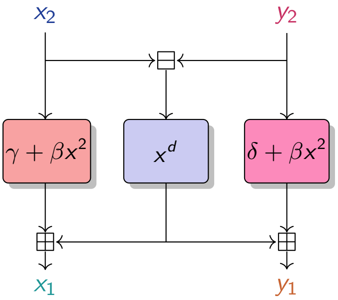
Flystel in $\mathbb{F}_p$

$$Q_\gamma(x) = \gamma + \beta x^2 , \quad Q_\delta(x) = \delta + \beta x^2 , \quad \text{and} \quad E(x) = x^d$$



Open $\texttt{Flystel}_p$.

usually
$d = 3$ or 5.



Closed $\texttt{Flystel}_p$.

Properties of FLYSTEL in $\mathbb{F}_p$

⋆ Differential properties

$\texttt{Flystel}_\texttt{p}$ has a differential uniformity:

$$\delta_{\mathcal{H}} = \max_{a \neq 0, b} \left| \{ x \in \mathbb{F}_p^2, \mathcal{H}(x + a) - \mathcal{H}(x) = b \} \right| \leq d - 1$$

Properties of FLYSTEL in $\mathbb{F}_p$

⋆ Differential properties

$\texttt{Flystel}_\texttt{p}$ has a differential uniformity:

$$\delta_{\mathcal{H}} = \max_{a \neq 0, b} |\{x \in \mathbb{F}_p^2, \mathcal{H}(x+a) - \mathcal{H}(x) = b\}| \leq d - 1$$

Solving the open problem of finding an APN (Almost-Perfect Non-linear) permutation over $\mathbb{F}_p^2$

Properties of Flystel in $\mathbb{F}_p$

⋆ Differential properties

$\texttt{Flystel}_\texttt{p}$ has a differential uniformity:

$$\delta_{\mathcal{H}} = \max_{a \neq 0, b} |\{x \in \mathbb{F}_p^2, \mathcal{H}(x+a) - \mathcal{H}(x) = b\}| \leq d - 1$$

Solving the open problem of finding an APN (Almost-Perfect Non-linear) permutation over $\mathbb{F}_p^2$

⋆ Linear properties

Conjecture:

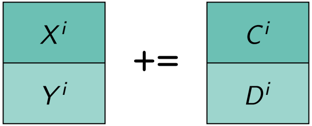
$$\mathcal{W}_{\mathcal{H}} = \max_{a, b \neq 0} \left| \sum_{x \in \mathbb{F}_p^2} exp\left(\frac{2\pi i(\langle a, x\rangle - \langle b, \mathcal{H}(x)\rangle)}{p}\right) \right| \leq p \log p \ ?$$

The SPN Structure

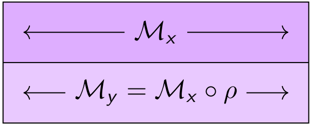
The internal state of Anemoi and its basic operations.

A Substitution-Permutation Network with:

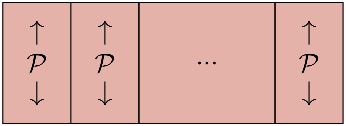
(a) *Internal state.*



(b) *The constant addition.*

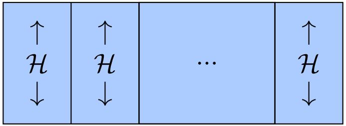


(c) *The diffusion layer.*



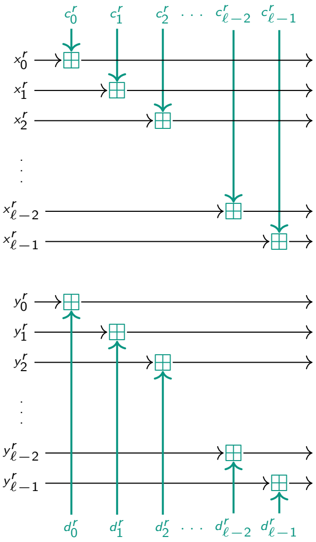
with $\mathcal{P} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$

(d) *The Pseudo-Hadamard Transform.*

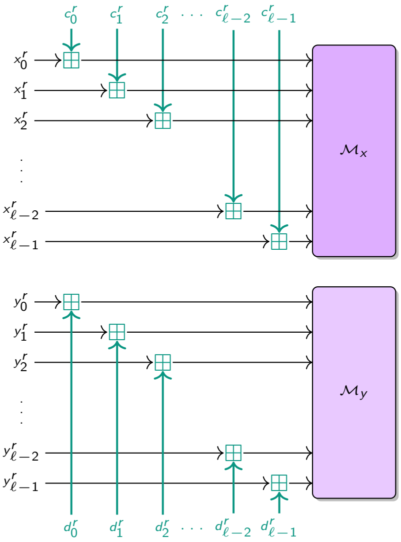


(e) *The S-box layer.*

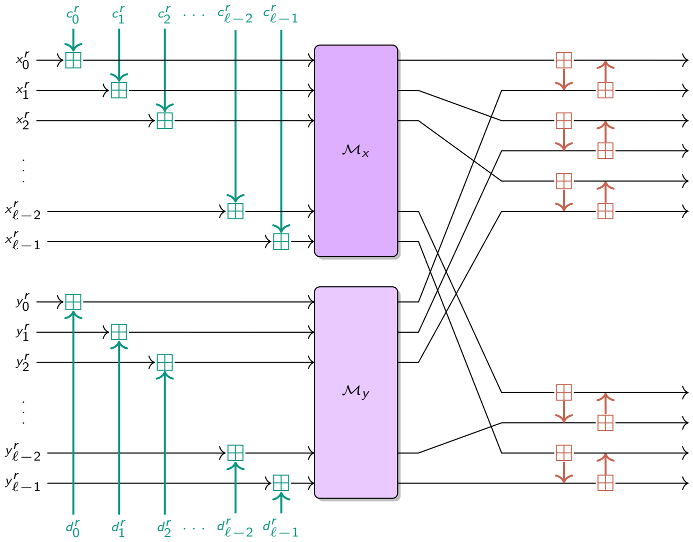
The SPN Structure



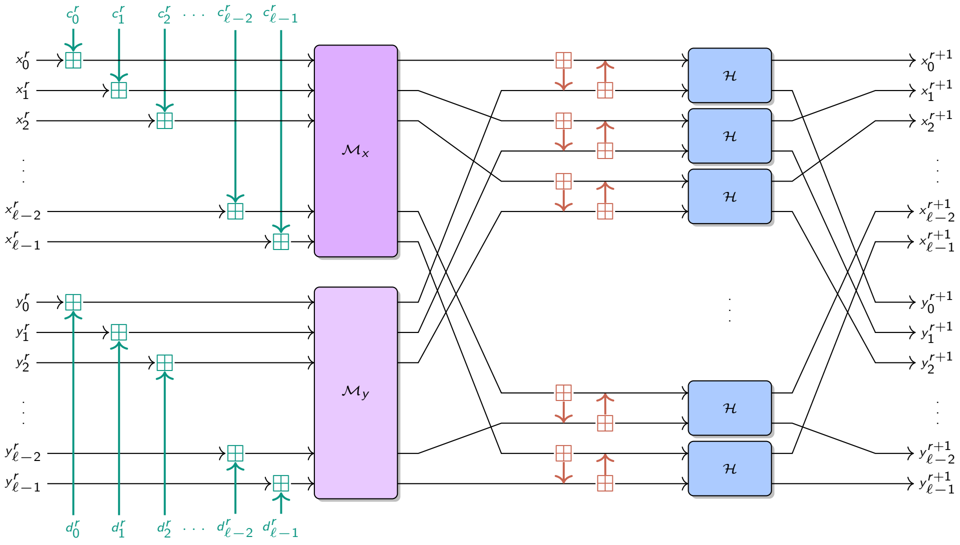
The SPN Structure



The SPN Structure



The SPN Structure



Performance metric

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

"It depends"

Example

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

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

$t_0 = a \cdot x$

$t_1 = t_0 + b$

$t_2 = t_1 \times t_1$

$t_3 = t_2 \times t_1$

$t_4 = c \cdot x$

$t_5 = t_4 + d$

$t_6 = t_3 \times t_5$

$t_7 = e \cdot x$

$t_8 = t_6 + t_7$

3 constraints

Some Benchmarks

	m $(= 2\ell)$	*RP*	*Poseidon*	*Griffin*	*Anemoi*
R1CS	2	208	198	-	**76**
	4	224	232	112	**96**
	6	216	264	-	**120**
	8	256	296	176	**160**
Plonk	2	312	380	-	**191**
	4	560	832	**260**	316
	6	756	1344	-	**460**
	8	1152	1920	**574**	648
AIR	2	156	300	-	**126**
	4	**168**	348	**168**	**168**
	6	**162**	396	-	216
	8	**192**	456	264	288

(a) *when* $d = 3$.

	m $(= 2\ell)$	*RP*	*Poseidon*	*Griffin*	*Anemoi*
R1CS	2	240	216	-	**95**
	4	264	264	**110**	120
	6	288	315	-	**150**
	8	384	363	**162**	200
Plonk	2	320	344	-	**212**
	4	528	696	**222**	344
	6	768	1125	-	**496**
	8	1280	1609	**492**	696
AIR	2	**200**	360	-	210
	4	**220**	440	**220**	280
	6	**240**	540	-	360
	8	**320**	640	360	480

(b) *when* $d = 5$.

Constraint comparison for standard arithmetization, without optimization $(s = 128)$.

Some Benchmarks

*** Numbers to be updated! ***

	m $(=2\ell)$	*RP*	*Poseidon*	*Griffin*	*Anemoi*
R1CS	2	208	198	-	**76**
	4	224	232	112	**96**
	6	216	264	-	**120**
	8	256	296	176	**160**
Plonk	2	312	380	-	**191**
	4	560	832	**260**	316
	6	756	1344	-	**460**
	8	1152	1920	**574**	648
AIR	2	156	300	-	**126**
	4	**168**	348	**168**	**168**
	6	**162**	396	-	216
	8	**192**	456	264	288

(a) *when* $d = 3$.

	m $(=2\ell)$	*RP*	*Poseidon*	*Griffin*	*Anemoi*
R1CS	2	240	216	-	**95**
	4	264	264	**110**	120
	6	288	315	-	**150**
	8	384	363	**162**	200
Plonk	2	320	344	-	**212**
	4	528	696	**222**	344
	6	768	1125	-	**496**
	8	1280	1609	**492**	696
AIR	2	**200**	360	-	210
	4	**220**	440	**220**	280
	6	**240**	540	-	360
	8	**320**	640	360	480

(b) *when* $d = 5$.

Constraint comparison for standard arithmetization, without optimization ($s = 128$).

Type II

Type II: Primitives based on equivalence

Slow in plain

Fewer rounds

Fewer constraints

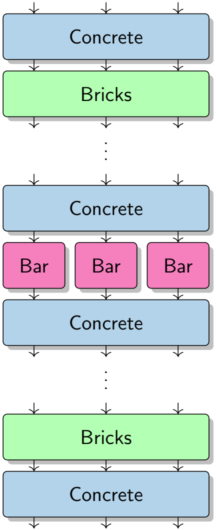
Type III: Primitives using Look-up-Tables

Examples:

Reinforced Concrete [GKLRSW22]

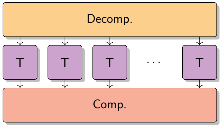
Skyscraper [BGKKRSS25]

Example of Type III: Reinforced Concrete



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

- S-box:

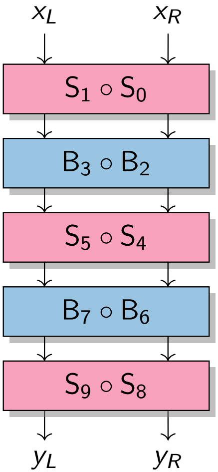


- Nb rounds:

$$R = 7$$

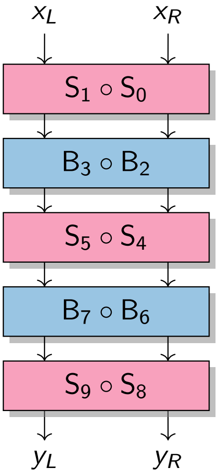
Overview of Skyscraper

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

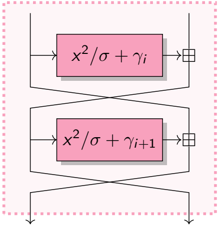


Overview of Skyscraper

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

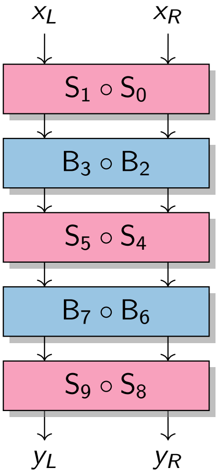


- Square operation S_i
  - Non-invertible x^2
  - Good statistical properties
  - Speed-up via Montgomery

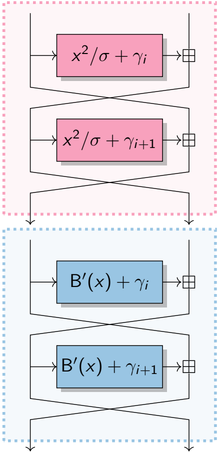


Overview of Skyscraper

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



- Square operation S_i
  - Non-invertible x^2
  - Good statistical properties
  - Speed-up via Montgomery
- Bars operation B_i
  - Non-invertible S-Box B'
  - Applicable to any prime
  - High algebraic degree
  - Speed-up via efficient bit operations

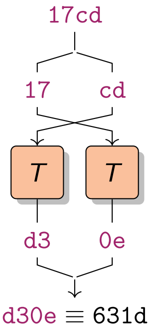


S-Box component B′

Examples: Let $B' : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ for $p = 28657$ (15-bit prime)

$$T(v) = \left(v \oplus \left((\overline{v} \lll 1) \odot (v \lll 2) \odot (v \lll 3)\right)\right) \lll 1$$

Case $n = 1$

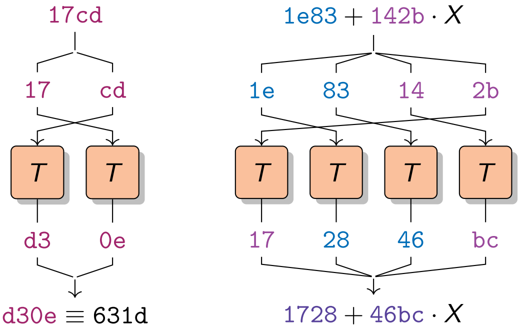


S-Box component B′

Examples: Let $B' : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ for $p = 28657$ (15-bit prime)

$$T(v) = \left(v \oplus \left((\overline{v} \lll 1) \odot (v \lll 2) \odot (v \lll 3)\right)\right) \lll 1$$

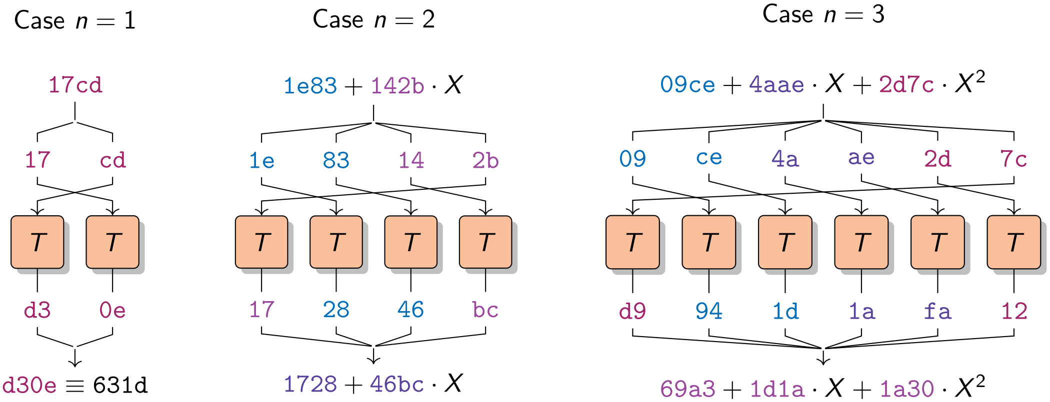
Case $n = 1$ Case $n = 2$



S-Box component B′

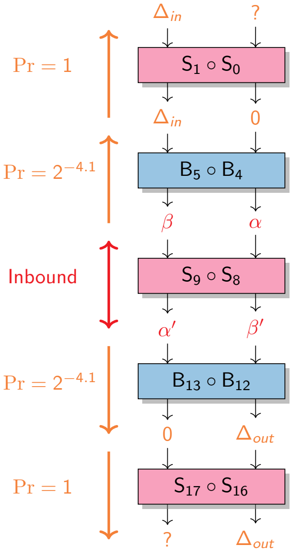
Examples: Let $B' : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ for $p = 28657$ (15-bit prime)

$$T(v) = \left(v \oplus \left((\overline{v} \lll 1) \odot (v \lll 2) \odot (v \lll 3)\right)\right) \lll 1$$



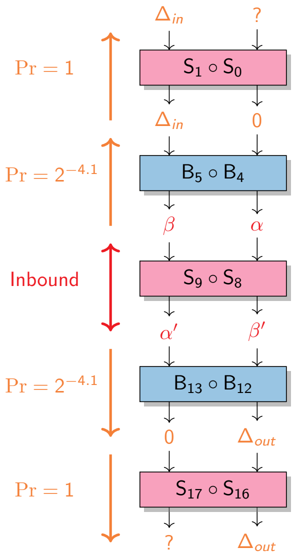
Security Issues

- Recent analysis
  - Rebound attack by A. Bak [Bak25]
  - Truncated differential using $\sim 2^{8.19}$ evaluations
  - Collision attack on 9-round version
  - No security margin



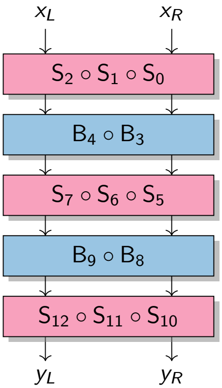
Security Issues

- Recent analysis
  - Rebound attack by A. Bak [Bak25]
  - Truncated differential using $\sim 2^{8.19}$ evaluations
  - Collision attack on 9-round version
  - No security margin
- Skyscraper update
  - Increase number of rounds
  - Additional Squares impact native performance
  - Additional Bars impact ZKP performance



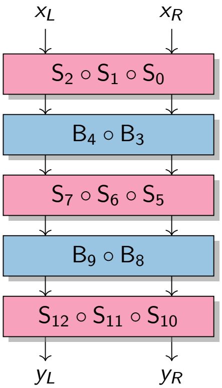
Potential extensions

Alternative 1

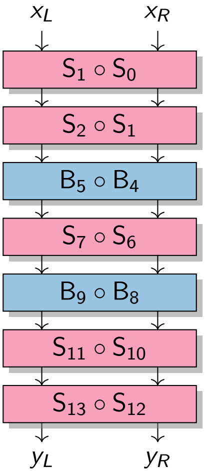


Potential extensions

Alternative 1

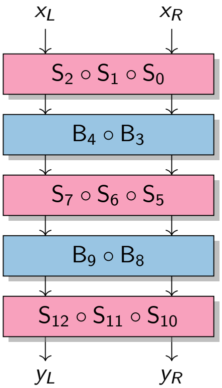


Alternative 2

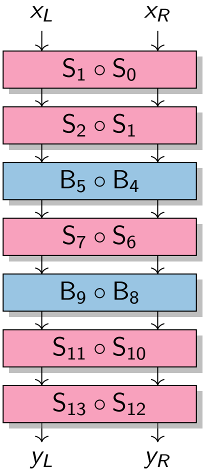


Potential extensions

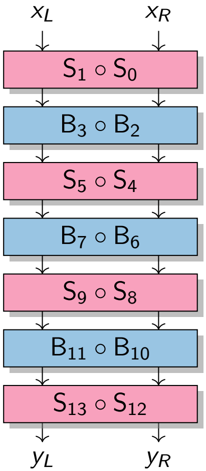
Alternative 1



Alternative 2



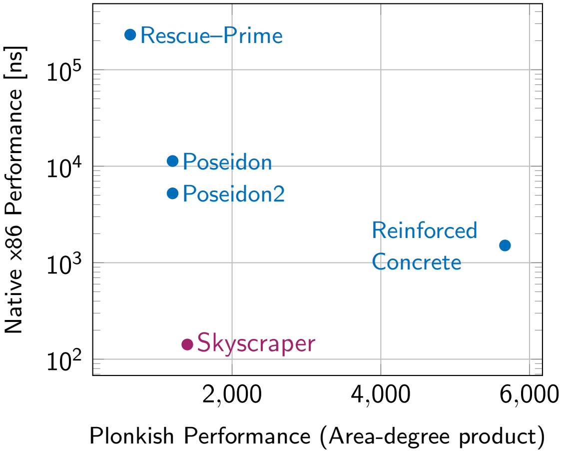
Alternative 3



Some Benchmarks

Performance Comparison for BN254

Hash Function	x86	ZK
Skyscraper	142	1 398
RC	1 510	5 670
Poseidon	11 324	1 200
Poseidon2	5 233	1 200
Rescue–Prime	230 950	630



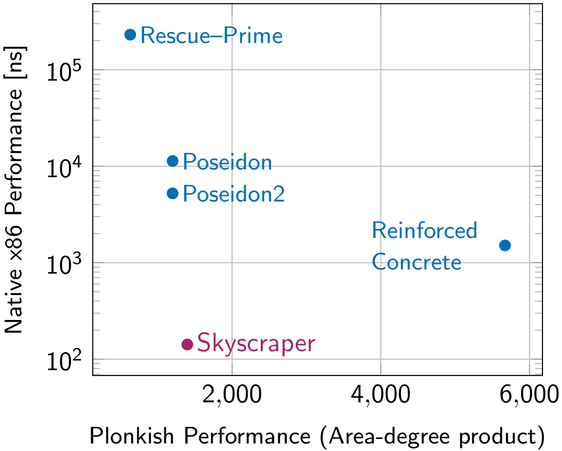
Area-degree product = size of witness matrix × max. degree of polynomial that encodes a gate

Some Benchmarks

*** Numbers to be updated! ***

Performance Comparison for BN254

Hash Function	x86	ZK
Skyscraper	142	1 398
RC	1 510	5 670
Poseidon	11 324	1 200
Poseidon2	5 233	1 200
Rescue–Prime	230 950	630



Area-degree product = size of witness matrix × max. degree of polynomial that encodes a gate

Type III: Primitives using Look-up-Tables

Faster in plain

Fewer rounds

Constraints depending on proof systems

Take-away

	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

CRYPTANALYSIS

Cryptanalysis

Design

Type I

- MiMC [AGRRT16] / Feistel-MiMC [AGRRT16]
- Poseidon [GKRRS21]

Type II

- Rescue [AABDS20] / Rescue-Prime [SAD20]
- Anemoi [BBCPSVW23]

Type III

- Reinforced-Concrete [GKLRSW22]
- Skyscraper [BGKKRSS25]

Cryptanalysis

Cryptanalysis

Design

Type I
- MiMC [AGRRT16] / Feistel-MiMC [AGRRT16]
- Poseidon [GKRRS21]

Type II
- Rescue [AABDS20] / Rescue-Prime [SAD20]
- Anemoi [BBCPSVW23]

Type III
- Reinforced-Concrete [GKLRSW22]
- Skyscraper [BGKKRSS25]

Cryptanalysis

- HO differential attacks [BCP22]
- Algebraic attacks [BBLP22, BBCPSVW23, BBLMOPR24]
- Linear attacks [BB24]

Higher-Order differential attacks

Exact algebraic degree of MiMC [BCP22]

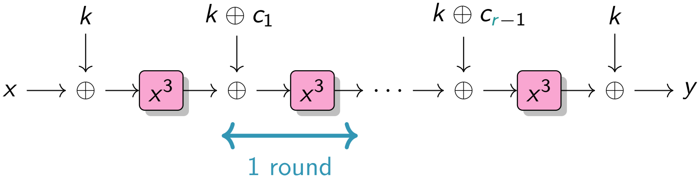
The block cipher MiMC

- Minimize the number of multiplications in $\mathbb{F}_{2^n}$.
- Construction of MiMC$_3$ [AGRRT16]:
  - n-bit blocks (n odd ≈ 129): $x \in \mathbb{F}_{2^n}$
  - n-bit key: $k \in \mathbb{F}_{2^n}$
  - decryption : replacing x^3 by x^s where $s = (2^{n+1} - 1)/3$

$$r := \lceil n \log_3 2 \rceil \, .$$

n	129	255	769	1025
r	82	161	486	647

Number of rounds for MiMC.



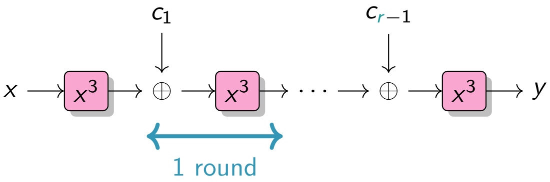
The block cipher MiMC

- Minimize the number of multiplications in $\mathbb{F}_{2^n}$.
- Construction of MiMC$_3$ [AGRRT16]:
  - n-bit blocks (n odd ≈ 129): $x \in \mathbb{F}_{2^n}$
  - n-bit key: $k \in \mathbb{F}_{2^n}$
  - decryption : replacing x^3 by x^s where $s = (2^{n+1} - 1)/3$

$$r := \lceil n \log_3 2 \rceil .$$

n	129	255	769	1025
r	82	161	486	647

Number of rounds for MiMC.



Algebraic degree

Let $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$. 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

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

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

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 $\deg^a(x \mapsto x^3) = 2$.

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

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

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 $= n - 1$

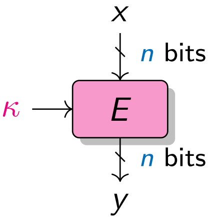
Higher-Order differential attacks

Exploiting a low algebraic degree

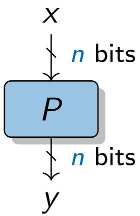
For any affine subspace $\mathcal{V} \subset \mathbb{F}_2^n$ with $\dim \mathcal{V} \geq \deg^a(F) + 1$, we have a 0-sum distinguisher:

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

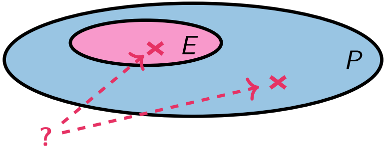
Random permutation: degree $= n - 1$



(a) *Block cipher*

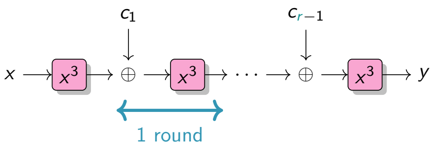


(b) *Random permutation*



First Plateau

C. Bouvier, A. Canteaut and L. Perrin, 2024

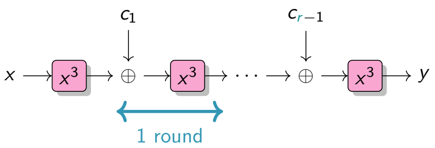


Polynomial representing r rounds of MIMC_3:

$$\mathcal{P}_{3,r}(x) = F_r \circ \dots F_1(x) \ , \ \text{where } F_i = (x + c_{i-1})^3 \ .$$

First Plateau

C. Bouvier, A. Canteaut and L. Perrin, 2024



Polynomial representing r rounds of MIMC$_3$:

$$\mathcal{P}_{3,r}(x) = F_r \circ \ldots F_1(x) \text{ , where } F_i = (x + c_{i-1})^3 \text{ .}$$

Upper bound [EGLORSW20]:

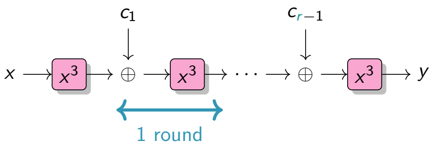
$$\lceil r \log_2 3 \rceil \text{ .}$$

Aim: determine

$$B_3^r := \max_c \deg^a(\mathcal{P}_{3,r}) \text{ .}$$

First Plateau

C. Bouvier, A. Canteaut and L. Perrin, 2024



Polynomial representing r rounds of MIMC$_3$:

$$\mathcal{P}_{3,r}(x) = F_r \circ \ldots F_1(x) \text{ , where } F_i = (x + c_{i-1})^3 \text{ .}$$

Example

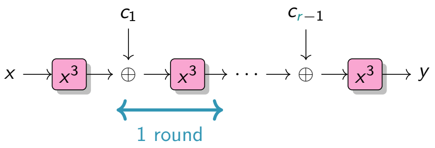
- ⋆ Round 1: $B_3^1 = 2$

$$\mathcal{P}_{3,1}(x) = x^3$$

$$3 = [11]_2$$

First Plateau

C. Bouvier, A. Canteaut and L. Perrin, 2024



Polynomial representing r rounds of MIMC$_3$:

$$\mathcal{P}_{3,r}(x) = F_r \circ \ldots F_1(x) \ , \ \text{where } F_i = (x + c_{i-1})^3 \ .$$

Example

⋆ Round 1: $B_3^1 = 2$

$$\mathcal{P}_{3,1}(x) = x^3$$

$$3 = [11]_2$$

⋆ Round 2: $B_3^2 = 2$

$$\mathcal{P}_{3,2}(x) = x^9 + c_1 x^6 + c_1^2 x^3 + c_1^3$$

$$9 = [1001]_2 \ 6 = [110]_2 \ 3 = [11]_2$$

Observed degree

Definition

There is a **plateau** between rounds r and $r+1$ whenever:

$$B_3^{r+1} = B_3^r \ .$$

Proposition

If $d = 2^j - 1$, there is always a **plateau** between rounds 1 and 2:

$$B_d^2 = B_d^1 \ .$$

Observed degree

Definition

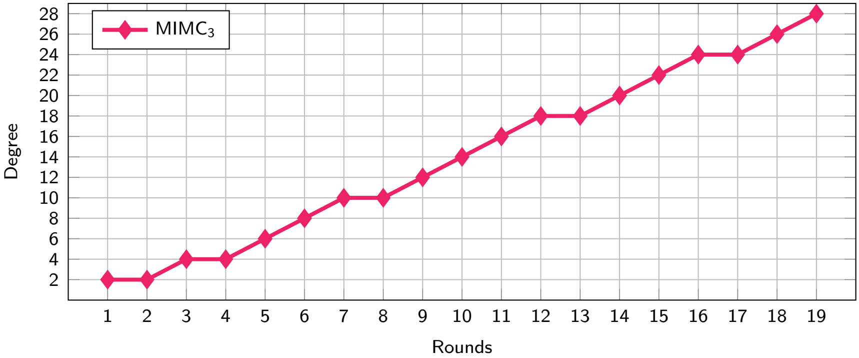
There is a **plateau** between rounds r and $r+1$ whenever:

$$B_3^{r+1} = B_3^r \ .$$

Proposition

If $d = 2^j - 1$, there is always a **plateau** between rounds 1 and 2:

$$B_d^2 = B_d^1 \ .$$



Algebraic degree observed for $n = 31$.

Missing exponents

Proposition

Set of exponents that might appear in the polynomial:

$$\mathcal{E}_{3,r} = \{3 \times j \bmod (2^n - 1) \text{ where } j \text{ is covered by } i,\ i \in \mathcal{E}_{3,r-1}\}$$

Missing exponents

Proposition

Set of exponents that might appear in the polynomial:

$$\mathcal{E}_{3,r} = \{3 \times j \bmod (2^n - 1) \text{ where } j \text{ is covered by } i,\ i \in \mathcal{E}_{3,r-1}\}$$

Example

$$\mathcal{P}_{3,1}(x) = x^3 \quad \text{so} \quad \mathcal{E}_{3,1} = \{3\} .$$

$$3 = [11]_2 \xrightarrow{\text{cover}} \begin{cases} [00]_2 = 0 & \xrightarrow{\times 3} & 0 \\ [01]_2 = 1 & \xrightarrow{\times 3} & 3 \\ [10]_2 = 2 & \xrightarrow{\times 3} & 6 \\ [11]_2 = 3 & \xrightarrow{\times 3} & 9 \end{cases}$$

$$\mathcal{E}_{3,2} = \{0, 3, 6, 9\} , \quad \text{indeed} \quad \mathcal{P}_{3,2}(x) = x^9 + c_1 x^6 + c_1^2 x^3 + c_1^3 .$$

Missing exponents

Proposition

Set of exponents that might appear in the polynomial:

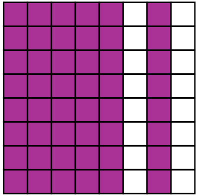
$$\mathcal{E}_{3,r} = \{3 \times j \bmod (2^n - 1) \text{ where } j \text{ is covered by } i,\ i \in \mathcal{E}_{3,r-1}\}$$

Missing exponents: no exponent $2^{2k} - 1$

$$\forall i \in \mathcal{E}_{3,r}, i \not\equiv 5, 7 \bmod 8$$

0	1	2	3	4	5	6	7
8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23
24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47
48	49	50	51	52	53	54	55
56	57	58	59	60	61	62	63

Representation of exponents.



Missing exponents mod8.

Bounding the degree

Theorem

After r rounds of MIMC_3, the algebraic degree is

$$B_3^r \leq 2 \times \lceil \lfloor r \log_2 3 \rfloor / 2 - 1 \rceil$$

Bounding the degree

Theorem

After r rounds of MIMC$_3$, the algebraic degree is

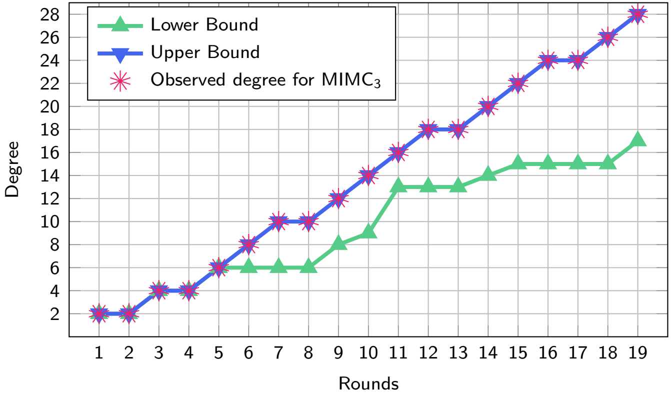
$$B_3^r \leq 2 \times \lceil \lfloor r \log_2 3 \rfloor / 2 - 1 \rceil$$

If $3^r < 2^n - 1$:

- A lower bound

$$B_3^r \geq \max\{\mathrm{wt}(3^i), i \leq r\}$$

- **Upper bound reached for almost 16265 rounds**

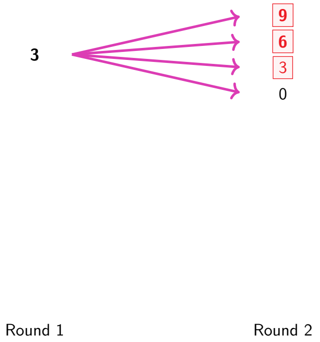


Tracing exponents

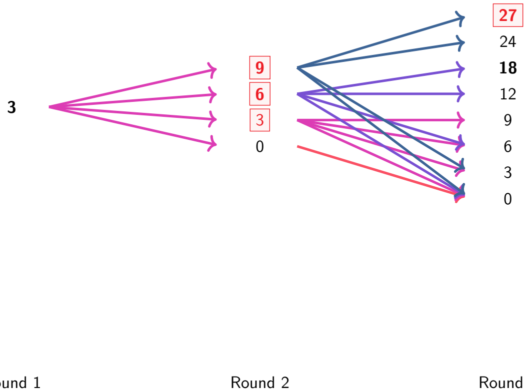
3

Round 1

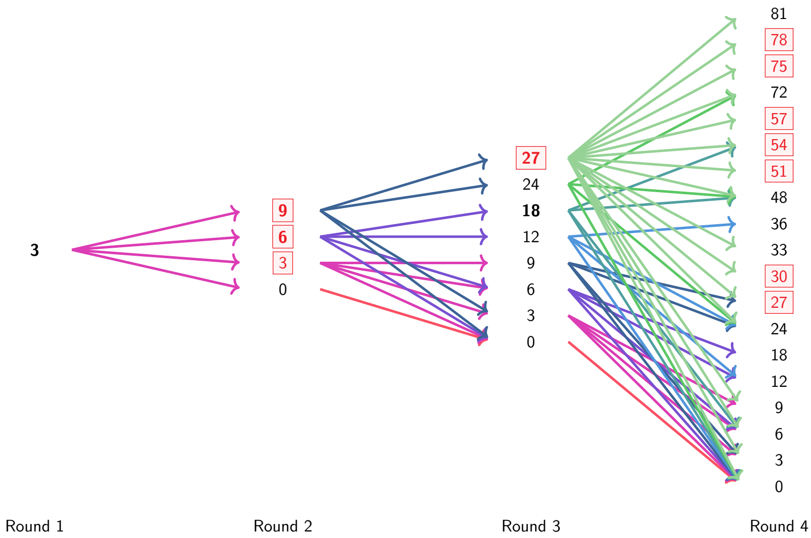
Tracing exponents



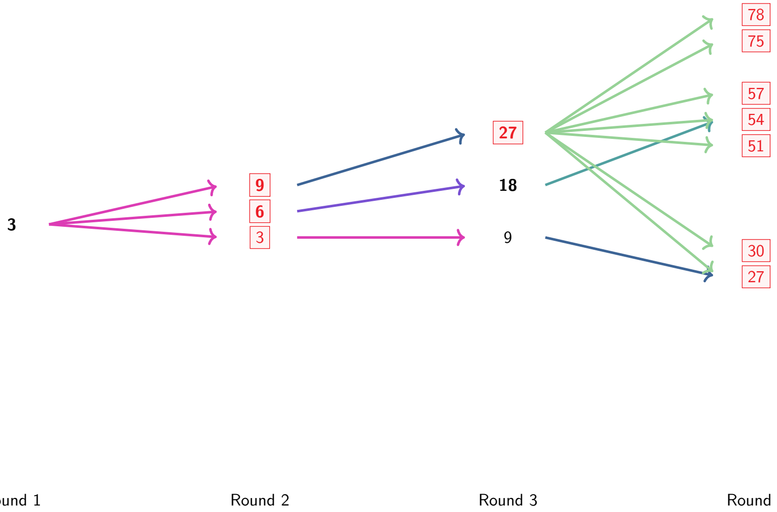
Tracing exponents



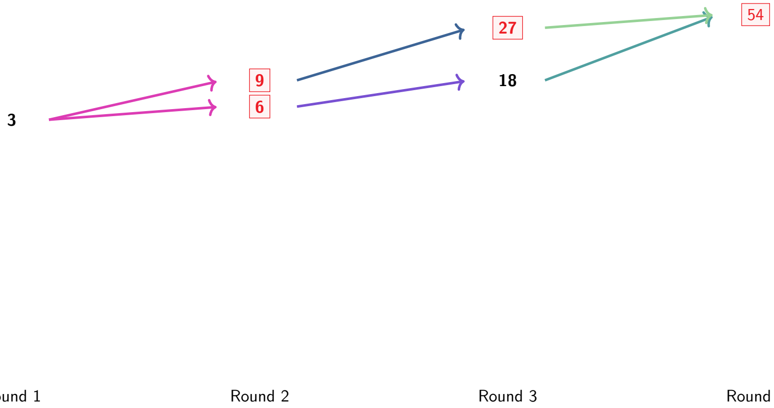
Tracing exponents



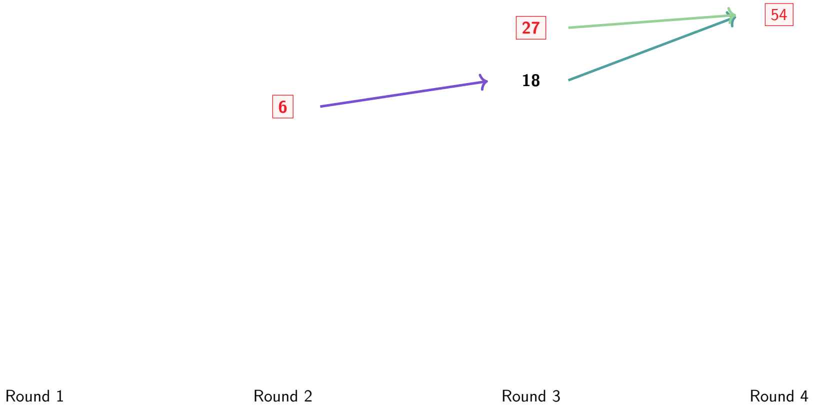
Tracing exponents



Tracing exponents



Tracing exponents

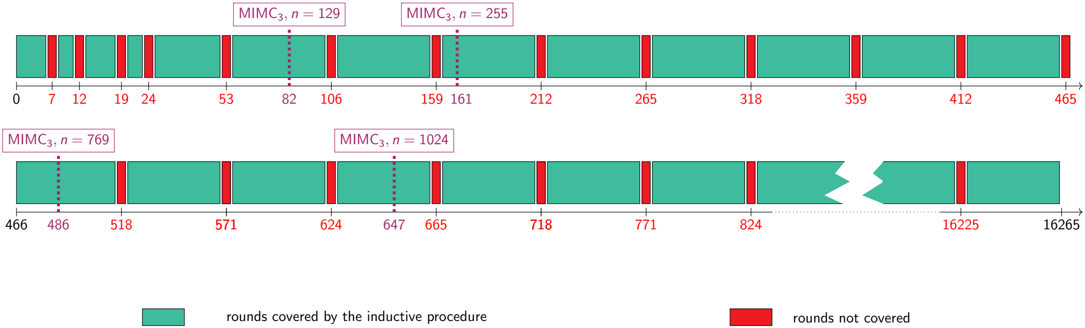


Covered rounds

Idea of the proof:

⋆ inductive proof: existence of "good" ℓ s.t. $\omega_{r-\ell} \in \mathcal{E}_{3,r-\ell} \Rightarrow \omega_r \in \mathcal{E}_{3,r}$

Rounds for which we are able to exhibit a maximum-weight exponent.

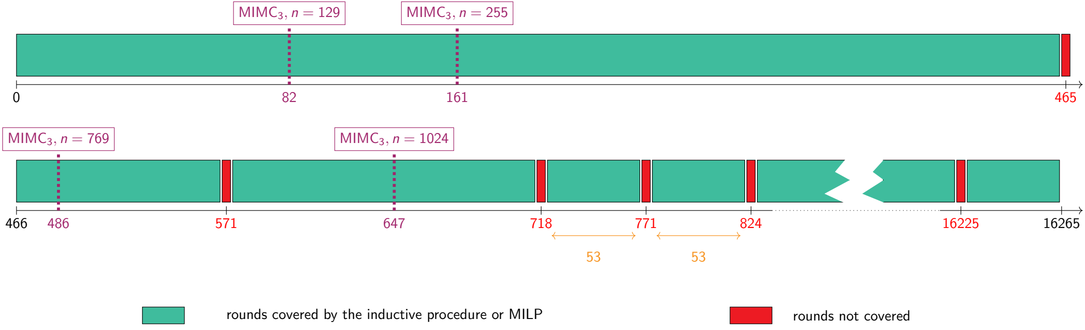


Covered rounds

Idea of the proof:

- ⋆ inductive proof: existence of “good” ℓ s.t. $\omega_{r-\ell} \in \mathcal{E}_{3,r-\ell} \Rightarrow \omega_r \in \mathcal{E}_{3,r}$
- ⋆ MILP solver (`PySCIPOpt`)

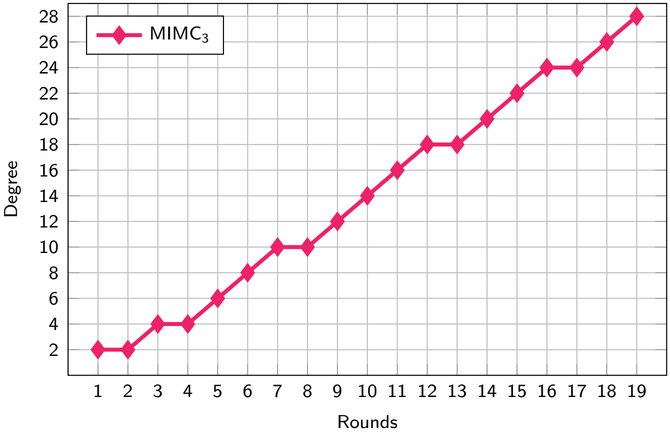
Rounds for which we are able to exhibit a maximum-weight exponent.



Plateau

Proposition

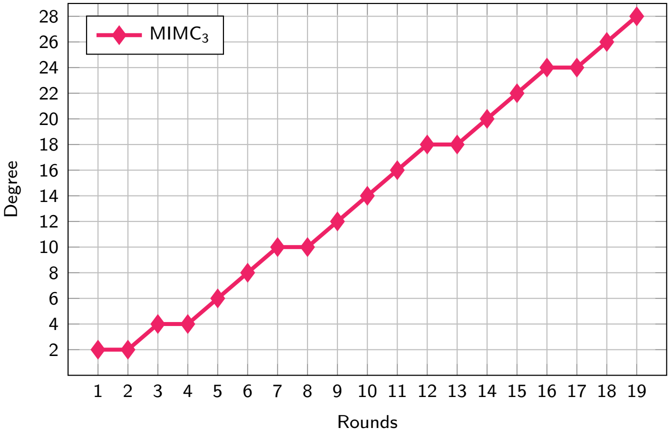
There is a plateau when $k_r = \lfloor r \log_2 3 \rfloor = 1 \bmod 2$ and $k_{r+1} = \lfloor (r+1) \log_2 3 \rfloor = 0 \bmod 2$



Plateau

Proposition

There is a plateau when $k_r = \lfloor r \log_2 3 \rfloor = 1 \bmod 2$ and $k_{r+1} = \lfloor (r+1) \log_2 3 \rfloor = 0 \bmod 2$



If we have a plateau

$$B_3^r = B_3^{r+1} ,$$

Then the next one is

$$B_3^{r+4} = B_3^{r+5}$$

or

$$B_3^{r+5} = B_3^{r+6} .$$

Music in MIMC_3

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

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

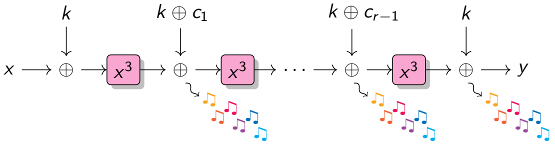
$$\mathfrak{D} = \{\boxed{1}, \boxed{2}, 3, 5, \boxed{7}, \boxed{12}, 17, 29, 41, \boxed{53}, 94, 147, 200, 253, 306, \boxed{359}, \ldots\},$$

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

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

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

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



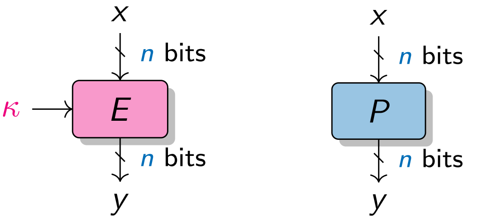
Higher-Order differential attacks

Exploiting a low algebraic degree

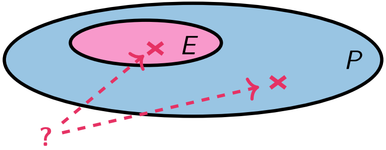
For any affine subspace $\mathcal{V} \subset \mathbb{F}_2^n$ with $\dim \mathcal{V} \geq \deg^a(F) + 1$, we have a 0-sum distinguisher:

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

Random permutation: degree $= n - 1$

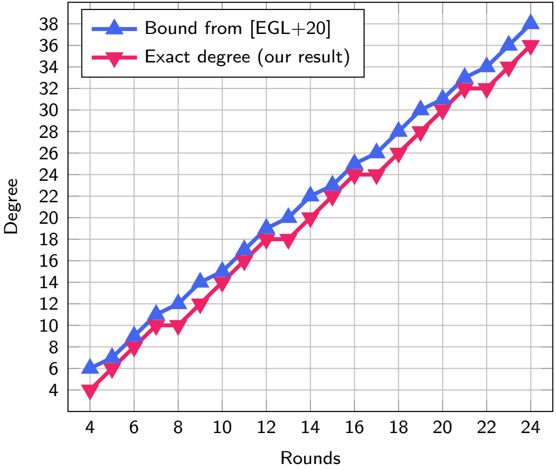


(a) *Block cipher* **(b)** *Random permutation*



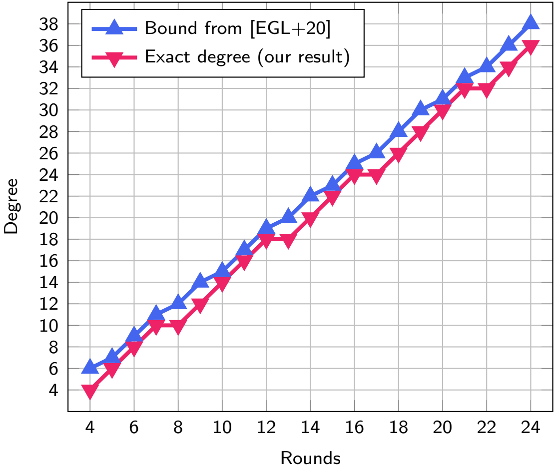
Comparison to previous work

First Bound: $\lceil r \log_2 3 \rceil$ Exact degree: $2 \times \lceil \lfloor r \log_2 3 \rfloor / 2 - 1 \rceil$.



Comparison to previous work

First Bound: $\lceil r \log_2 3 \rceil$ Exact degree: $2 \times \lceil \lfloor r \log_2 3 \rfloor / 2 - 1 \rceil$.



For $n = 129$, $\text{MIMC}_3 = 82$ rounds

Rounds	Time	Data	Source
80/82	2^{128}XOR	2^{128}	[EGL+20]
81/82	2^{128}XOR	2^{128}	**Our**
80/82	2^{125}XOR	2^{125}	**Our**

Secret-key distinguishers ($n = 129$)

Take-away

A better understanding of the algebraic degree of MiMC

- ⋆ guarantee on the degree of MIMC_3
  - ⋆ upper bound on the algebraic degree

$$2 \times \lceil \lfloor r \log_2 3 \rfloor / 2 - 1 \rceil .$$

  - ⋆ bound tight, up to 16265 rounds
- ⋆ minimal complexity for higher-order differential attack

Take-away

A better understanding of the algebraic degree of MiMC

- guarantee on the degree of MIMC_3
  - upper bound on the algebraic degree

$$2 \times \lceil \lfloor r \log_2 3 \rfloor / 2 - 1 \rceil \ .$$

  - bound tight, up to 16265 rounds
- minimal complexity for higher-order differential attack

Missing exponents in the univariate representation

Take-away

A better understanding of the algebraic degree of MiMC

- guarantee on the degree of MIMC_3
  - upper bound on the algebraic degree

$$2 \times \lceil \lfloor r \log_2 3 \rfloor / 2 - 1 \rceil .$$

  - bound tight, up to 16265 rounds
- minimal complexity for higher-order differential attack

Missing exponents in the univariate representation

↓

Bounds on the algebraic degree

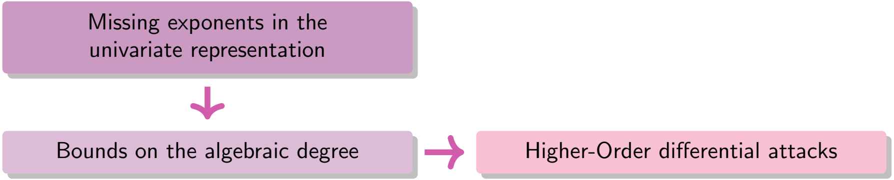
Take-away

A better understanding of the algebraic degree of MiMC

- $\star$ guarantee on the degree of MIMC_3
  - $\star$ upper bound on the algebraic degree

$$2 \times \lceil \lfloor r \log_2 3 \rfloor / 2 - 1 \rceil \; .$$

  - $\star$ bound tight, up to 16265 rounds
- $\star$ minimal complexity for higher-order differential attack



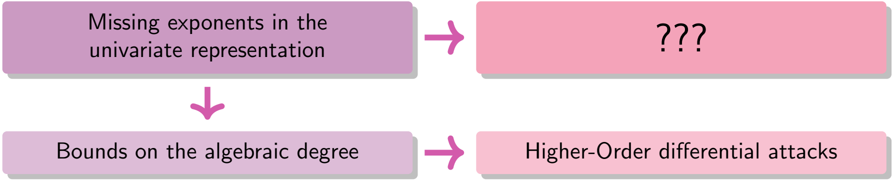
Take-away

A better understanding of the algebraic degree of MiMC

- ⋆ guarantee on the degree of MIMC_3
  - ⋆ upper bound on the algebraic degree

$$2 \times \lceil \lfloor r \log_2 3 \rfloor / 2 - 1 \rceil \ .$$

  - ⋆ bound tight, up to 16265 rounds
- ⋆ minimal complexity for higher-order differential attack



Algebraic attacks

Trick to bypass SPN rounds [BBLP22]

Importance of the modeling [BBCPSVW23]

Importance of the ordering [BBLMOPR24]

CICO Problem

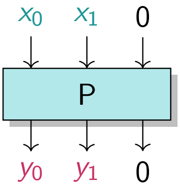
CICO: Constrained Input Constrained Output

Definition

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

The **CICO** problem is:

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



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

CICO Problem

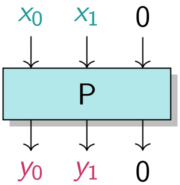
CICO: Constrained Input Constrained Output

Definition

Let $P : \mathbb{F}_q^t \to \mathbb{F}_q^t$ 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 $t = 3,\ u = 1.$

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

- ⋆ Feistel–MiMC [AGRRT16]
- ⋆ Poseidon [GKRRS21]
- ⋆ Rescue–Prime [SAD20]
- ⋆ Reinforced Concrete [GKLRSW22]

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 $\mathcal{P}_j \in \mathbb{F}_q[X_0, \ldots, X_{n-1}]$

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

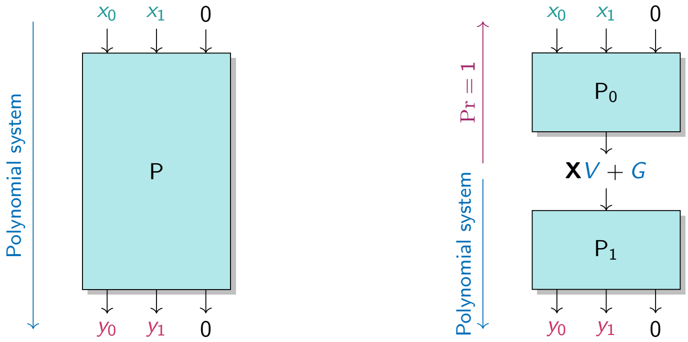
- ⋆ Compute a grevlex order GB (**F5** algorithm)
- ⋆ Convert it into lex order GB (**FGLM** algorithm)
- ⋆ Find the roots in $\mathbb{F}_q^n$ of the GB polynomials using univariate system resolution.

Trick for SPN

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

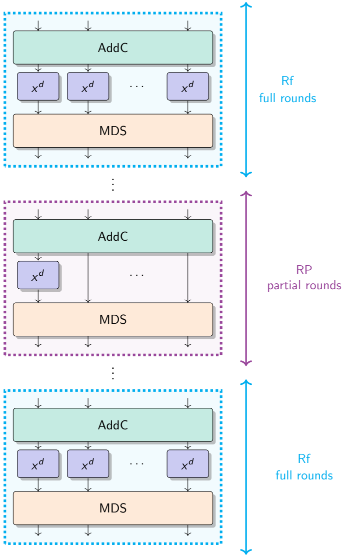
Let $P = P_0 \circ P_1$ be a permutation of $\mathbb{F}_p^3$ and suppose

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



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

Poseidon

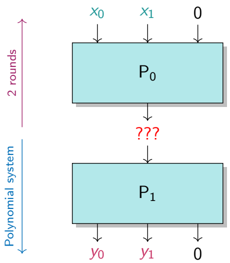


- ⋆ S-box:

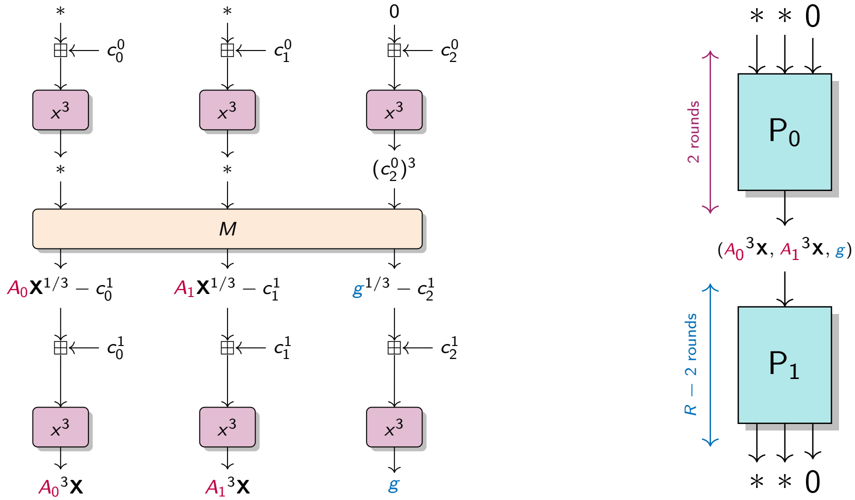
$$x \mapsto x^3$$

- ⋆ Nb rounds:

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

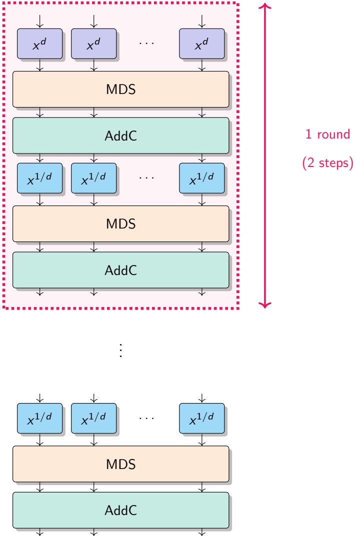


Trick for Poseidon



(a) *First two rounds.* **(b)** *Overview.*

Rescue–Prime



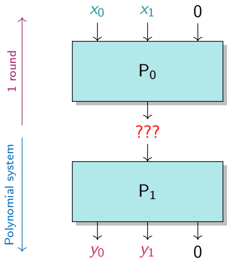
- S-box:

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

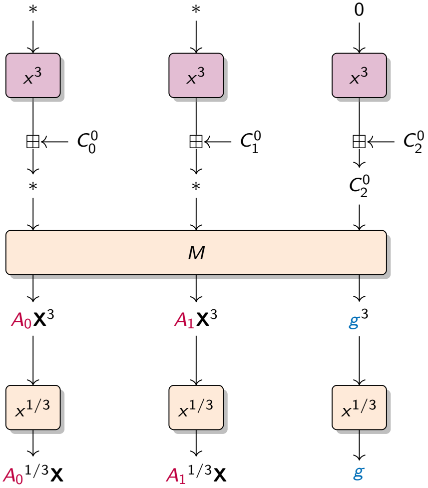
- Nb rounds:

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

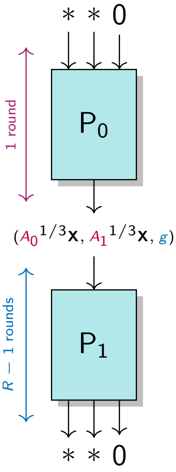
(2 S-boxes per round)



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*

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*

\$26,000

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

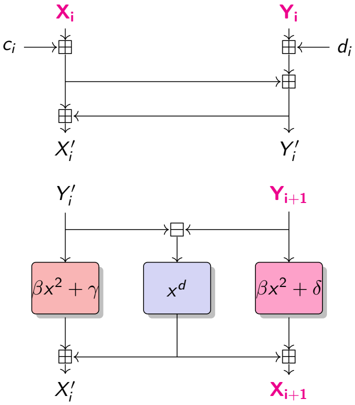
(c) *Poseidon*

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

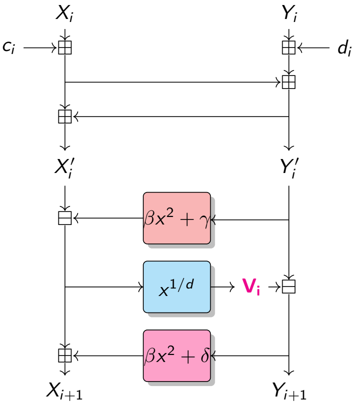
(d) *Reinforced Concrete*

Modeling of Anemoi

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

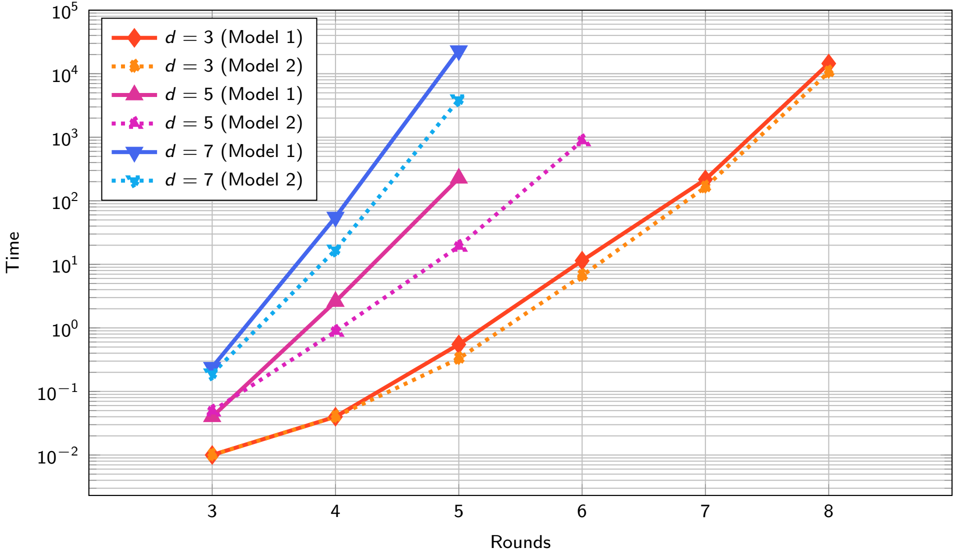


Model 1.



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.

Impact on the security of:

- ⋆ Griffin (CICO solution for 7 out of 10 rounds)
- ⋆ Arion
- ⋆ Anemoi (need some tweak)

Take-away

Lessons for future design:

- ⋆ try as many modeling as possible
- ⋆ try as many ordering as possible
- ⋆ prefer univariate instead of multivariate system
- ⋆ be careful of tricks to bypass rounds

Take-away

Lessons for future design:

- ⋆ try as many modeling as possible
- ⋆ try as many ordering as possible
- ⋆ prefer univariate instead of multivariate system
- ⋆ be careful of tricks to bypass rounds

Algebraic attacks on AOP: a new lucrative business?

- ⋆ Ethereum Challenges (Nov. 2021)

  Feistel-MiMC, Poseidon, Rescue-Prime, Reinforced-Concrete

- ⋆ Ethereum Initiative (Nov. 2024)

  Poseidon

Linear attacks

Solving conjecture for the Flystel [BB24]

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

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

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

Linearity

Definition

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

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

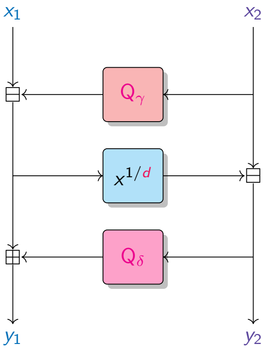
$$\boxed{\mathcal{W}_{u,v}^{F} = q^n \cdot C_{u,v}^{F}}$$

Definition

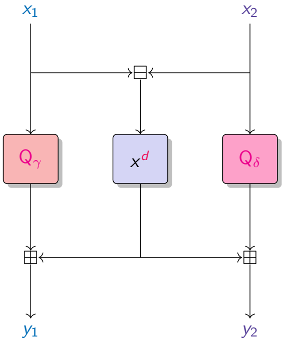
The **Linearity** $\mathcal{L}_F$ of $F : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^m$ is the highest Walsh coefficient.

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

Flystel - Definition



Open variant.

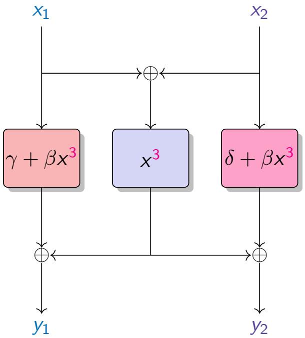


Closed variant.

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

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

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



Closed Flystel.

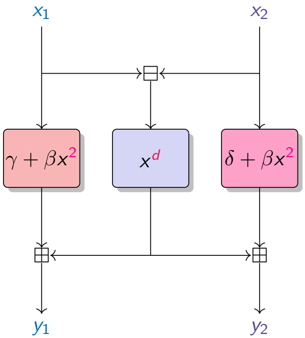
$$\mathcal{L}_F = \max_{u,v \neq 0} \left| \sum_{x \in \mathbb{F}_{2^n}^2} (-1)^{(\langle v, F(x) \rangle - \langle u, x \rangle)} \right|$$

Bound

Linearity bound for the Flystel:

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

Closed Flystel in $\mathbb{F}_p$

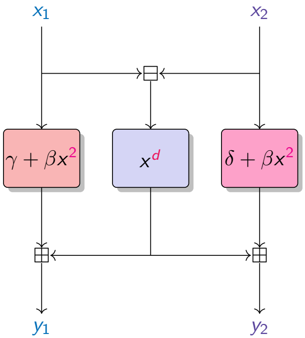


Closed Flystel.

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 $\mathbb{F}_p$



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

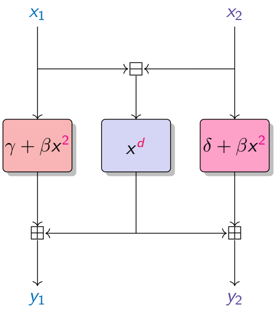
$$\mathcal{L}_f \leq (d-1)\sqrt{p}$$

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.

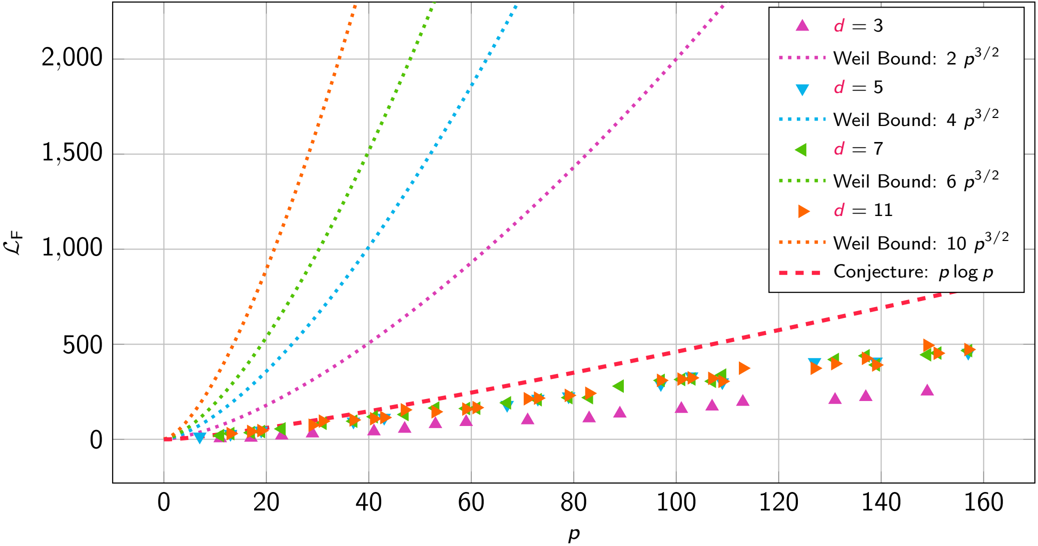
$$\mathcal{L}_F \leq (d-1)p\sqrt{p} \;?$$

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

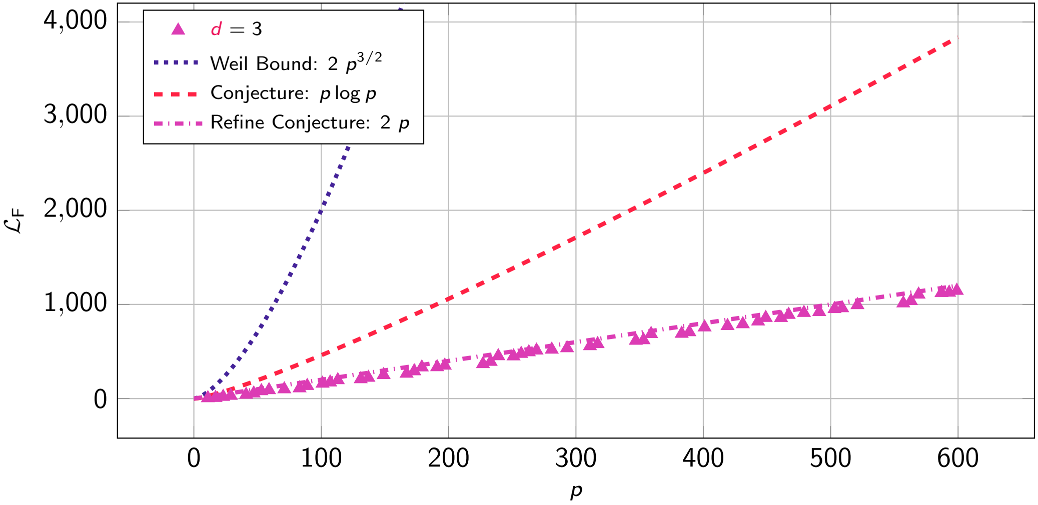
Conjecture

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

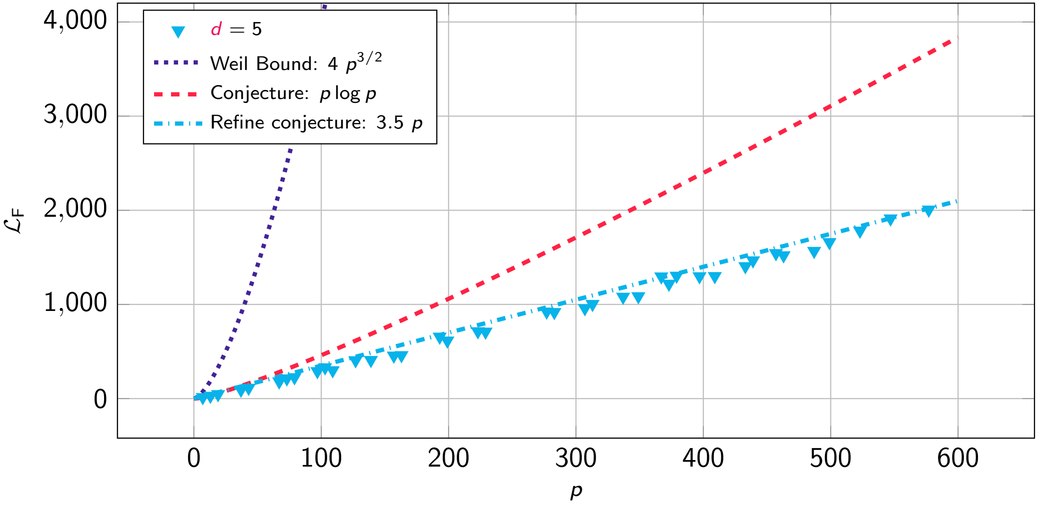
Experimental results



Experimental results ($d = 3$)



Experimental results ($d = 5$)



Exponential sums

T. Beyne and C. Bouvier, 2024

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

$$\mathcal{W}_{u,v}^{\mathsf{F}} = \sum_{x \in \mathbb{F}_q^n} \omega^{(\langle v, \mathsf{F}(x)\rangle - \langle u, x\rangle)} \quad \rightarrow \quad S(f) = \sum_{x \in \mathbb{F}_q^n} e^{\left(\frac{2i\pi}{p}\right) \cdot f(x)} .$$

  - Theorem of Deligne [Del74]
  - Theorem of Denef and Loeser [DL91]
  - Theorem of Rojas-León [Roj06]

Exponential sums

T. Beyne and C. Bouvier, 2024

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

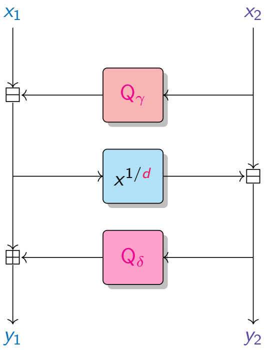
$$\mathcal{W}^{\mathsf{F}}_{u,v} = \sum_{x \in \mathbb{F}_q^n} \omega^{(\langle v, \mathsf{F}(x)\rangle - \langle u, x\rangle)} \quad \rightarrow \quad S(f) = \sum_{x \in \mathbb{F}_q^n} e^{\left(\frac{2i\pi}{p}\right) \cdot f(x)} .$$

  - Theorem of Deligne [Del74]
  - Theorem of Denef and Loeser [DL91]
  - Theorem of Rojas-León [Roj06]

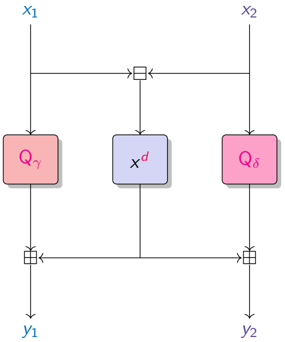
- Functions with 2 variables $\mathsf{F} \in \mathbb{F}_q[x_1, x_2]$.
  - Generalized Butterfly construction
  - 3-round Feistel construction
  - Generalized Flystel construction

Flystel - Definition

Let $x \mapsto x^d$ be a permutation, and Q_γ, Q_γ quadratic functions.



Open variant.



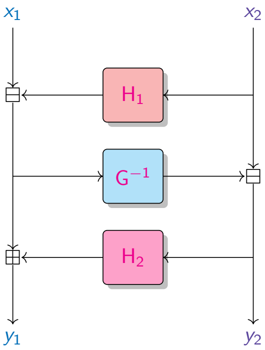
Closed variant.

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

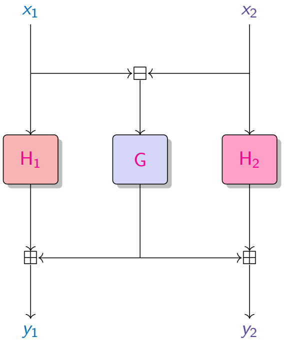
$$\begin{cases} y_1 &= (x_1 - x_2)^d + Q_\gamma(x_1) \\ y_2 &= (x_1 - x_2)^d + Q_\delta(x_2) . \end{cases}$$

Generalized Flystel - Definition

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



Open variant.



Closed variant.

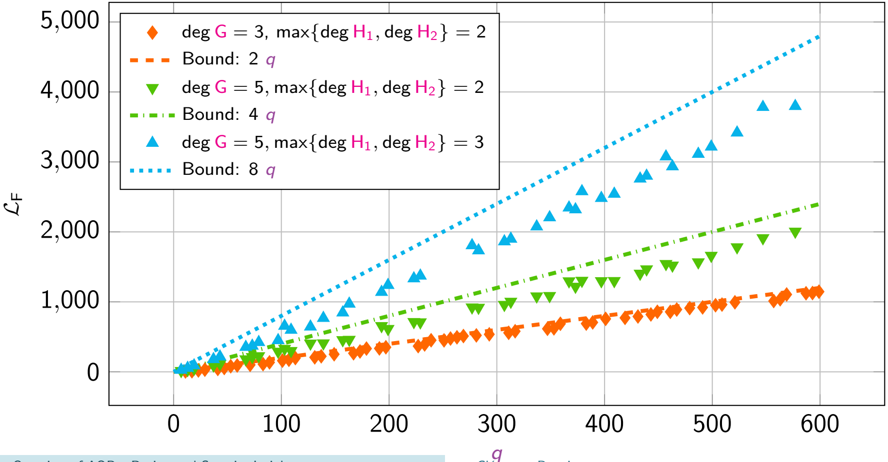
$$\begin{cases} y_1 &= x_1 - \mathsf{H}_1(x_2) + \mathsf{H}_2(x_2 - \mathsf{G}^{-1}(x_1 - \mathsf{H}_1(x_2))) \\ y_2 &= x_2 - \mathsf{G}^{-1}(x_1 - \mathsf{H}_1(x_2)) \,. \end{cases}$$

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

Generalized Flystel - Results

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

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

$$\mathcal{L}_F \leq p \log p \ .$$

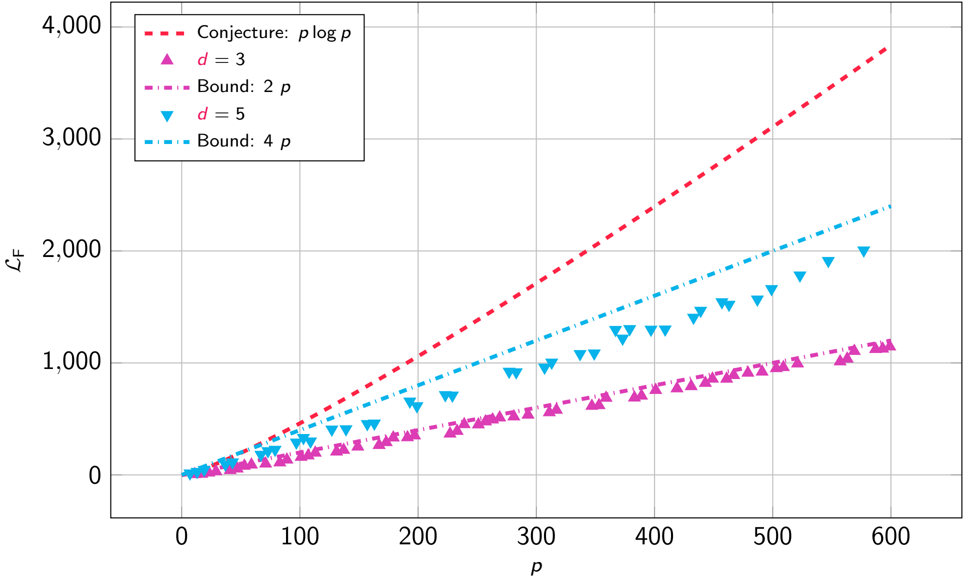
Conjecture proved for $d \leq \log p$

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

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

Solving conjecture



Take-away

- 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

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

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

Take-away

- 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

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

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

Contribute to the cryptanalysis efforts for AOP.

Take-away

- ⋆ 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

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

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

Contribute to the cryptanalysis efforts for AOP.

Perspectives:

- ⋆ Can we refine bounds in particular for small degree functions over smaller prime fields?
- ⋆ Can we generalize to other constructions?

Website

`stap-zoo.com`

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.

Conclusions

⋆ Many new primitives have been proposed

Anemoi, Skyscraper and many others...

Conclusions

- ⋆ Many new primitives have been proposed

  Anemoi, Skyscraper and many others...

- ⋆ Some cryptanalysis progress have been done

  In particular for algebraic attacks.

Conclusions

- Many new primitives have been proposed

  Anemoi, Skyscraper and many others...

- Some cryptanalysis progress have been done

  In particular for algebraic attacks.

Cryptanalysis and design of AOPs remain to be explored

Conclusions

- ⋆ Many new primitives have been proposed

  Anemoi, Skyscraper and many others...

- ⋆ Some cryptanalysis progress have been done

  In particular for algebraic attacks.

Cryptanalysis and design of AOPs remain to be explored

Thank you