Design and Cryptanalysis of Arithmetization-Oriented Primitives.

Clémence Bouvier [1,2]

including joint works with Augustin Bariant[2], Pierre Briaud[1,2], Anne Canteaut[2], Pyrros Chaidos[3], Gaëtan Leurent[2], Léo Perrin[2], Robin Salen[4], Vesselin Velichkov[5,6] and Danny Willems[7,8]

[1]Sorbonne Université, [2]Inria Paris,

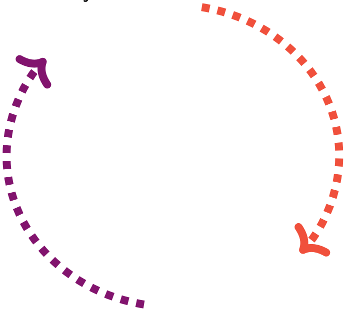
[3]National & Kapodistrian University of Athens, [4]Toposware Inc., Boston,
[5]University of Edinburgh, [6]Clearmatics, London, [7]Nomadic Labs, Paris, [8]Inria and LIX, CNRS

May, 2023

Motivation

Primitives need to be analysed.

Cryptanalysis



Design

Lessons learnt for other designs.

Motivation

Primitives need to be analysed.

Cryptanalysis

- ☞ Algebraic Degree of MiMC [BCP, DCC23]
- ☞ Algebraic attacks [BBLP, ToSC22(3)]

Design

Lessons learnt for other designs.

Motivation

Primitives need to be analysed.

Cryptanalysis

- ☞ Algebraic Degree of MiMC [BCP, DCC23]
- ☞ Algebraic attacks [BBLP, ToSC22(3)]

Design

- ☞ Anemoi [BBC+22]

Lessons learnt for other designs.

Content

Design and Cryptanalysis of Arithmetization-Oriented Primitives.

Comparison with "usual" case

A new environment

"Usual" case

- ⋆ Field size:
  $\mathbb{F}_{2^n}$, with $n \simeq 4, 8$ (AES: $n = 8$).
- ⋆ Operations:
  logical gates/CPU instructions

Arithmetization-friendly

- ⋆ Field size:
  $\mathbb{F}_q$, with $q \in \{2^n, p\}, p \simeq 2^n$, $n \geq 64$
- ⋆ Operations:
  large finite-field arithmetic

Comparison with "usual" case

A new environment

"Usual" case

- Field size:
  $\mathbb{F}_{2^n}$, with $n \simeq 4, 8$ (AES: $n = 8$).
- Operations:
  logical gates/CPU instructions

Arithmetization-friendly

- Field size:
  $\mathbb{F}_q$, with $q \in \{2^n, p\}, p \simeq 2^n,\ n \geq 64$
- Operations:
  large finite-field arithmetic

$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, with p given by the order of some elliptic curves

Examples:

- Curve BLS12-381 $\log_2 p = 255$

  $p = 52435875175126190479447740508185965837690552500527637822603658699938581184513$

- Curve BLS12-377 $\log_2 p = 253$

  $p = 8444461749428370424248824938781546531375899335154063827935233455917409239041$

Comparison with "usual" case

A new environment

"Usual" case

- Field size:
  $\mathbb{F}_{2^n}$, with $n \simeq 4, 8$ (AES: $n = 8$).
- Operations:
  logical gates/CPU instructions

Arithmetization-friendly

- Field size:
  $\mathbb{F}_q$, with $q \in \{2^n, p\}, p \simeq 2^n$, $n \geq 64$
- Operations:
  large finite-field arithmetic

New properties

"Usual" case

$$y \leftarrow E(x)$$

- Optimized for:
  implementation in software/hardware

Arithmetization-friendly

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

- Optimized for:
  integration within advanced protocols

Comparison with “usual” case

A new environment

“Usual” case

- Field size: $\mathbb{F}_{2^n}$, with $n \simeq 4, 8$ (AES: $n = 8$).
- Operations: logical gates/CPU in...

Arithmetization-friendly

- Field size: $\mathbb{F}_q$, with $q \in \{2^n, p\}, p \simeq 2^n$, $n \geq 64$.
- Operations: large finite-field arithmeti...

Decades of Cryptanalysis

$\leq$ 5 years of Cryptanalysis

N...

“Usual” case

$$y \leftarrow E(x)$$

- Optimized for: implementation in software/hardware

Arithmetization-friendly

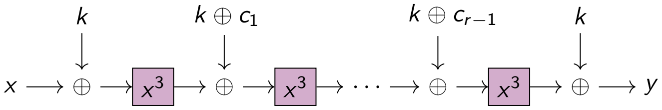
$$y \leftarrow E(x) \quad \text{and} \quad y == E(x)$$

- Optimized for: integration within advanced protocols

1. Emerging uses in symmetric cryptography
2. Algebraic Degree of MiMC
   - Exact degree
   - Integral attacks
3. Algebraic Attacks
   - Tricks for SPN
   - Applied to POSEIDON and Rescue–Prime
4. `Anemoi`
   - CCZ-equivalence
   - New S-box: `Flystel`
   - New mode: `Jive`

The block cipher MiMC

- Minimize the number of multiplications in $\mathbb{F}_{2^n}$.
- Construction of MiMC_3 [Albrecht et al., Asiacrypt16]:
  - 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 $s = (2^{n+1} - 1)/3$



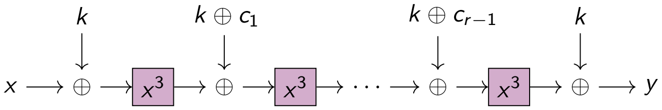
The block cipher MiMC

- Minimize the number of multiplications in $\mathbb{F}_{2^n}$.
- Construction of MiMC$_3$ [Albrecht et al., Asiacrypt16]:
  - 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.



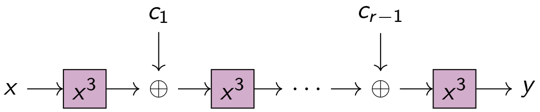
The block cipher MiMC

- Minimize the number of multiplications in $\mathbb{F}_{2^n}$.
- Construction of MiMC_3 [Albrecht et al., Asiacrypt16]:
  - 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 - 1st definition

Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$, there is **a unique multivariate polynomial** in $\mathbb{F}_2[x_1, \ldots x_n] / \left((x_i^2 + x_i)_{1 \le i \le n}\right)$:

$$f(x_1, \ldots, x_n) = \sum_{u \in \mathbb{F}_2^n} a_u x^u, \text{ where } a_u \in \mathbb{F}_2, \ x^u = \prod_{i=1}^{n} x_i^{u_i} .$$

This is the **Algebraic Normal Form (ANF)** of f.

Definition

Algebraic Degree of $f : \mathbb{F}_2^n \to \mathbb{F}_2$:

$$\deg^a(f) = \max\left\{\mathrm{hw}(u) : u \in \mathbb{F}_2^n, a_u \neq 0\right\} ,$$

Algebraic degree - 1st definition

Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$, there is **a unique multivariate polynomial** in $\mathbb{F}_2[x_1, \ldots x_n] / \left((x_i^2 + x_i)_{1 \le i \le n}\right)$:

$$f(x_1, \ldots, x_n) = \sum_{u \in \mathbb{F}_2^n} a_u x^u, \text{ where } a_u \in \mathbb{F}_2,\ x^u = \prod_{i=1}^{n} x_i^{u_i} \ .$$

This is the **Algebraic Normal Form (ANF)** of f.

Definition

Algebraic Degree of $f : \mathbb{F}_2^n \to \mathbb{F}_2$:

$$\deg^a(f) = \max\left\{\mathrm{hw}(u) : u \in \mathbb{F}_2^n, a_u \neq 0\right\} ,$$

If $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, then

$$\deg^a(F) = \max\{\deg^a(f_i),\ 1 \le i \le m\} \ .$$

where $F(x) = (f_1(x), \ldots f_m(x))$.

Algebraic degree - 1st definition

Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$, there is **a unique multivariate polynomial** in $\mathbb{F}_2[x_1, \ldots x_n]/\left((x_i^2 + x_i)_{1 \le i \le n}\right)$:

$$f(x_1, \ldots, x_n) = \sum_{u \in \mathbb{F}_2^n} a_u x^u, \text{ where } a_u \in \mathbb{F}_2,\ x^u = \prod_{i=1}^{n} x_i^{u_i} .$$

This is the **Algebraic Normal Form (ANF)** of f.

Example: $F : \mathbb{F}_{2^{11}} \to \mathbb{F}_{2^{11}}, x \mapsto x^3$

$F : \mathbb{F}_2^{11} \to \mathbb{F}_2^{11}, (x_0, \ldots, x_{10}) \mapsto$

$(x_0x_{10} + x_0 + x_1x_5 + x_1x_9 + x_2x_7 + x_2x_9 + x_2x_{10} + x_3x_4 + x_3x_5 + x_4x_8 + x_4x_9 + x_5x_{10} + x_6x_7 + x_6x_{10} + x_7x_8 + x_9x_{10},$

$x_0x_1 + x_0x_6 + x_2x_5 + x_2x_8 + x_3x_6 + x_3x_9 + x_3x_{10} + x_4 + x_5x_8 + x_5x_9 + x_6x_9 + x_7x_8 + x_7x_9 + x_7 + x_{10},$

$x_0x_1 + x_0x_2 + x_0x_{10} + x_1x_5 + x_1x_6 + x_1x_9 + x_2x_7 + x_3x_4 + x_3x_7 + x_4x_5 + x_4x_8 + x_4x_{10} + x_5x_{10} + x_6x_7 + x_6x_8 + x_6x_9 + x_7x_{10} + x_8 + x_9x_{10},$

$x_0x_3 + x_0x_6 + x_0x_7 + x_1 + x_2x_5 + x_2x_6 + x_2x_8 + x_2x_{10} + x_3x_6 + x_3x_8 + x_3x_9 + x_4x_5 + x_4x_6 + x_4 + x_5x_8 + x_5x_{10} + x_6x_9 + x_7x_9 + x_7 + x_8x_9 + x_{10},$

$x_0x_2 + x_0x_4 + x_1x_2 + x_1x_6 + x_1x_7 + x_2x_9 + x_2x_{10} + x_3x_5 + x_3x_6 + x_3x_7 + x_3x_9 + x_4x_5 + x_4x_7 + x_4x_9 + x_5 + x_6x_8 + x_7x_8 + x_8x_9 + x_8x_{10},$

$x_0x_5 + x_0x_7 + x_0x_8 + x_1x_2 + x_1x_3 + x_2x_6 + x_2x_7 + x_2x_{10} + x_3x_8 + x_4x_5 + x_4x_8 + x_5x_6 + x_5x_9 + x_7x_8 + x_7x_9 + x_7x_{10} + x_9,$

$x_0x_3 + x_0x_6 + x_1x_4 + x_1x_7 + x_1x_8 + x_2 + x_3x_6 + x_3x_7 + x_3x_9 + x_4x_7 + x_4x_9 + x_4x_{10} + x_5x_6 + x_5x_7 + x_5 + x_6x_9 + x_7x_{10} + x_8x_{10} + x_8 + x_9x_{10},$

$x_0x_7 + x_0x_8 + x_0x_9 + x_1x_3 + x_1x_5 + x_2x_3 + x_2x_7 + x_2x_8 + x_3x_{10} + x_4x_6 + x_4x_7 + x_4x_8 + x_4x_{10} + x_5x_6 + x_5x_8 + x_5x_{10} + x_6 + x_7x_9 + x_8x_9 + x_9x_{10},$

$x_0x_4 + x_0x_8 + x_1x_6 + x_1x_8 + x_1x_9 + x_2x_3 + x_2x_4 + x_3x_7 + x_3x_8 + x_4x_9 + x_5x_6 + x_5x_9 + x_6x_7 + x_6x_{10} + x_8x_9 + x_8x_{10} + x_{10},$

$x_0x_{10} + x_1x_4 + x_1x_7 + x_2x_5 + x_2x_8 + x_2x_9 + x_3 + x_4x_7 + x_4x_8 + x_4x_{10} + x_5x_8 + x_5x_{10} + x_6x_7 + x_6x_8 + x_6 + x_7x_{10} + x_9,$

$x_0x_5 + x_0x_{10} + x_1x_8 + x_1x_9 + x_1x_{10} + x_2x_4 + x_2x_6 + x_3x_4 + x_3x_8 + x_3x_9 + x_5x_7 + x_5x_8 + x_5x_9 + x_6x_7 + x_6x_9 + x_7 + x_8x_{10} + x_9x_{10}) .$

Algebraic degree - 2nd definition

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$. Then 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 $2^n - 1$:

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

Definition

Algebraic degree of $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$:

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

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

Algebraic degree - 2nd definition

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$. Then 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 $2^n - 1$:

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

Definition

Algebraic degree of $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$:

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

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

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

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

Integral attack

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 $= n - 1$

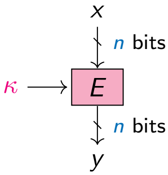
Integral attack

Exploiting a low algebraic degree

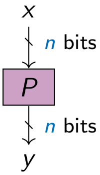
For any affine subspace $\mathcal{V} \subset \mathbb{F}_2^n$ with $\dim \mathcal{V} \geq \deg^a(F) + 1$, we have a 0-sum distinguisher:

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

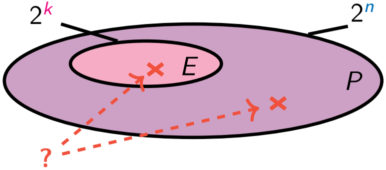
Random permutation: degree $= n - 1$



Block cipher



Random permutation



First Plateau

Round i of MiMC$_3$: $x \mapsto (x + c_{i-1})^3$.

For r rounds:

- ⋆ Upper bound [Eichlseder et al., Asiacrypt20]: $\lceil r \log_2 3 \rceil$.
- ⋆ Aim: determine $B_3^r := \max_c \deg^a \mathsf{MIMC}_{3,c}[r]$.

First Plateau

Round i of MiMC_3: $x \mapsto (x + c_{i-1})^3$.

For r rounds:

- ⋆ Upper bound [Eichlseder et al., Asiacrypt20]: $\lceil r \log_2 3 \rceil$.
- ⋆ Aim: determine $B_3^r := \max_c \deg^a \mathrm{MIMC}_{3,c}[r]$.

⋆ Round 1: $B_3^1 = 2$

$$\mathcal{P}_1(x) = x^3, \quad (c_0 = 0)$$

$$3 = [11]_2$$

First Plateau

Round i of MiMC_3: $x \mapsto (x + c_{i-1})^3$.

For r rounds:

- ⋆ Upper bound [Eichlseder et al., Asiacrypt20]: $\lceil r \log_2 3 \rceil$.
- ⋆ Aim: determine $B_3^r := \max_c \deg^a \text{MIMC}_{3,c}[r]$.

- ⋆ Round 1: $B_3^1 = 2$

$$\mathcal{P}_1(x) = x^3, \quad (c_0 = 0)$$

$$3 = [11]_2$$

- ⋆ Round 2: $B_3^2 = 2$

$$\mathcal{P}_2(x) = x^9 + c_1 x^6 + c_1^2 x^3 + c_1^3$$

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

First Plateau

Round i of MiMC_3: $x \mapsto (x + c_{i-1})^3$.

For r rounds:

- ⋆ Upper bound [Eichlseder et al., Asiacrypt20]: $\lceil r \log_2 3 \rceil$.
- ⋆ Aim: determine $B_3^r := \max_c \deg^a \text{MIMC}_{3,c}[r]$.

⋆ Round 1: $\boxed{B_3^1 = 2}$

$$\mathcal{P}_1(x) = x^3, \quad (c_0 = 0)$$

$$3 = [11]_2$$

⋆ Round 2: $\boxed{B_3^2 = 2}$

$$\mathcal{P}_2(x) = x^9 + c_1 x^6 + c_1^2 x^3 + c_1^3$$

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

First Plateau

Round i of MiMC$_3$: $x \mapsto (x + c_{i-1})^3$.

For r rounds:

- ⋆ Upper bound [Eichlseder et al., Asiacrypt20]: $\lceil r \log_2 3 \rceil$.
- ⋆ Aim: determine $B_3^r := \max_c \deg^a \text{MIMC}_{3,c}[r]$.

Definition

There is a **plateau** whenever $B_3^r = B_3^{r-1}$.

⋆ Round 1: $B_3^1 = 2$

$$\mathcal{P}_1(x) = x^3, \quad (c_0 = 0)$$

$$3 = [11]_2$$

⋆ Round 2: $B_3^2 = 2$

$$\mathcal{P}_2(x) = x^9 + c_1 x^6 + c_1^2 x^3 + c_1^3$$

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

First Plateau

Round i of MiMC$_3$: $x \mapsto (x + c_{i-1})^3$.

For r rounds:

- ⋆ Upper bound [Eichlseder et al., Asiacrypt20]: $\lceil r \log_2 3 \rceil$.
- ⋆ Aim: determine $B_3^r := \max_c \deg^a \mathrm{MIMC}_{3,c}[r]$.

⋆ Round 1: $B_3^1 = 2$

$$\mathcal{P}_1(x) = x^3, \quad (c_0 = 0)$$

$$3 = [11]_2$$

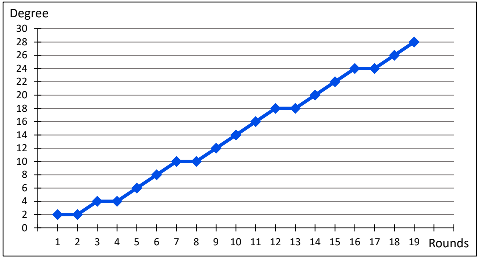
⋆ Round 2: $B_3^2 = 2$

$$\mathcal{P}_2(x) = x^9 + c_1 x^6 + c_1^2 x^3 + c_1^3$$

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

Definition

There is a **plateau** whenever $B_3^r = B_3^{r-1}$.



Algebraic degree observed for $n = 31$.

First Plateau

Round i of MiMC_3: $x \mapsto (x + c_{i-1})^3$.

For r rounds:

- ⋆ Upper bound [Eichlseder et al., Asiacrypt20]: $\lceil r \log_2 3 \rceil$.
- ⋆ Aim: determine $B_3^r := \max_c \deg^a \text{MIMC}_{3,c}[r]$.

Definition

There is a **plateau** whenever $B_3^r = B_3^{r-1}$.

- ⋆ Round 1: $B_3^1 = 2$

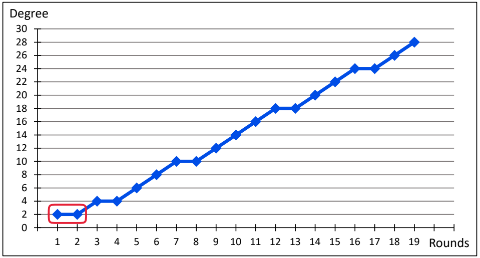
$$\mathcal{P}_1(x) = x^3, \quad (c_0 = 0)$$

$$3 = [11]_2$$

- ⋆ Round 2: $B_3^2 = 2$

$$\mathcal{P}_2(x) = x^9 + c_1 x^6 + c_1^2 x^3 + c_1^3$$

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



Algebraic degree observed for $n = 31$.

First Plateau

Round i of MiMC$_3$: $x \mapsto (x + c_{i-1})^3$.

For r rounds:

- ⋆ Upper bound [Eichlseder et al., Asiacrypt20]: $\lceil r \log_2 3 \rceil$.
- ⋆ Aim: determine $B_3^r := \max_c \deg^a \text{MIMC}_{3,c}[r]$.

Definition

There is a **plateau** whenever $B_3^r = B_3^{r-1}$.

- ⋆ Round 1: $B_3^1 = 2$

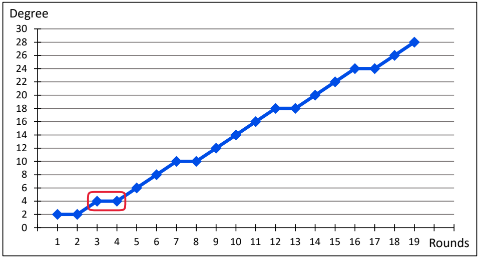
$$\mathcal{P}_1(x) = x^3, \quad (c_0 = 0)$$

$$3 = [11]_2$$

- ⋆ Round 2: $B_3^2 = 2$

$$\mathcal{P}_2(x) = x^9 + c_1 x^6 + c_1^2 x^3 + c_1^3$$

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



Algebraic degree observed for $n = 31$.

First Plateau

Round i of MiMC_3: $x \mapsto (x + c_{i-1})^3$.

For r rounds:

- ⋆ Upper bound [Eichlseder et al., Asiacrypt20]: $\lceil r \log_2 3 \rceil$.
- ⋆ Aim: determine $B_3^r := \max_c \deg^a \text{MIMC}_{3,c}[r]$.

⋆ Round 1: $B_3^1 = 2$

$$\mathcal{P}_1(x) = x^3, \quad (c_0 = 0)$$

$$3 = [11]_2$$

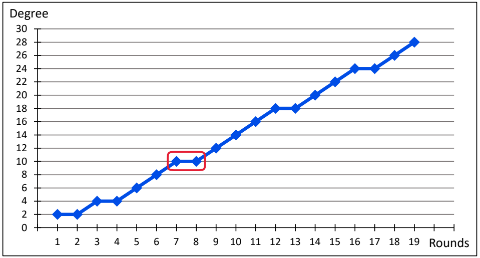
⋆ Round 2: $B_3^2 = 2$

$$\mathcal{P}_2(x) = x^9 + c_1 x^6 + c_1^2 x^3 + c_1^3$$

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

Definition

There is a **plateau** whenever $B_3^r = B_3^{r-1}$.



Algebraic degree observed for $n = 31$.

First Plateau

Round i of MiMC_3: $x \mapsto (x + c_{i-1})^3$.

For r rounds:

- ⋆ Upper bound [Eichlseder et al., Asiacrypt20]: $\lceil r \log_2 3 \rceil$.
- ⋆ Aim: determine $B_3^r := \max_c \deg^a \text{MIMC}_{3,c}[r]$.

Definition

There is a **plateau** whenever $B_3^r = B_3^{r-1}$.

⋆ Round 1: $B_3^1 = 2$

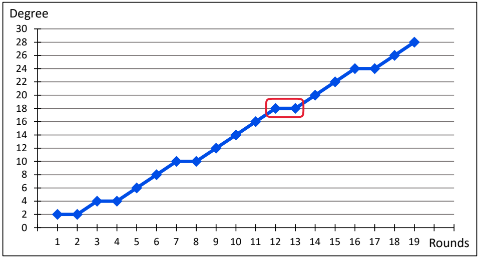
$$\mathcal{P}_1(x) = x^3, \quad (c_0 = 0)$$

$$3 = [11]_2$$

⋆ Round 2: $B_3^2 = 2$

$$\mathcal{P}_2(x) = x^9 + c_1 x^6 + c_1^2 x^3 + c_1^3$$

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



Algebraic degree observed for $n = 31$.

First Plateau

Round i of MiMC_3: $x \mapsto (x + c_{i-1})^3$.

For r rounds:

- ⋆ Upper bound [Eichlseder et al., Asiacrypt20]: $\lceil r \log_2 3 \rceil$.
- ⋆ Aim: determine $B_3^r := \max_c \deg^a \text{MIMC}_{3,c}[r]$.

Definition

There is a **plateau** whenever $B_3^r = B_3^{r-1}$.

- ⋆ Round 1: $B_3^1 = 2$

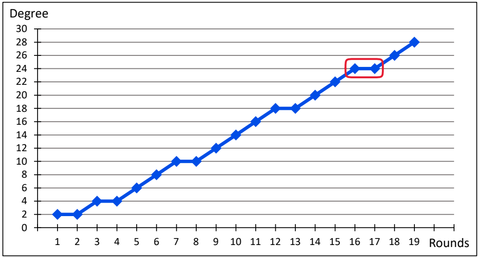
$$\mathcal{P}_1(x) = x^3, \quad (c_0 = 0)$$

$$3 = [11]_2$$

- ⋆ Round 2: $B_3^2 = 2$

$$\mathcal{P}_2(x) = x^9 + c_1 x^6 + c_1^2 x^3 + c_1^3$$

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



Algebraic degree observed for $n = 31$.

An upper bound

Proposition

Set of exponents that might appear in the polynomial:

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

An upper bound

Proposition

Set of exponents that might appear in the polynomial:

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

Example:

$$\mathcal{P}_1(x) = x^3 \quad \Rightarrow \quad \mathcal{E}_1 = \{3\} \ .$$

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

$$\mathcal{E}_2 = \{0, 3, 6, 9\} \ ,$$

$$\mathcal{P}_2(x) = x^9 + c_1 x^6 + c_1^2 x^3 + c_1^3 \ .$$

An upper bound

Proposition

Set of exponents that might appear in the polynomial:

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

No exponent $\equiv 5, 7 \bmod 8 \Rightarrow$ No exponent $2^{2k} - 1$

$\mathcal{E}_r \subseteq \{$

0	3	6	9	12	~~15~~	18	~~21~~
24	27	30	33	36	~~39~~	42	~~45~~
48	51	54	57	60	~~63~~	66	~~69~~

$\ldots \quad 3^r\}$

Example: $63 = 2^{2\times 3} - 1 \notin \mathcal{E}_4 = \{0, 3, \ldots, 81\}$ $\Rightarrow B_3^4 < 6 = wt(63)$

$\forall e \in \mathcal{E}_4 \backslash \{63\}, wt(e) \leq 4$ $\Rightarrow B_3^4 \leq 4$

Bounding the degree

Theorem

After r rounds of MiMC, the algebraic degree is

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

Bounding the degree

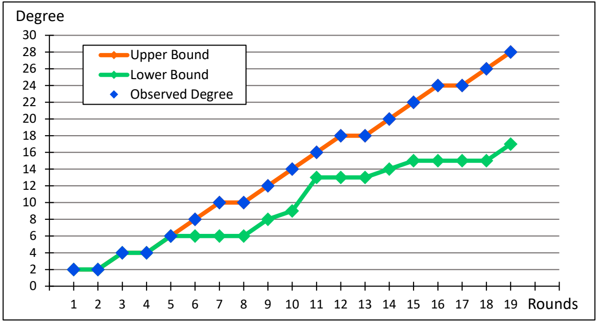
Theorem

After r rounds of MiMC, the algebraic degree is

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

And a lower bound if $3^r < 2^n - 1$:

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



Exact degree

Maximum-weight exponents:

Let $k_r = \lfloor \log_2 3^r \rfloor$.

$\forall r \in \{4, \ldots, 16265\} \backslash \mathcal{F}$ with $\mathcal{F} = \{465, 571, \ldots\}$:

- if $k_r = 1 \bmod 2$,
$$\omega_r = 2^{k_r} - 5 \in \mathcal{E}_r,$$
- if $k_r = 0 \bmod 2$,
$$\omega_r = 2^{k_r} - 7 \in \mathcal{E}_r.$$

Example:

$$123 = 2^7 - 5 = 2^{k_5} - 5 \qquad \in \mathcal{E}_5,$$
$$4089 = 2^{12} - 7 = 2^{k_8} - 7 \qquad \in \mathcal{E}_8.$$

Exact degree

Maximum-weight exponents:

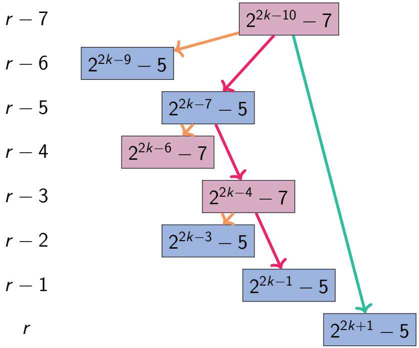
Let $k_r = \lfloor \log_2 3^r \rfloor$.

$\forall r \in \{4, \ldots, 16265\} \backslash \mathcal{F}$ with $\mathcal{F} = \{465, 571, \ldots\}$:

- ⋆ if $k_r = 1 \bmod 2$,
$$\omega_r = 2^{k_r} - 5 \in \mathcal{E}_r,$$
- ⋆ if $k_r = 0 \bmod 2$,
$$\omega_r = 2^{k_r} - 7 \in \mathcal{E}_r.$$

Example:

$$123 = 2^7 - 5 = 2^{k_5} - 5 \qquad \in \mathcal{E}_5,$$
$$4089 = 2^{12} - 7 = 2^{k_8} - 7 \qquad \in \mathcal{E}_8.$$



Constructing exponents.

$$\exists\, \ell \text{ s.t. } \quad \omega_{r-\ell} \in \mathcal{E}_{r-\ell} \Rightarrow \omega_r \in \mathcal{E}_r$$

Exact degree

Maximum-weight exponents:

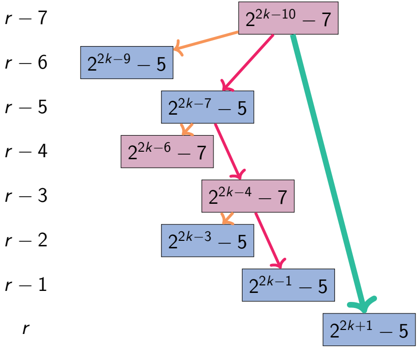
Let $k_r = \lfloor \log_2 3^r \rfloor$.

$\forall r \in \{4, \ldots, 16265\} \backslash \mathcal{F}$ with $\mathcal{F} = \{465, 571, \ldots\}$:

- if $k_r = 1 \bmod 2$,
$$\omega_r = 2^{k_r} - 5 \in \mathcal{E}_r,$$
- if $k_r = 0 \bmod 2$,
$$\omega_r = 2^{k_r} - 7 \in \mathcal{E}_r.$$

Example:

$$123 = 2^7 - 5 = 2^{k_5} - 5 \in \mathcal{E}_5,$$
$$4089 = 2^{12} - 7 = 2^{k_8} - 7 \in \mathcal{E}_8.$$



Constructing exponents.

$$\exists \ell \text{ s.t. } \quad \omega_{r-\ell} \in \mathcal{E}_{r-\ell} \Rightarrow \omega_r \in \mathcal{E}_r$$

Exact degree

Maximum-weight exponents:

Let $k_r = \lfloor \log_2 3^r \rfloor$.

$\forall r \in \{4, \ldots, 16265\} \backslash \mathcal{F}$ with $\mathcal{F} = \{465, 571, \ldots\}$:

- ⋆ if $k_r = 1 \bmod 2$,

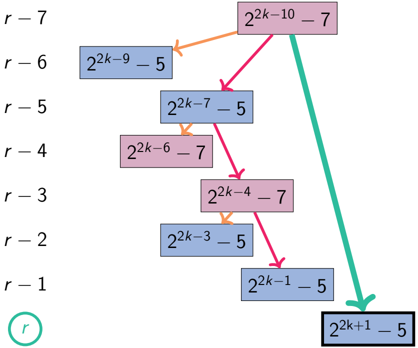
$$\omega_r = 2^{k_r} - 5 \in \mathcal{E}_r,$$

- ⋆ if $k_r = 0 \bmod 2$,

$$\omega_r = 2^{k_r} - 7 \in \mathcal{E}_r.$$

Example:

$$123 = 2^7 - 5 = 2^{k_5} - 5 \qquad \in \mathcal{E}_5,$$
$$4089 = 2^{12} - 7 = 2^{k_8} - 7 \qquad \in \mathcal{E}_8.$$



Constructing exponents.

$$\exists \ell \text{ s.t. } \quad \omega_{r-\ell} \in \mathcal{E}_{r-\ell} \Rightarrow \omega_r \in \mathcal{E}_r$$

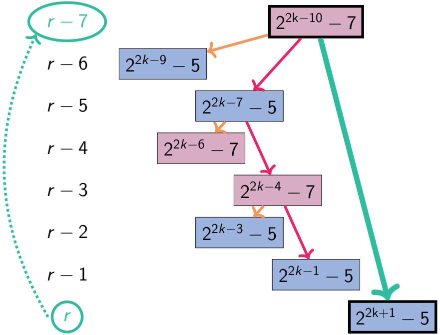
Exact degree

Maximum-weight exponents:

Let $k_r = \lfloor \log_2 3^r \rfloor$.

$\forall r \in \{4, \ldots, 16265\} \backslash \mathcal{F}$ with $\mathcal{F} = \{465, 571, \ldots\}$:

- if $k_r = 1 \bmod 2$,
$$\omega_r = 2^{k_r} - 5 \in \mathcal{E}_r,$$
- if $k_r = 0 \bmod 2$,
$$\omega_r = 2^{k_r} - 7 \in \mathcal{E}_r.$$



Constructing exponents.

Example:

$$123 = 2^7 - 5 = 2^{k_5} - 5 \quad \in \mathcal{E}_5,$$
$$4089 = 2^{12} - 7 = 2^{k_8} - 7 \quad \in \mathcal{E}_8.$$

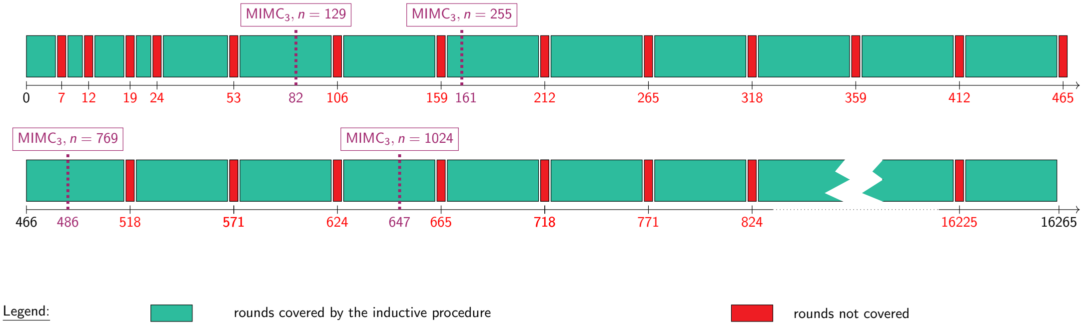
$$\exists \ell \text{ s.t. } \quad \omega_{r-\ell} \in \mathcal{E}_{r-\ell} \Rightarrow \omega_r \in \mathcal{E}_r$$

Covered rounds

Idea of the proof:

- ⋆ inductive proof: existence of "good" ℓ

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

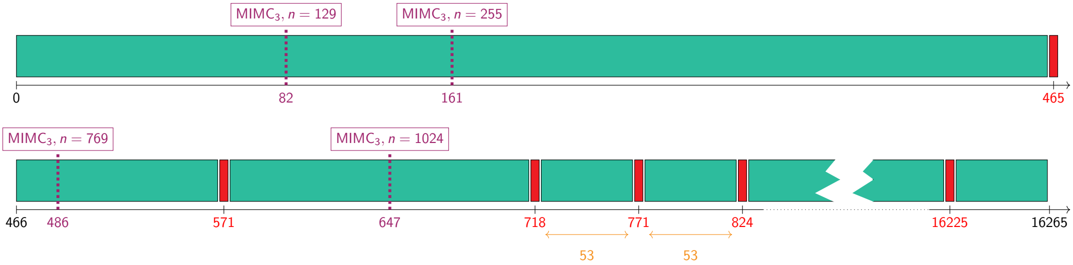


Covered rounds

Idea of the proof:

- ⋆ inductive proof: existence of "good" ℓ
- ⋆ MILP solver (`PySCIPOpt`)

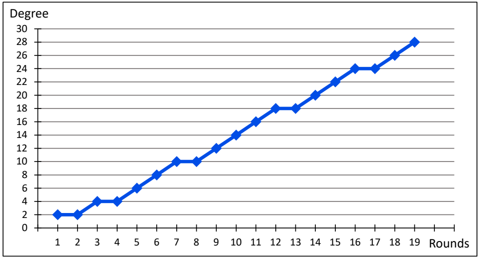
Rounds for which we are able to exhibit a maximum-weight exponent.



Legend: rounds covered by the inductive procedure or MILP — rounds not covered

Plateau

$\Rightarrow$ plateau when $k_r = \lfloor \log_2 3^r \rfloor = 1 \bmod 2$ and $k_{r+1} = \lfloor \log_2 3^{r+1} \rfloor = 0 \bmod 2$



Algebraic degree observed for $n = 31$.

If we have a plateau

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

Then the next one is

$$B_3^{r+4} = B_3^{r+5} \quad \text{or} \quad B_3^{r+5} = B_3^{r+6} .$$

Music in $MIMC_3$

- Patterns in sequence $(k_r)_{r>0}$:

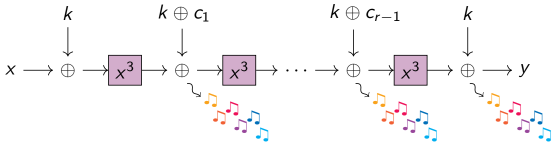
$$\Rightarrow \text{denominators of semiconvergents of } \log_2(3) \simeq 1.5849625$$

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

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

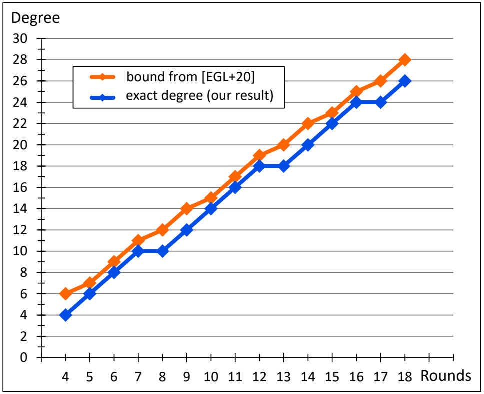
- **Music theory:**
  - perfect octave 2:1
  - perfect fifth 3:2

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



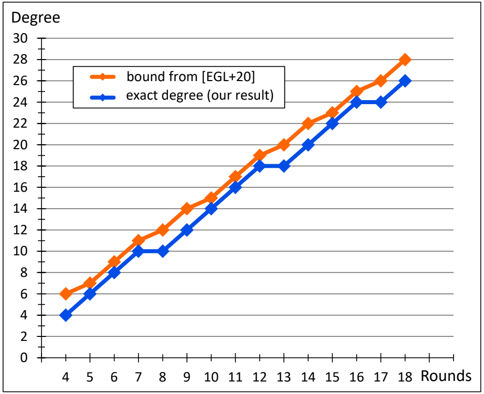
Comparison to previous work

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



Comparison to previous work

First Bound: $\lceil r \log_2 3 \rceil \quad \Rightarrow \quad$ 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}	New
80/82	2^{125}XOR	2^{125}	New

Secret-key distinguishers ($n = 129$)

Take-Away

Algebraic Degree of MiMC

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

$$2 \times \left\lceil \lfloor \log_2(3^r) \rfloor / 2 - 1 \right\rceil .$$

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

1. Emerging uses in symmetric cryptography
2. Algebraic Degree of MiMC
   - Exact degree
   - Integral attacks
3. Algebraic Attacks
   - Tricks for SPN
   - Applied to Poseidon and Rescue–Prime
4. Anemoi
   - CCZ-equivalence
   - New S-box: Flystel
   - New mode: Jive

Ethereum Challenges

In Nov. 2021, a Cryptanalysis Challenge for AOP by the Ethereum Foundation.

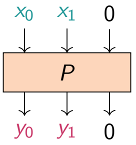
Feistel–MiMC, Rescue–Prime, POSEIDON, Reinforced Concrete

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

Ethereum Challenges

In Nov. 2021, a Cryptanalysis Challenge for AOP by the Ethereum Foundation.

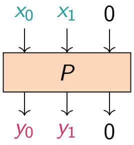
Feistel–MiMC, Rescue–Prime, Poseidon, Reinforced Concrete

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 $t = 3,\ u = 1$.

Solving Systems:

- ⋆ **Univariate systems**: Find the roots of a polynomial $P \in \mathbb{F}_q[X]$: $\widetilde{\mathcal{O}}(d)$, $d = \deg(P)$
- ⋆ **Multivariate systems**: Compute a Gröbner basis from polynomial equations in $\mathbb{F}_q[X_1, \ldots, X_n]$: $P_{j, j=1,\ldots,n}(X_1, \ldots X_n) = 0$: $\widetilde{\mathcal{O}}(d^3)$

Ethereum Challenges

In Nov. 2021, a Cryptanalysis Challenge for AOP by the Ethereum Foundation.

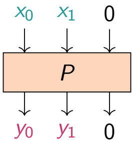
Feistel–MiMC, Rescue–Prime, Poseidon, Reinforced Concrete

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

Solving Systems:

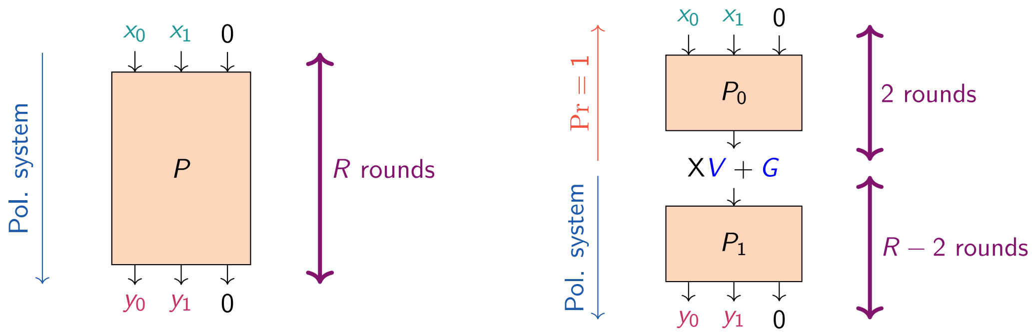
- ⋆ **Univariate systems**: Find the roots of a polynomial $P \in \mathbb{F}_q[X]$: $\widetilde{\mathcal{O}}(d)$, $d = \deg(P)$
- ⋆ **Multivariate systems**: Compute a Gröbner basis from polynomial equations in $\mathbb{F}_q[X_1, \ldots, X_n]$: $P_{j, j=1,\ldots,n}(X_1, \ldots X_n) = 0$: $\widetilde{\mathcal{O}}(d^3)$

$\Rightarrow$ **build univariate systems when possible!**

Trick for SPN

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

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



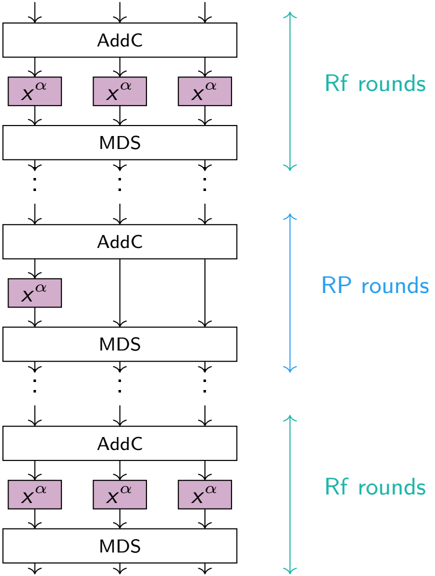
Approach used against Poseidon and Rescue–Prime

POSEIDON

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

- SPN construction:
  - S-Box layer: $x \mapsto x^\alpha$, $(\alpha = 3)$
  - Linear layer: MDS
  - Round constants addition: AddC
- Number of rounds (for challenges):

$$\begin{aligned} R &= 2 \times \mathrm{Rf} + \mathrm{RP} \\ &= 8 + (\text{from 3 to 24}) \ . \end{aligned}$$



Poseidon

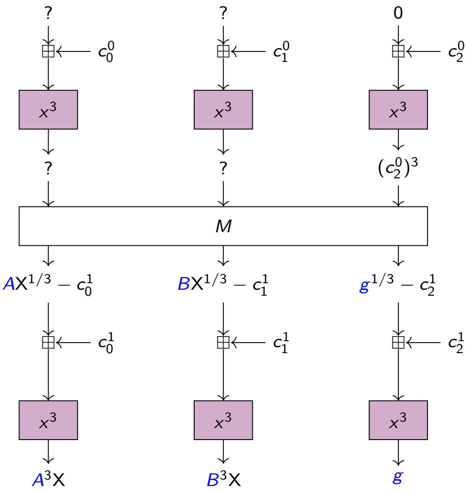
$$\begin{cases} V &= (A^3, B^3, 0)\ , \\ G &= (0, 0, g)\ , \end{cases}$$

with

$$\begin{cases} B &= -\frac{\alpha_{0,2}}{\alpha_{1,2}} A \\ g &= \left(\frac{1}{\alpha_{2,2}} \left(\alpha_{0,2} c_0^1 + \alpha_{1,2} c_1^1 \right) + c_2^1 + (c_2^0)^3 \right)^3 \ . \end{cases}$$

R	Designers claims	Ethereum estimations	d	complexity
$8+3$	2^{17}	2^{45}	3^9	2^{26}
$8+8$	2^{25}	2^{53}	3^{14}	2^{35}
$8+13$	2^{33}	2^{61}	3^{19}	2^{44}
$8+19$	2^{42}	2^{69}	3^{25}	2^{54}
$8+24$	2^{50}	2^{77}	3^{30}	2^{62}

Complexity of our attack against Poseidon.



Rescue–Prime

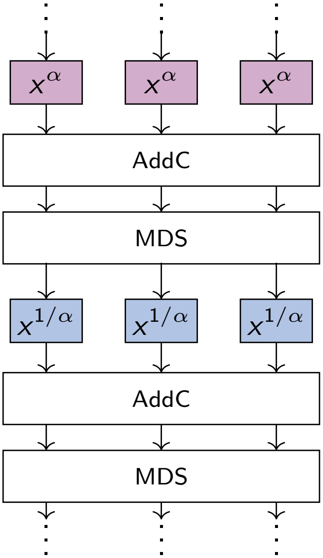
A. Aly, T. Ashur, E. Ben-Sasson, S. Dhooghe and A. Szepieniec, *ToSC 2020*

- SPN construction:
  - S-Box layer: $x \mapsto x^\alpha$ and $x \mapsto x^{1/\alpha}$, $(\alpha = 3)$
  - Linear layer: MDS
  - Round constants addition: AddC

- Number of rounds (for challenges):

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

(2 S-boxes per round).



Rescue–Prime

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

- SPN construction:
  - S-Box layer: $x \mapsto x^\alpha$ and $x \mapsto x^{1/\alpha}$, $(\alpha = 3)$
  - Linear layer: MDS
  - Round constants addition: AddC
- Number of rounds (for challenges):

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

(2 S-boxes per round).

Example of parameters

$$p = 18446744073709551557$$
$$\simeq 2^{64}$$
$$\alpha = 3$$
$$\alpha^{-1} = 12297829382473034371$$

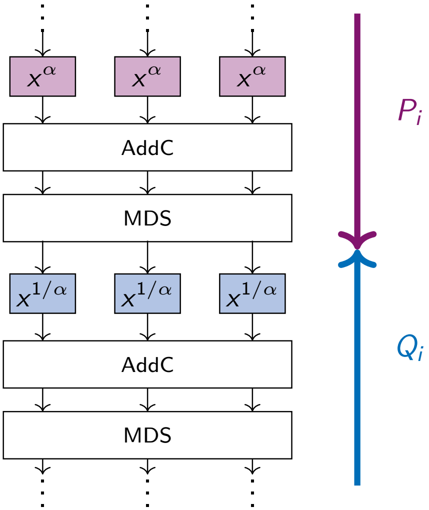
Rescue–Prime

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

- SPN construction:
  - S-Box layer: $x \mapsto x^{\alpha}$ and $x \mapsto x^{1/\alpha}$, $(\alpha = 3)$
  - Linear layer: MDS
  - Round constants addition: AddC
- Number of rounds (for challenges):

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

(2 S-boxes per round).



Rescue–Prime

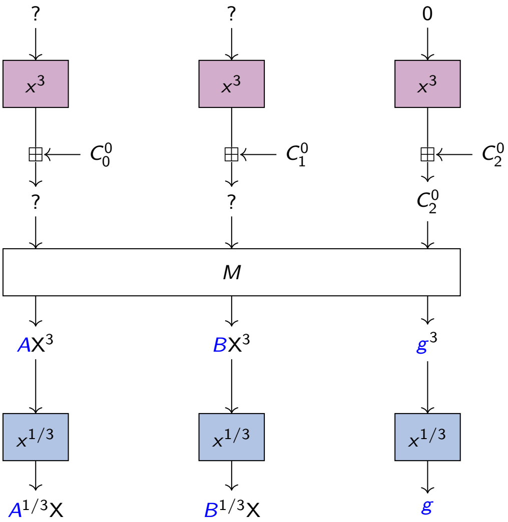
$$\begin{cases} V &= (A^3, B^3, 0)\ , \\ G &= (0, 0, g)\ , \end{cases}$$

with

$$\begin{cases} B &= -\frac{\alpha_{0,2}}{\alpha_{1,2}} A \\ g &= \left(\frac{1}{\alpha_{2,2}} \left(\alpha_{0,2} c_0^0 + \alpha_{1,2} c_1^0 \right) + c_2^0 \right)^{1/3} \end{cases}\ .$$

R	m	Designers claims	Ethereum estimations	d	complexity
4	3	2^{36}	$2^{37.5}$	3^9	2^{43}
6	2	2^{40}	$2^{37.5}$	3^{11}	2^{53}
7	2	2^{48}	$2^{43.5}$	3^{13}	2^{62}
5	3	2^{48}	2^{45}	3^{12}	2^{57}
8	2	2^{56}	$2^{49.5}$	3^{15}	2^{72}

Complexity of our attack against Rescue.



Take-Away

Algebraic Attacks against some AOP

- ⋆ consider as many variants of encoding as possible
- ⋆ build univariate instead of multivariate systems
- ⋆ start (and end) with a linear layer
- ⋆ 2 rounds can be skipped with the trick

1. Emerging uses in symmetric cryptography

2. Algebraic Degree of MiMC
   - Exact degree
   - Integral attacks

3. Algebraic Attacks
   - Tricks for SPN
   - Applied to POSEIDON and Rescue–Prime

4. Anemoi
   - CCZ-equivalence
   - New S-box: Flystel
   - New mode: Jive

Why Anemoi?

- Anemoi
  Family of ZK-friendly Hash functions

Why Anemoi?

- **Anemoi**
  Family of ZK-friendly Hash functions

⇓

- **Anemoi**
  Greek gods of winds

Our approach

Need: verification using few multiplications.

Our approach

Need: verification using few multiplications.

First approach: evaluation also using few multiplications.

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

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

Our approach

Need: verification using few multiplications.

First approach: evaluation also using few multiplications.

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

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

$\Rightarrow$ vulnerability to some attacks?

Our approach

Need: verification using few multiplications.

First approach: evaluation also using few multiplications.

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

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

$\Rightarrow$ vulnerability to some attacks?

New approach:

using CCZ-equivalence

Our vision

A function is arithmetization-oriented if it is **CCZ-equivalent** to a function that can be verified efficiently.

Our approach

Need: verification using few multiplications.

First approach: evaluation also using few multiplications.

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

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

$\Rightarrow$ vulnerability to some attacks?

New approach:

using CCZ-equivalence

Our vision

A function is arithmetization-oriented if it is **CCZ-equivalent** to a function that can be verified efficiently.

$y \leftarrow F(x)$ $\rightsquigarrow$ F: high degree

$v == G(u)$ $\rightsquigarrow$ G: low degree

CCZ-equivalence

Definition [Carlet, Charpin, Zinoviev, DCC98]

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

$$\Gamma_F = \left\{ (x, F(x)) \mid x \in \mathbb{F}_q \right\} = \mathcal{A}(\Gamma_G) = \left\{ \mathcal{A}(x, G(x)) \mid x \in \mathbb{F}_q \right\},$$

where $\mathcal{A}$ is an affine permutation, $\mathcal{A}(x) = \mathcal{L}(x) + c$.

CCZ-equivalence

Definition [Carlet, Charpin, Zinoviev, DCC98]

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

$$\Gamma_F = \{ (x, F(x)) \mid x \in \mathbb{F}_q \} = \mathcal{A}(\Gamma_G) = \{ \mathcal{A}(x, G(x)) \mid x \in \mathbb{F}_q \} ,$$

where $\mathcal{A}$ is an affine permutation, $\mathcal{A}(x) = \mathcal{L}(x) + c$.

- ⋆ F and G have the same differential properties: $\delta_F = \delta_G$.

CCZ-equivalence

Definition [Carlet, Charpin, Zinoviev, DCC98]

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

$$\Gamma_F = \left\{ (x, F(x)) \mid x \in \mathbb{F}_q \right\} = \mathcal{A}(\Gamma_G) = \left\{ \mathcal{A}(x, G(x)) \mid x \in \mathbb{F}_q \right\},$$

where $\mathcal{A}$ is an affine permutation, $\mathcal{A}(x) = \mathcal{L}(x) + c$.

- ⋆ F and G have the same differential properties: $\delta_F = \delta_G$.
- ⋆ F and G have the same linear properties: $\mathcal{W}_F = \mathcal{W}_G$.

CCZ-equivalence

Definition [Carlet, Charpin, Zinoviev, DCC98]

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

$$\Gamma_F = \{ (x, F(x)) \mid x \in \mathbb{F}_q \} = \mathcal{A}(\Gamma_G) = \{ \mathcal{A}(x, G(x)) \mid x \in \mathbb{F}_q \},$$

where $\mathcal{A}$ is an affine permutation, $\mathcal{A}(x) = \mathcal{L}(x) + c$.

- ⋆ F and G have the same differential properties: $\delta_F = \delta_G$.
- ⋆ F and G have the same linear properties: $\mathcal{W}_F = \mathcal{W}_G$.
- ⋆ Verification is the same: if $y \leftarrow F(x)$, $v \leftarrow G(u)$

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

CCZ-equivalence

Definition [Carlet, Charpin, Zinoviev, DCC98]

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

$$\Gamma_F = \{ (x, F(x)) \mid x \in \mathbb{F}_q \} = \mathcal{A}(\Gamma_G) = \{ \mathcal{A}(x, G(x)) \mid x \in \mathbb{F}_q \},$$

where $\mathcal{A}$ is an affine permutation, $\mathcal{A}(x) = \mathcal{L}(x) + c$.

- ⋆ F and G have the same differential properties: $\delta_F = \delta_G$.
- ⋆ F and G have the same linear properties: $\mathcal{W}_F = \mathcal{W}_G$.
- ⋆ Verification is the same: if $y \leftarrow F(x)$, $v \leftarrow G(u)$

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

- ⋆ The degree is not preserved.

CCZ-equivalence

Definition [Carlet, Charpin, Zinoviev, DCC98]

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

$$\Gamma_F = \{ (x, F(x)) \mid x \in \mathbb{F}_q \} = \mathcal{A}(\Gamma_G) = \{\mathcal{A}(x, G(x)) \mid x \in \mathbb{F}_q\} ,$$

where $\mathcal{A}$ is an affine permutation, $\mathcal{A}(x) = \mathcal{L}(x) + c$.

- ⋆ F and G have the same differential properties: $\delta_F = \delta_G$.
- ⋆ F and G have the same linear properties: $\mathcal{W}_F = \mathcal{W}_G$.
- ⋆ Verification is the same: if $y \leftarrow F(x)$, $v \leftarrow G(u)$

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

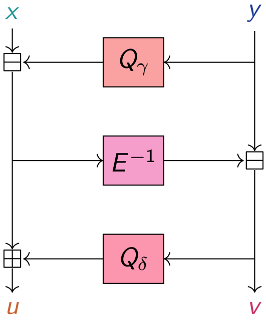
- ⋆ The degree is not preserved.

The Flystel

Butterfly + Feistel ⇒ Flystel

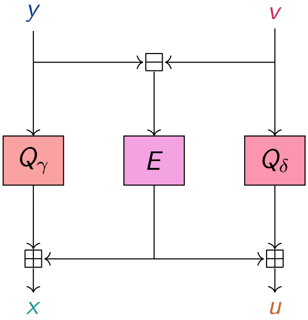
A 3-round Feistel-network with
$Q_\gamma : \mathbb{F}_q \rightarrow \mathbb{F}_q$ and $Q_\delta : \mathbb{F}_q \rightarrow \mathbb{F}_q$ two quadratic functions, and $E : \mathbb{F}_q \rightarrow \mathbb{F}_q$ a permutation

High-degree permutation



Open Flystel $\mathcal{H}$.

Low-degree function

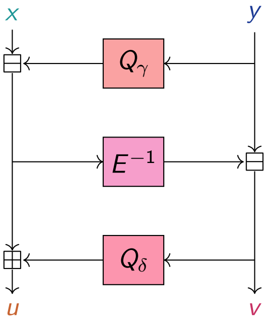


Closed Flystel $\mathcal{V}$.

The Flystel

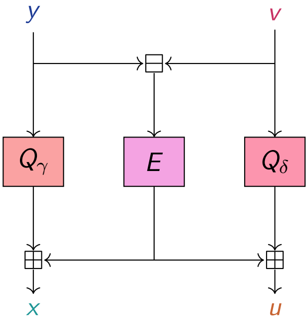
$$\Gamma_{\mathcal{H}} = \{((x,y),\ \mathcal{H}((x,y))) \mid (x,y) \in \mathbb{F}_q^2\}$$
$$= \mathcal{A}\left(\{((v,y),\ \mathcal{V}((v,y))) \mid (v,y) \in \mathbb{F}_q^2\}\right)$$
$$= \mathcal{A}(\Gamma_{\mathcal{V}})$$

High-degree permutation



Open Flystel $\mathcal{H}$.

Low-degree function

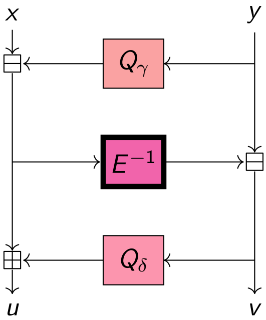


Closed Flystel $\mathcal{V}$.

Advantage of CCZ-equivalence

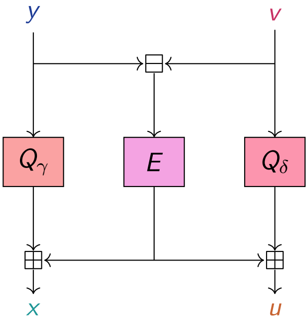
- ⋆ High Degree Evaluation.

High-degree permutation



Open `Flystel` $\mathcal{H}$.

Low-degree function



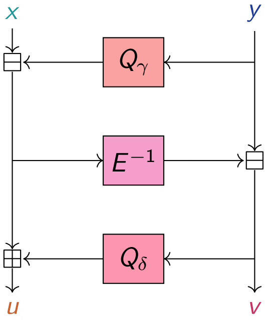
Closed `Flystel` $\mathcal{V}$.

Advantage of CCZ-equivalence

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

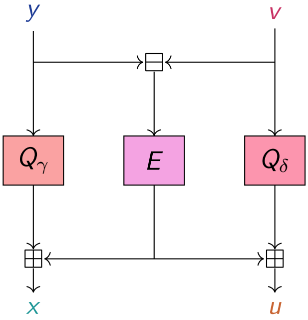
$$(u, v) == \mathcal{H}(x, y) \Leftrightarrow (x, u) == \mathcal{V}(y, v)$$

High-degree permutation



Open Flystel $\mathcal{H}$.

Low-degree function

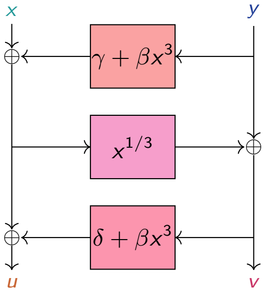


Closed Flystel $\mathcal{V}$.

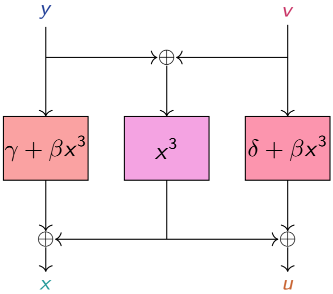
Flystel in $\mathbb{F}_{2^n}$

$$\mathcal{H} : \begin{cases} \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} & \to \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \\ (x, y) \mapsto & \left(x + \beta y^3 + \gamma + \beta \left(y + (x + \beta y^3 + \gamma)^{1/3}\right)^3 + \delta \right., \\ & \left. y + (x + \beta y^3 - \gamma)^{1/3}\right) . \end{cases}$$

$$\mathcal{V} : \begin{cases} \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} & \to \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \\ (x, y) & \mapsto \left((y + v)^3 + \beta y^3 + \gamma \right., \\ & \left. (y + v)^3 + \beta v^3 + \delta\right) , \end{cases}$$

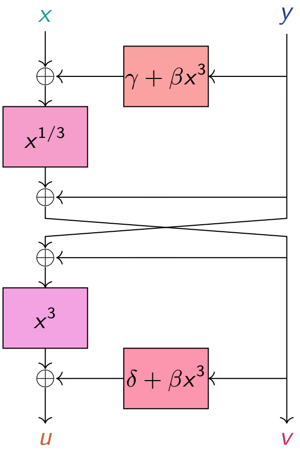


Open Flystel$_2$.



Closed Flystel$_2$.

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



Degenerated Butterfly.

First introduced by [Perrin et al. 2016].

Well-studied butterfly.

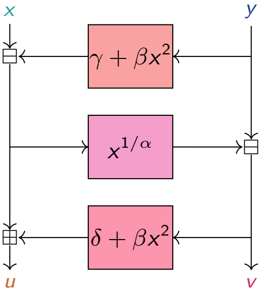
Theorems in [Li et al. 2018] state that if $\beta \neq 0$:

- Differential properties
  - Flystel$_2$: $\delta_{\mathcal{H}} = \delta_{\mathcal{V}} = 4$
- Linear properties
  - Flystel$_2$: $\mathcal{W}_{\mathcal{H}} = \mathcal{W}_{\mathcal{V}} = 2^{n+1}$
- Algebraic degree
  - Open Flystel$_2$: $\deg_{\mathcal{H}} = n$
  - Closed Flystel$_2$: $\deg_{\mathcal{V}} = 2$

Flystel in $\mathbb{F}_p$

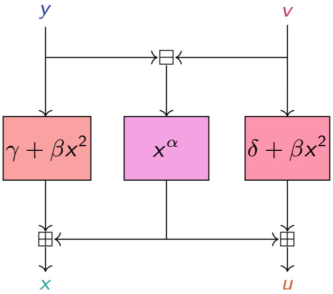
$$\mathcal{H} : \begin{cases} \mathbb{F}_p \times \mathbb{F}_p & \to \mathbb{F}_p \times \mathbb{F}_p \\ (x, y) & \mapsto \Big(x - \beta y^2 - \gamma + \beta \left(y - (x - \beta y^2 - \gamma)^{1/\alpha}\right)^2 + \delta \,, \\ & \quad y - (x - \beta y^2 - \gamma)^{1/\alpha}\Big) \,. \end{cases}$$

$$\mathcal{V} : \begin{cases} \mathbb{F}_p \times \mathbb{F}_p & \to \mathbb{F}_p \times \mathbb{F}_p \\ (y, v) & \mapsto \big((y - v)^\alpha + \beta y^2 + \gamma \,, \\ & \quad (v - y)^\alpha + \beta v^2 + \delta\big) \,. \end{cases}$$



Open $\texttt{Flystel}_p$.

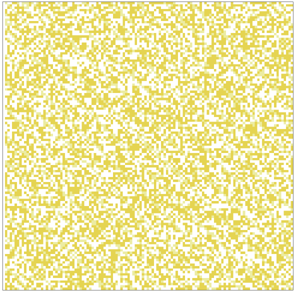
usually
$\alpha = 3$ or 5.



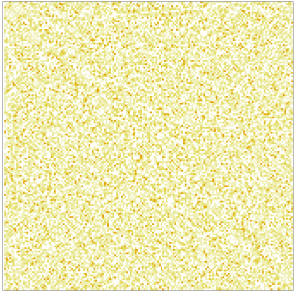
Closed $\texttt{Flystel}_p$.

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

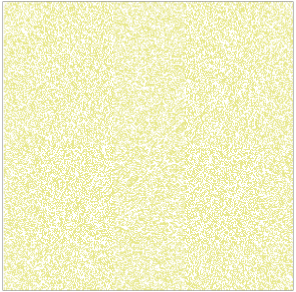
- Differential properties
  $\texttt{Flystel}_\texttt{p}$ has a differential uniformity equals to $\alpha - 1$.



(a) *when $p = 11$ and $\alpha = 3$.*



(b) *when $p = 13$ and $\alpha = 5$.*



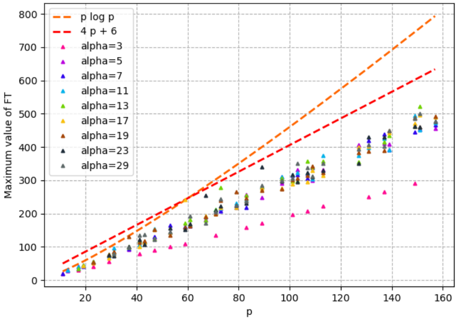
(c) *when $p = 17$ and $\alpha = 3$.*

DDT of $\texttt{Flystel}_p$.

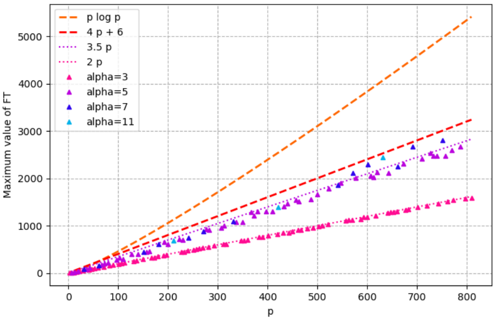
Properties of Flystel in $\mathbb{F}_p$

- Linear properties

$$\mathcal{W} \leq p \log p \ ?$$



(a) *For different α.*



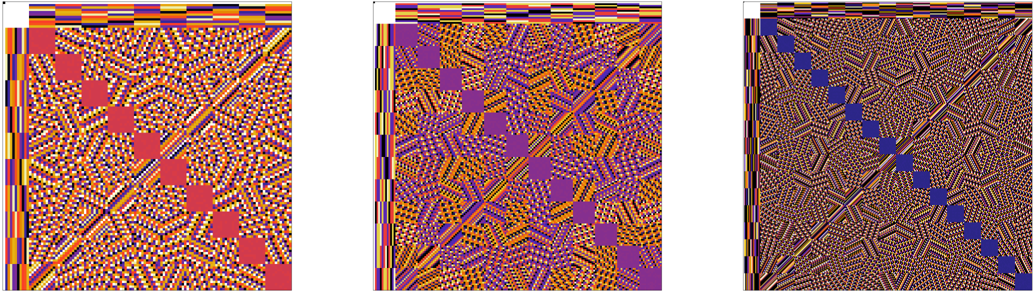
(b) *For the smallest α.*

Conjecture for the linearity.

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

- Linear properties

$$\mathcal{W} \leq p \log p \ ?$$

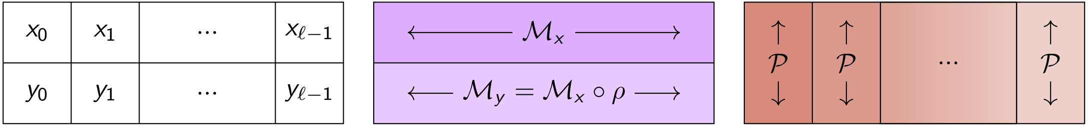


(a) *when* $p = 11$ *and* $\alpha = 3$. **(b)** *when* $p = 13$ *and* $\alpha = 5$. **(c)** *when* $p = 17$ *and* $\alpha = 3$.

LAT of $\texttt{Flystel}_p$.

The SPN Structure

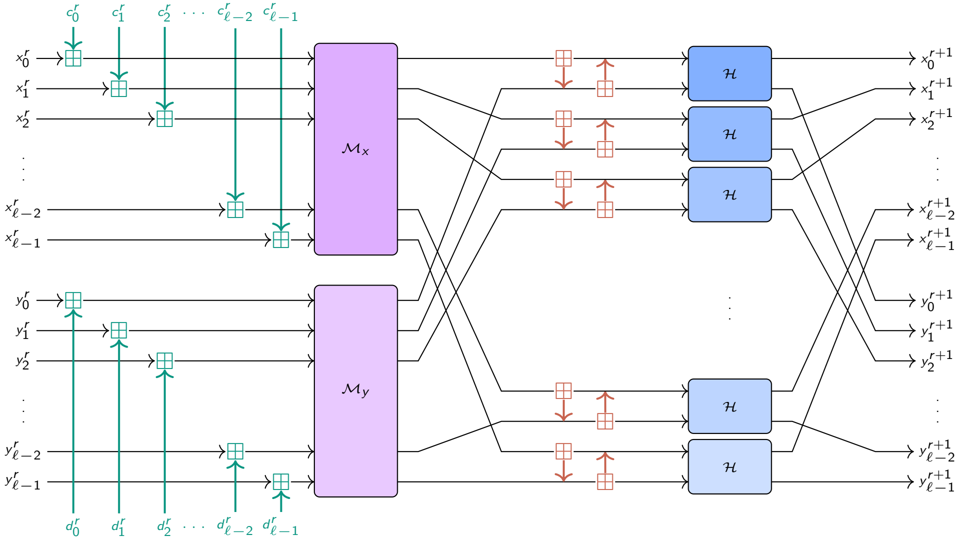
The internal state of Anemoi and its basic operations.



(a) *Internal state* **(b)** *The diffusion layer $\mathcal{M}$.* **(c)** *The PHT $\mathcal{P}$.*

(d) *The S-box layer $\mathcal{S}$.* **(e)** *The constant addition $\mathcal{A}$.*

The SPN Structure



Number of rounds

$$\texttt{Anemoi}_{q,\alpha,\ell} = \mathcal{M} \circ \mathrm{R}_{n_r-1} \circ \ldots \circ \mathrm{R}_0$$

⇒ Choosing the number of rounds:

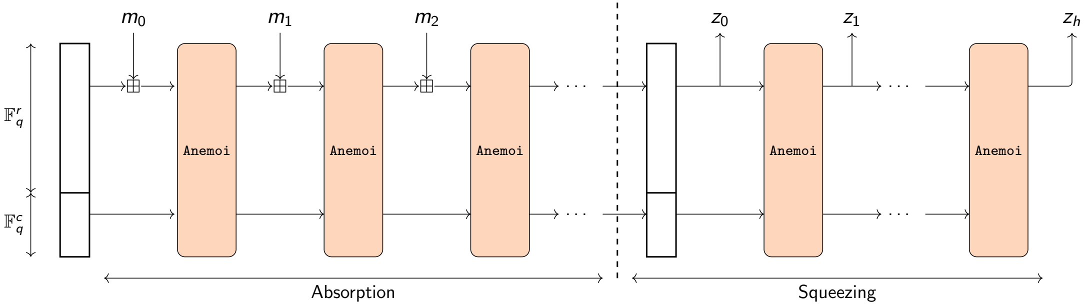
$$n_r \geq \max\left\{8\ ,\ \underbrace{\min(5, 1+\ell)}_{\text{security margin}} + \underbrace{2 + \min\left\{r \in \mathbb{N} \;\middle|\; \binom{4\ell r + \kappa_\alpha}{2\ell r}^2 \geq 2^s\right\}}_{\text{to prevent algebraic attacks}}\right\}.$$

α (κ_α)	3 (1)	5 (2)	7 (4)	11 (9)
$\ell = 1$	21	21	20	19
$\ell = 2$	14	14	13	13
$\ell = 3$	12	12	12	11
$\ell = 4$	12	12	11	11

Number of Rounds of Anemoi *($s = 128$).*

New Mode: Jive

- Hash function (random oracle):
  - input: arbitrary length
  - ouput: fixed length

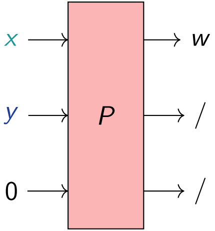


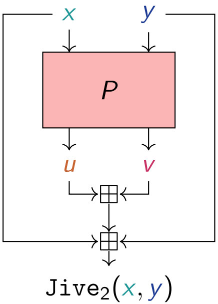
New Mode: Jive

- Hash function (random oracle):
  - input: arbitrary length
  - ouput: fixed length
- Compression function (Merkle-tree):
  - input: fixed length
  - output: (input length) /2

Dedicated mode ⇒ 2 words in 1

$$(x, y) \mapsto x + y + u + v \ .$$



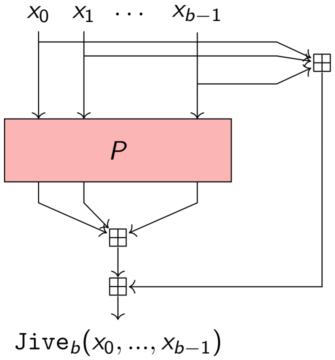


New Mode: Jive

- Hash function (random oracle):
  - input: arbitrary length
  - ouput: fixed length
- Compression function (Merkle-tree):
  - input: fixed length
  - output: (input length) /b

Dedicated mode ⇒ b words in 1

$$\texttt{Jive}_b(P) : \begin{cases} (\mathbb{F}_q^m)^b & \to \mathbb{F}_q^m \\ (x_0, \ldots, x_{b-1}) & \mapsto \sum_{i=0}^{b-1} (x_i + P_i(x_0, \ldots, x_{b-1})) \end{cases} .$$



Some Benchmarks

	m	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	-	**189**
	4	560	1336	**260**	308
	6	756	3024	-	**444**
	8	1152	5448	**574**	624
AIR	2	156	300	-	**126**
	4	**168**	348	**168**	**168**
	6	**162**	396	-	216
	8	**192**	480	264	288

(a) *when* $\alpha = 3$

	m	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	-	**210**
	4	528	1032	**222**	336
	6	768	2265	-	**480**
	8	1280	4003	**492**	672
AIR	2	**200**	360	-	210
	4	**220**	440	**220**	280
	6	**240**	540	-	360
	8	**320**	640	360	480

(b) *when* $\alpha = 5$

Constraint comparison for Rescue–Prime, Poseidon, Griffin *and* Anemoi *(*$s = 128$*)*
for standard arithmetization, without optimization.

Take-Away

Anemoi

- A new family of ZK-friendly hash functions
- Contributions of fundamental interest:
  - New S-box: `Flystel`
  - New mode: `Jive`
- Identify a link between AO and CCZ-equivalence

Conclusions

- A better understanding of the algebraic degree of MIMC_3
  - ☞ More details on doi.org/10.1007/s10623-022-01136-x (or eprint.iacr.org/2022/366)
- Practical attacks against AO hash functions
  - ☞ More details on doi.org/10.46586/tosc.v2022.i3.73-101
- Anemoi: a new family of ZK-friendly hash functions
  - ☞ More details on eprint.iacr.org/2022/840

Conclusions

- ⋆ A better understanding of the algebraic degree of MIMC_3
  - ☞ More details on doi.org/10.1007/s10623-022-01136-x (or eprint.iacr.org/2022/366)
- ⋆ Practical attacks against AO hash functions
  - ☞ More details on doi.org/10.46586/tosc.v2022.i3.73-101
- ⋆ Anemoi: a new family of ZK-friendly hash functions
  - ☞ More details on eprint.iacr.org/2022/840

Cryptanalysis and designing of arithmetization-oriented primitives remain to be explored!

Thanks for your attention!