Arithmetization-Oriented primitives:

A need for mathematical tools.

Clémence Bouvier [1,2]

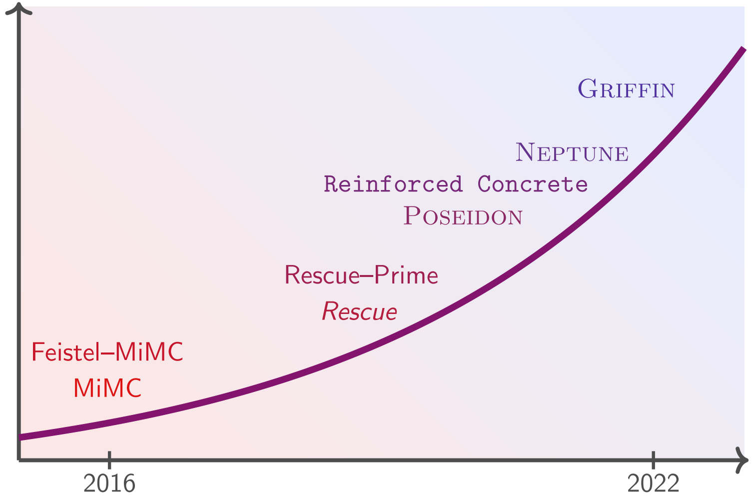
including joint works with Pierre Briaud[1,2], Anne Canteaut[2], Pyrros Chaidos[3], Léo Perrin[2], Robin Salen[4], Vesselin Velichkov[5,6] and Danny Willems[7,8]

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

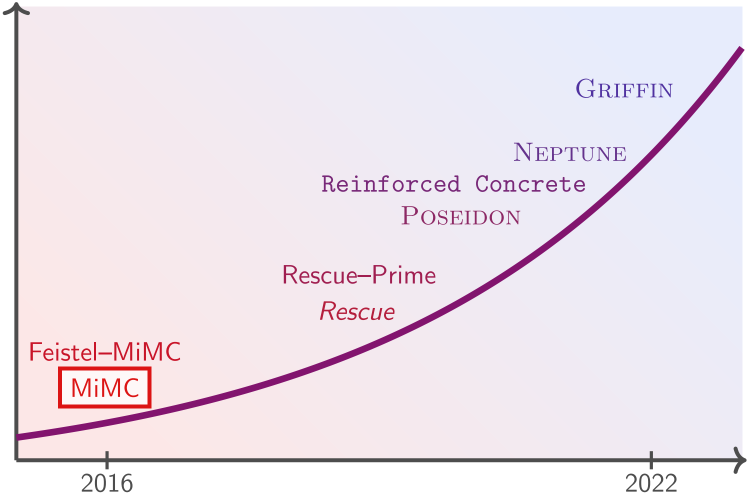
[3]National & Kapodistrian University of Athens, [4]Toposware Inc., Boston, [5]University of Edinburgh, [6]Clearmatics, London, [7]Nomadic Labs, Paris, [8]Inria and LIX, CNRS

October 20th, 2022

A fast moving domain



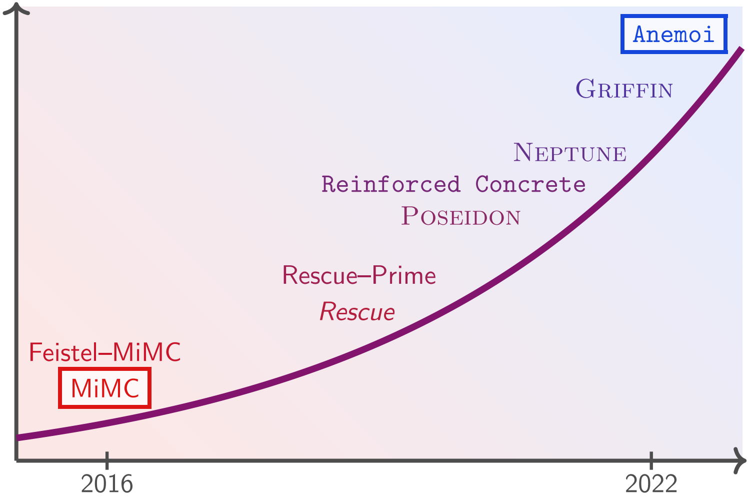
A fast moving domain



☞ [BCP22]

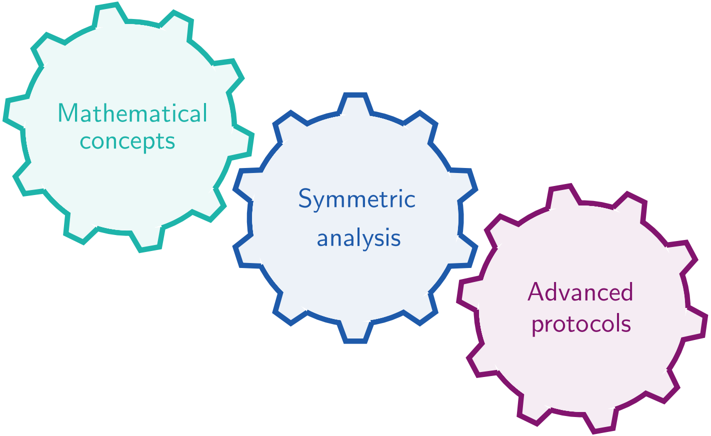
A fast moving domain

☞ [BCP22]



☞ [BBC+22]

Designing Arithmetization-Oriented Primitives



Content

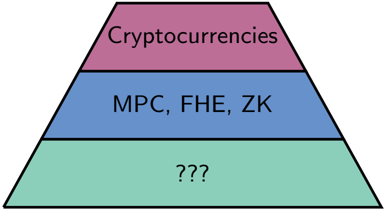
Arithmetization-Oriented primitives:
A need for mathematical tools.

A need of new primitives

Problem: Designing new symmetric primitives

Protocols requiring new primitives:

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

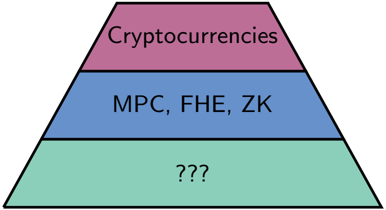


A need of new primitives

Problem: Designing new symmetric primitives

Protocols requiring new primitives:

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



Arithmetization-oriented primitives

$\Rightarrow$ What differs from the “usual” case?

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

$\mathbb{F}_p$, with p given by Standardized Elliptic Curves.

Examples:

- ⋆ Curve BLS12-381 $\log_2 p = 381$

$$p = 4002409555221667393417789825735904156556882819939007885332058136124031650490837864442687629129015664037894272559787$$

- ⋆ Curve BLS12-377 $\log_2 p = 377$

$$p = 258664426012969094010652733694893533536393512754914660539884262666720468348340822774968888139573360124440321458177$$

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

- Operations:
  $$y \leftarrow E(x)$$
- Efficiency:
  implementation in software/hardware

Arithmetization-friendly

- Operations:
  $$y == E(x)$$
- Efficiency:
  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 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

- Operations:
  $$y \leftarrow E(x)$$
- Efficiency:
  implementation in software/hardware

Arithmetization-friendly

- Operations:
  $$y == E(x)$$
- Efficiency:
  integration within advanced protocols

Symmetric cryptography

We assume that a key is already shared.

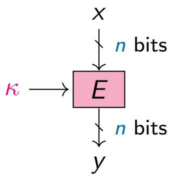
- Stream cipher
- Block cipher

Symmetric cryptography

We assume that a key is already shared.

- ⋆ Stream cipher
- ⋆ Block cipher

- ⋆ input: n-bit block x (i.e. $x \in \mathbb{F}_{2^n}$)
- ⋆ parameter: k-bit key κ (i.e. $\kappa \in \mathbb{F}_{2^k}$)
- ⋆ output: n-bit block $y = E_\kappa(x)$
- ⋆ symmetry: E and E^{-1} use the same κ

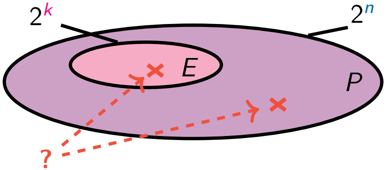


Block cipher

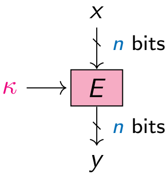
Symmetric cryptography

We assume that a key is already shared.

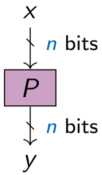
- Stream cipher
- Block cipher



- input: n-bit block x (i.e. $x \in \mathbb{F}_{2^n}$)
- parameter: k-bit key κ (i.e. $\kappa \in \mathbb{F}_{2^k}$)
- output: n-bit block $y = E_\kappa(x)$
- symmetry: E and E^{-1} use the same κ



Block cipher



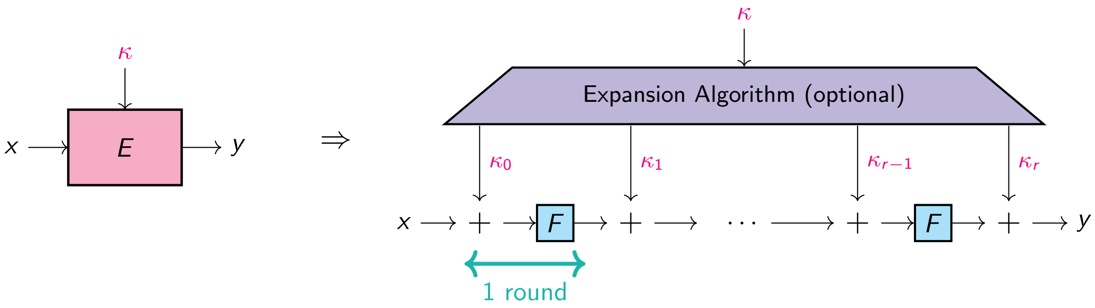
Random permutation

$\Rightarrow$ Block cipher: family of 2^k permutations of n bits.

Iterated constructions

⇒ How to build a block cipher?

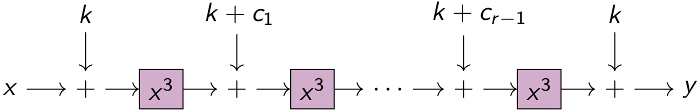
By iterating a round function.



Performance constraints! The primitive must be fast.

The block cipher MiMC

- ⋆ Minimize the number of multiplications in $\mathbb{F}_{2^n}$.
- ⋆ Construction of MiMC_3 [Albrecht et al., Eurocrypt16]:
  - ⋆ 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 $s = (2^{n+1} - 1)/3$



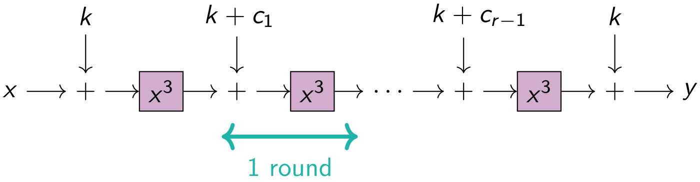
The block cipher MiMC

- Minimize the number of multiplications in $\mathbb{F}_{2^n}$.
- Construction of MiMC_3 [Albrecht et al., Eurocrypt16]:
  - 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.



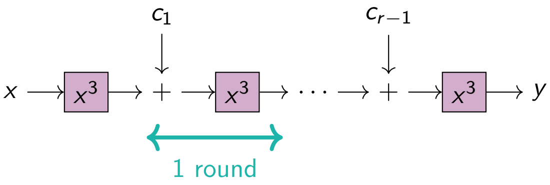
The block cipher MiMC

- Minimize the number of multiplications in $\mathbb{F}_{2^n}$.
- Construction of MiMC$_3$ [Albrecht et al., Eurocrypt16]:
  - 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 $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$, there is **a unique multivariate polynomial** in $\mathbb{F}_2[x_1, \ldots x_n]/\left((x_i^2 + x_i)_{1 \leq i \leq n}\right)$:

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

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

Definition

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

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

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 $\mathbb{F}_2[x_1, \ldots x_n] / \left((x_i^2 + x_i)_{1 \leq i \leq n} \right)$:

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

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

Algebraic degree - 2nd definition

Let $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$. 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 $F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$:

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

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

If $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ 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 $= n - 1$

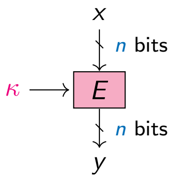
Integral attack

Exploiting a low algebraic degree

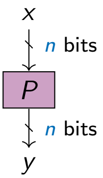
For any affine subspace $\mathcal{V} \subset \mathbb{F}_2^n$ with $\dim \mathcal{V} \geq \deg^a(F) + 1$, we have a 0-sum distinguisher:

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

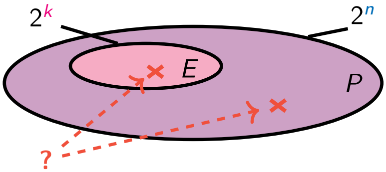
Random permutation: degree $= n - 1$



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 $B_3^r := \max_c \deg^a \text{MIMC}_{3,c}[r]$.

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 $B_3^r := \max_c \deg^a \mathrm{MIMC}_{3,c}[r]$.

⋆ Round 1: $B_3^1 = 2$

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

$$3 = [11]_2$$

⋆ Round 2: $B_3^2 = 2$

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

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

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: $B_3^2 = 2$

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

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

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 $B_3^r := \max_c \deg^a \text{MIMC}_{3,c}[r]$.

Definition

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

- Round 1: $B_3^1 = 2$

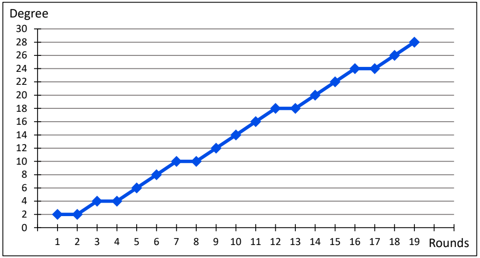
$$\mathcal{P}_1(x) = x^3, \quad (c_0 = 0)$$

$$3 = [11]_2$$

- 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 $B_3^r := \max_c \deg^a \mathrm{MIMC}_{3,c}[r]$.

Definition

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

- ⋆ Round 1: $B_3^1 = 2$

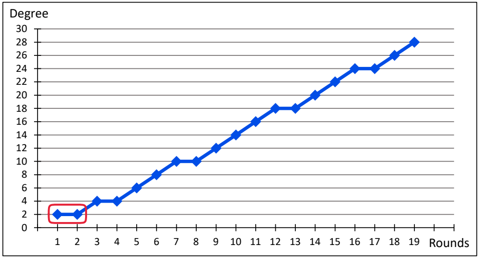
$$\mathcal{P}_1(x) = x^3, \quad (c_0 = 0)$$

$$3 = [11]_2$$

- ⋆ 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: $B_3^1 = 2$

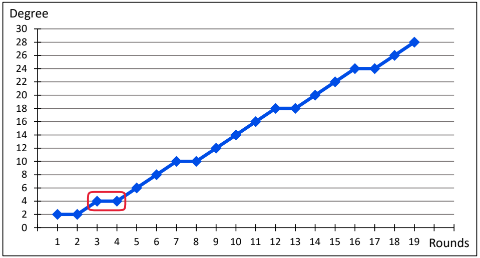
$$\mathcal{P}_1(x) = x^3, \quad (c_0 = 0)$$

$$3 = [11]_2$$

⋆ 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 $B_3^r := \max_c \deg^a \text{MIMC}_{3,c}[r]$.

Definition

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

⋆ <u>Round 1:</u> $B_3^1 = 2$

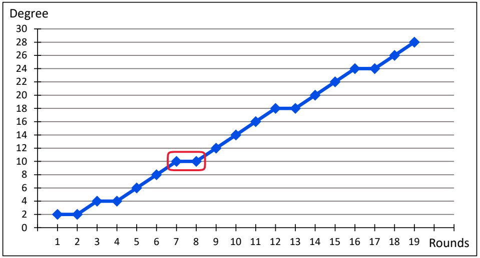
$$\mathcal{P}_1(x) = x^3, \quad (c_0 = 0)$$

$$3 = [11]_2$$

⋆ <u>Round 2:</u> $B_3^2 = 2$

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

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



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: $B_3^1 = 2$

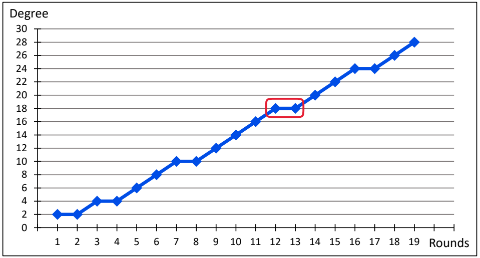
$$\mathcal{P}_1(x) = x^3, \quad (c_0 = 0)$$

$$3 = [11]_2$$

⋆ 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 $B_3^r := \max_c \deg^a \text{MIMC}_{3,c}[r]$.

Definition

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

⋆ Round 1: $B_3^1 = 2$

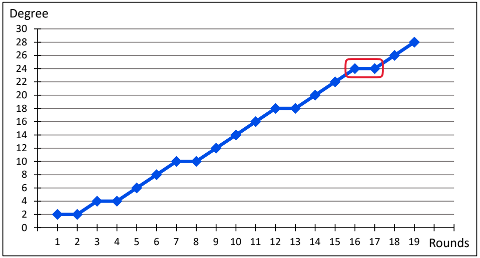
$$\mathcal{P}_1(x) = x^3, \quad (c_0 = 0)$$

$$3 = [11]_2$$

⋆ 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 $2^{2k} - 1$

$$\mathcal{E}_r \subseteq \{ \begin{array}{cccccccc} 0 & 3 & 6 & 9 & 12 & \not{15} & 18 & \not{21} \\ 24 & 27 & 30 & 33 & 36 & \not{39} & 42 & \not{45} \\ 48 & 51 & 54 & 57 & 60 & \not{63} & 66 & \not{69} \\ & & & & & & & \\ \dots & 3^r\} & & & & & & \end{array}$$

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

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

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

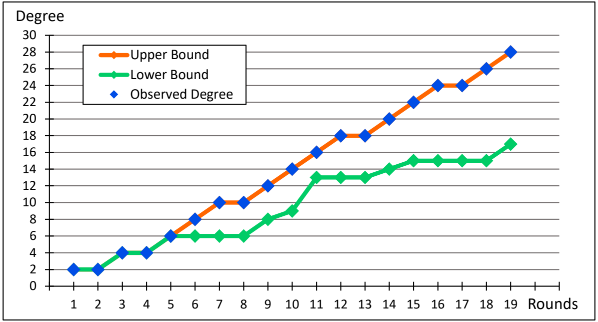
Theorem

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

Example:

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

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 $k_r = 1 \mod 2$,

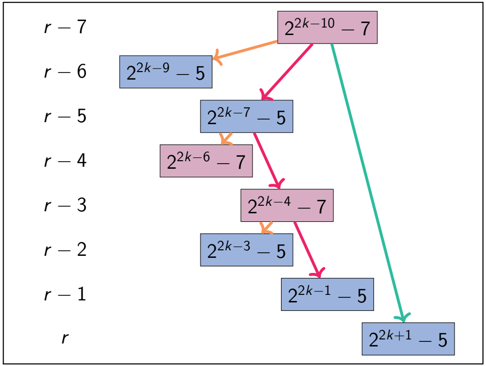
$$\omega_r = 2^{k_r} - 5 \in \mathcal{E}_r,$$

- if $k_r = 0 \mod 2$,

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

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.

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

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 $k_r = 1 \bmod 2$,

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

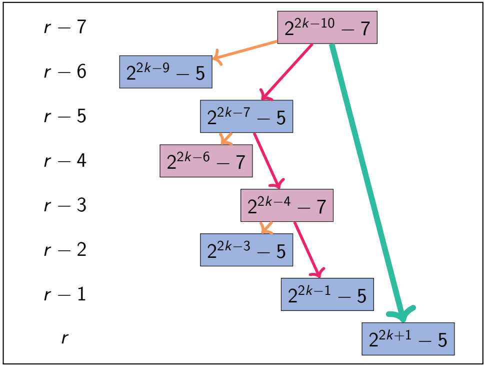
- ⋆ if $k_r = 0 \bmod 2$,

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

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.

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

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 $k_r = 1 \bmod 2$,

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

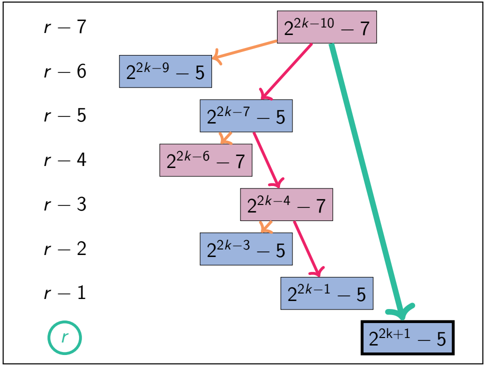
- if $k_r = 0 \bmod 2$,

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

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.

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

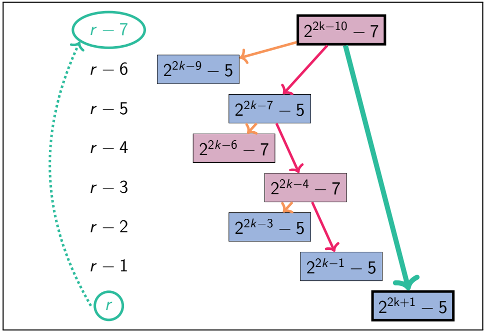
Exact degree

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:

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

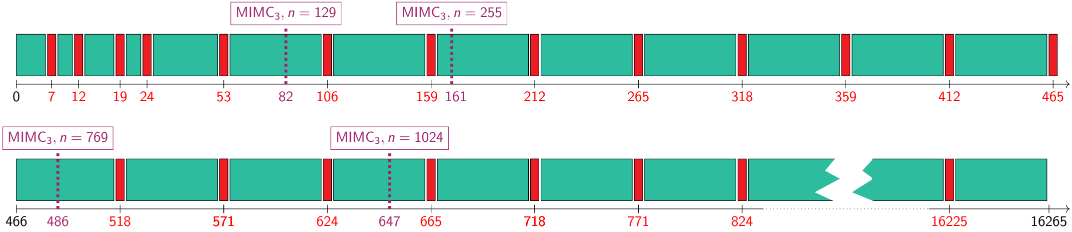
$$\exists \ell \text{ s.t. } \quad \omega_{r-\ell} \in \mathcal{E}_{r-\ell} \Rightarrow \omega_r \in \mathcal{E}_r$$

Covered rounds

Idea of the proof:

⋆ inductive proof: existence of "good" ℓ

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



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

Covered rounds

Idea of the proof:

- ⋆ inductive proof: existence of "good" ℓ

Limit: $\ell = 22$.

Observation

$$\forall\ 1 \leq t \leq 21,\ \forall\ x \in \mathbb{Z}/3^t\mathbb{Z},\ \exists\ \varepsilon_2, \ldots, \varepsilon_{2t+2} \in \{0,1\},\ \text{s.t. } x = \sum_{j=2}^{2t+2} \varepsilon_j 4^j \bmod 3^t\ .$$

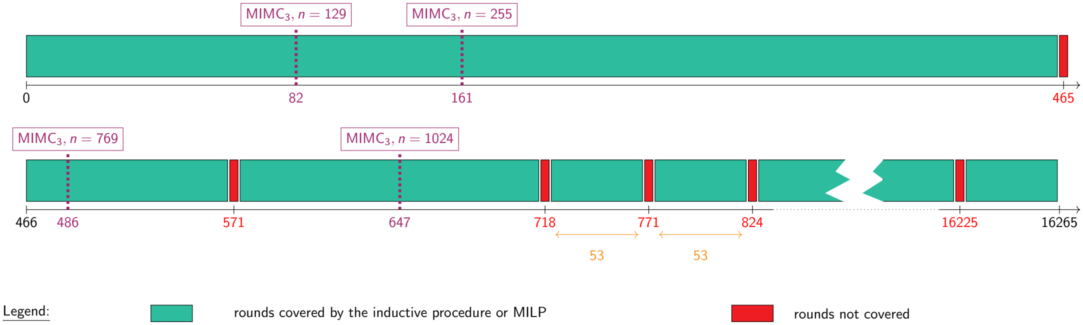
Is this true for any t? Should we consider more ε_j for larger t?

Covered rounds

Idea of the proof:

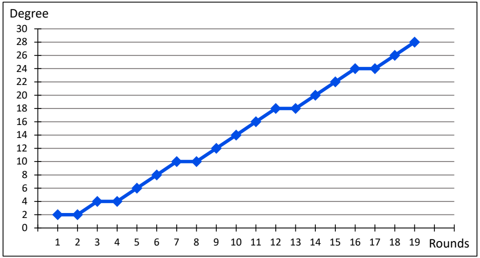
- ⋆ inductive proof: existence of “good” ℓ
- ⋆ MILP solver (`PySCIPOpt`)

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



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 $(k_r)_{r>0}$:

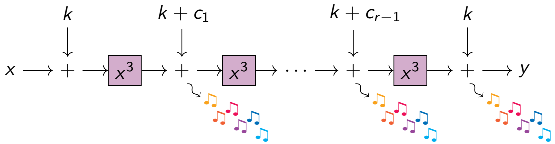
  $\Rightarrow$ denominators of semiconvergents of $\log_2(3) \simeq 1.5849625$

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

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

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

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



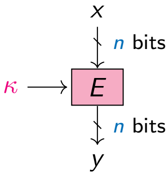
Integral attack

Exploiting a low algebraic degree

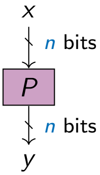
For any affine subspace $\mathcal{V} \subset \mathbb{F}_2^n$ with $\dim \mathcal{V} \geq \deg^a(F) + 1$, we have a 0-sum distinguisher:

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

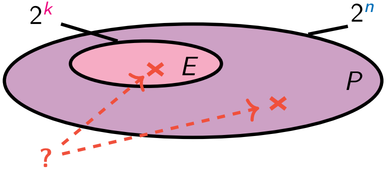
Random permutation: degree $= n - 1$



Block cipher

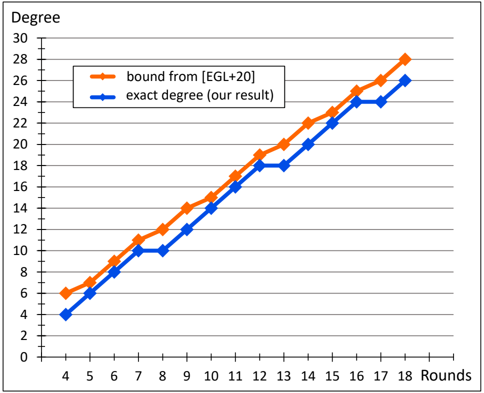


Random permutation



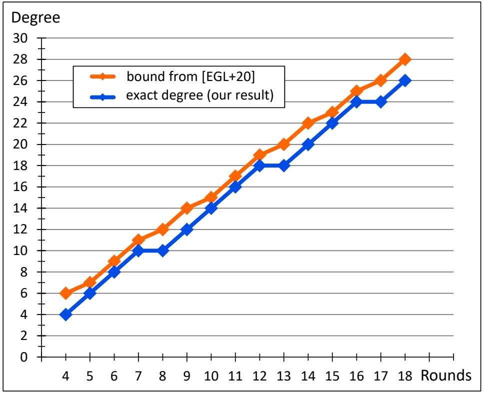
Comparison to previous work

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: $\lceil r \log_2 3 \rceil$ $\Rightarrow$ 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 ($n = 129$)

Anemoi

Why Anemoi?

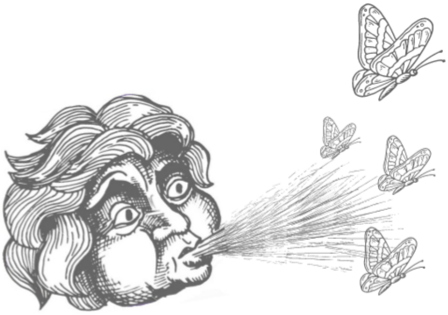
- Anemoi
  Family of ZK-friendly Hash functions

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.

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:

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:

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

Differential and Linear properties

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

- Differential uniformity: maximum value of the DDT (Difference Distribution Table)

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

- Linearity: maximum value of the LAT (Linear Approximation Table)

$$\mathcal{W}_F = \max_{a, b \neq 0} \left| \sum_{x \in \mathbb{F}_2^m} (-1)^{a \cdot x + b \cdot F(x)} \right|$$

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

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, $\mathcal{A}(x) = \mathcal{L}(x) + c$.

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: $\delta_F = \delta_G$.

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: $\mathcal{W}_F = \mathcal{W}_G$.

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]

$F : \mathbb{F}_q \to \mathbb{F}_q$ 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: $\mathcal{W}_F = \mathcal{W}_G$.
- ⋆ Verification is the same: if $y \leftarrow F(x)$, $v \leftarrow G(u)$

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

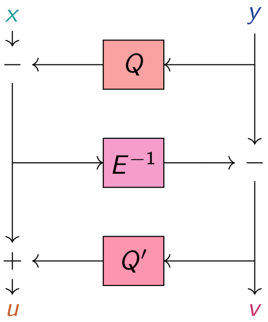
- ⋆ The degree is not preserved.

The Flystel

Butterfly + Feistel ⇒ Flystel

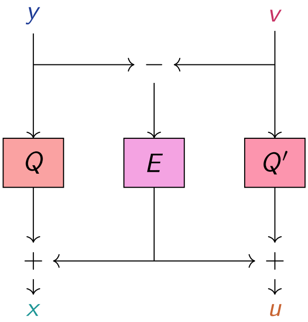
A 3-round Feistel-network with
$Q : \mathbb{F}_q \rightarrow \mathbb{F}_q$ and $Q' : \mathbb{F}_q \rightarrow \mathbb{F}_q$ two quadratic functions, and $E : \mathbb{F}_q \rightarrow \mathbb{F}_q$ a permutation

High-degree permutation



Open Flystel $\mathcal{H}$.

Low-degree function



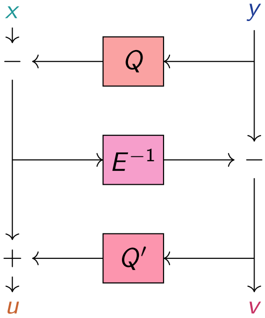
Closed Flystel $\mathcal{V}$.

The Flystel

$\mathcal{H}$ and $\mathcal{V}$
are CCZ-equivalent

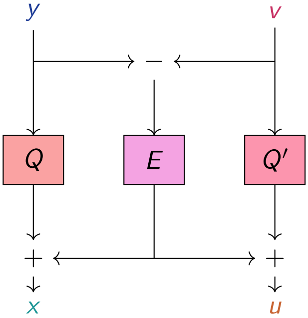
$$\Gamma_{\mathcal{H}} = \{(\ (x,y),\ \mathcal{H}((x,y))\ ) \mid (x,y) \in \mathbb{F}_q^2\}$$
$$= \mathcal{A}\left(\{(\ (v,y),\ \mathcal{V}((v,y))\ ) \mid (v,y) \in \mathbb{F}_q^2\}\right) = \mathcal{A}(\Gamma_{\mathcal{V}})$$

High-degree permutation



Open Flystel $\mathcal{H}$.

Low-degree function

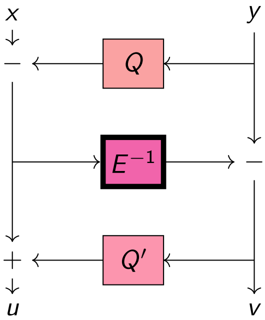


Closed Flystel $\mathcal{V}$.

Advantage of CCZ-equivalence

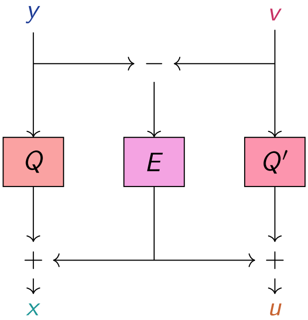
⋆ High Degree Evaluation.

High-degree permutation



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

Low-degree function



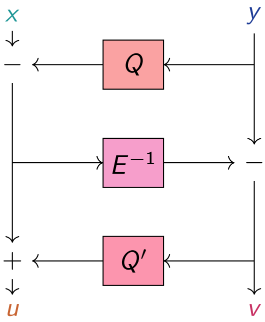
Closed `Flystel` $\mathcal{V}$.

Advantage of CCZ-equivalence

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

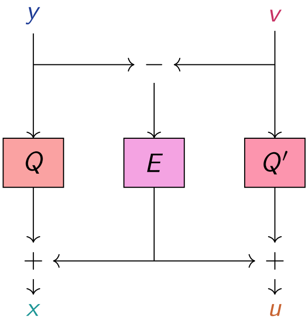
$$(u, v) == \mathcal{H}(x, y) \Leftrightarrow (x, u) == \mathcal{V}(y, v)$$

High-degree permutation



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

Low-degree function

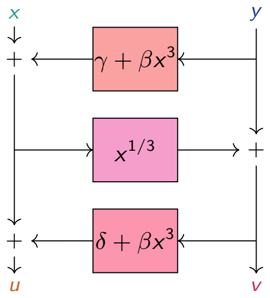


Closed `Flystel` $\mathcal{V}$.

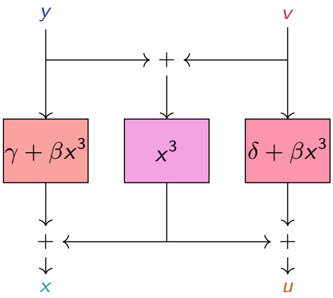
Flystel in $\mathbb{F}_{2^n}$

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

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

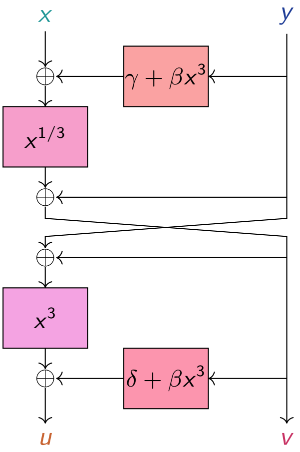


Open Flystel$_2$.



Closed Flystel$_2$.

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



Degenerated Butterfly.

First introduced by [Perrin et al. 2016].

Well-studied butterfly.

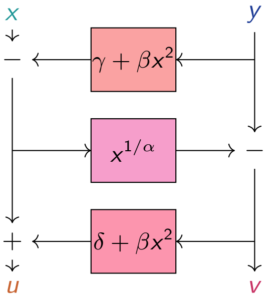
Theorems in [Li et al. 2018] state that if $\beta \neq 0$:

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

Flystel in $\mathbb{F}_p$

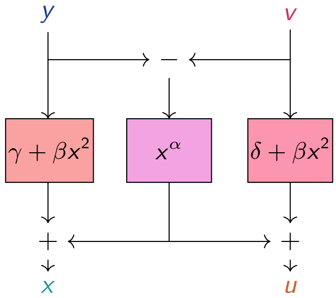
$$\mathcal{H} : \begin{cases} \mathbb{F}_p \times \mathbb{F}_p & \to \mathbb{F}_p \times \mathbb{F}_p \\ (x, y) & \mapsto \left(x - \beta y^2 - \gamma + \beta \left(y - (x - \beta y^2 - \gamma)^{1/\alpha} \right)^2 + \delta \,, \right. \\ & \quad \left. y - (x - \beta y^2 - \gamma)^{1/\alpha} \right)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

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



Open Flystel$_p$.

usually
$\alpha = 3$ or 5.

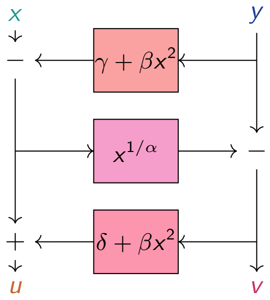


Closed Flystel$_p$.

Flystel in $\mathbb{F}_p$

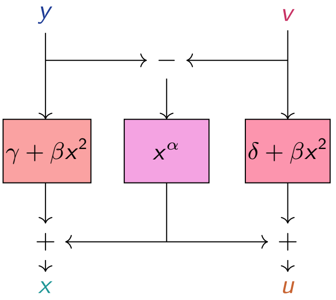
Example   Curve BLS12-381:

$$p = 4002409555221667393417789825735904156556882819939007885332$$
$$058136124031650490837864442687629129015664037894272559787$$
$$\alpha = 5$$
$$\alpha^{-1} = 3201927644177333914734231860588723325245506255951206308265$$
$$6465088992253203926702915541501033032125312303154180478 29$$



Open $\texttt{Flystel}_p$.

usually
$\alpha = 3$ or 5.

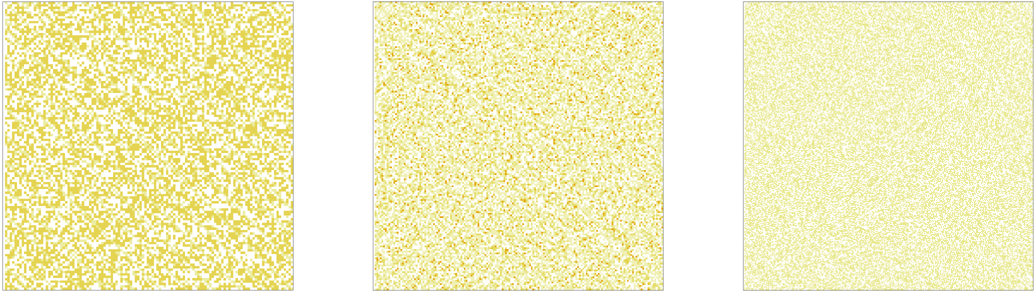


Closed $\texttt{Flystel}_p$.

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

⋆ Differential properties

$\mathtt{Flystel_p}$ has a differential uniformity equals to $\alpha - 1$.



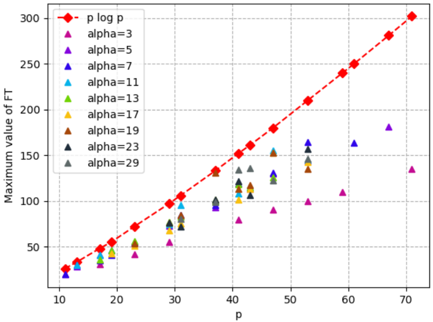
(a) *when* $p = 11$ *and* $\alpha = 3$. **(b)** *when* $p = 13$ *and* $\alpha = 5$. **(c)** *when* $p = 17$ *and* $\alpha = 3$.

DDT of $\mathtt{Flystel_p}$.

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

⋆ Linear properties

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

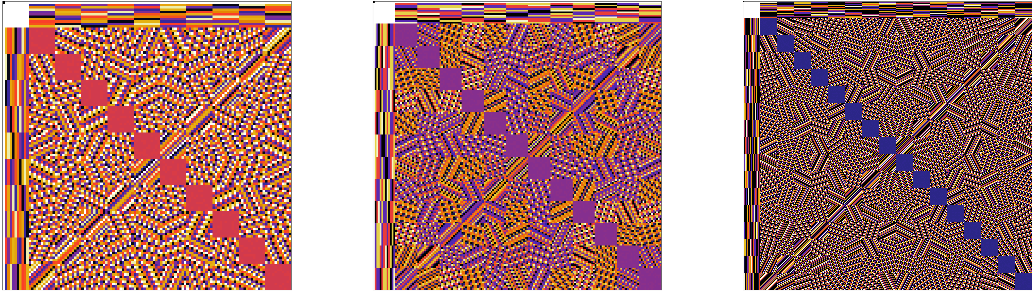


Conjecture for the linearity.

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

(**SPN:** Substitution-Permutation Network)

Let

$$X = \begin{pmatrix} x_0 & x_1 & \ldots & x_{\ell-1} \end{pmatrix} \text{ and } Y = \begin{pmatrix} y_0 & y_1 & \ldots & y_{\ell-1} \end{pmatrix} \text{ with } x_i, y_i \in \mathbb{F}_q \ .$$

The internal state of Anemoi can be represented as:

$$\begin{pmatrix} X \\ Y \end{pmatrix} .$$

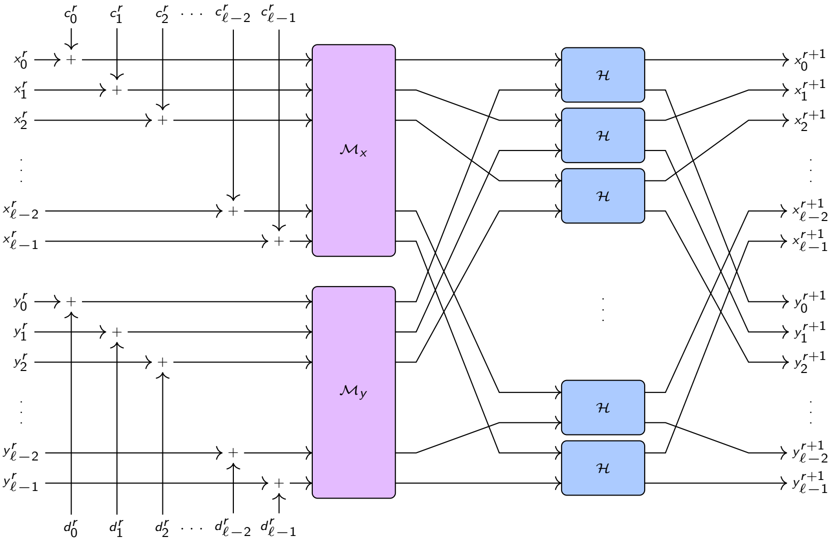
Addition of constants and the linear layer as:

$$\begin{pmatrix} X \\ Y \end{pmatrix} \mapsto \begin{pmatrix} X \\ Y \end{pmatrix} + \begin{pmatrix} C \\ D \end{pmatrix}, \quad \begin{pmatrix} X \\ Y \end{pmatrix} \mapsto \begin{pmatrix} X\mathcal{M}_x \\ Y\mathcal{M}_y \end{pmatrix} .$$

And the S-Box layer as:

$$\begin{pmatrix} X \\ Y \end{pmatrix} \mapsto \begin{pmatrix} {}^t\mathcal{H}(x_0, y_0) & {}^t\mathcal{H}(x_1, y_1) & \ldots & {}^t\mathcal{H}(x_{\ell-1}, y_{\ell-1}) \end{pmatrix} .$$

The SPN Structure



Overview of `Anemoi`*.*

Some Benchmarks

	m	*Rescue′*	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	-	**173**
	4	560	1336	291	**220**
	6	756	3024	-	**320**
	8	1152	5448	635	**456**
AIR	2	156	300	-	**114**
	4	168	348	168	**144**
	6	**162**	396	-	180
	8	**192**	480	264	240

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

	m	*Rescue′*	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	-	**192**
	4	528	1032	253	**244**
	6	768	2265	-	**350**
	8	1280	4003	543	**496**
AIR	2	200	360	-	**190**
	4	**220**	440	**220**	240
	6	**240**	540	-	300
	8	**320**	640	360	400

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

Constraint comparison for Rescue–Prime, Poseidon, Griffin *and* Anemoi *(we fix* $s = 128$*).*

Some Benchmarks

	m	Rescue′	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	-	**173**
	4	560	1336	291	**220**
	6	756	3024	-	**320**
	8	1152	5448	635	**456**
AIR	2	156	300	-	**114**
	4	168	348	168	**144**
	6	**162**	396	-	180
	8	**192**	480	264	240

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

	m	Rescue′	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	-	**192**
	4	528	1032	253	**244**
	6	768	2265	-	**350**
	8	1280	4003	543	**496**
AIR	2	200	360	-	**190**
	4	**220**	440	**220**	240
	6	**240**	540	-	300
	8	**320**	640	360	400

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

Constraint comparison for Rescue–Prime, Poseidon, Griffin *and* Anemoi *(we fix* $s = 128$*).*

Conclusions

- Algebraic degree of MIMC_3
  - A tight upper bound, up to 16265 rounds: $2 \times \lceil \lfloor \log_2(3^r) \rfloor /2 - 1 \rceil$.
  - The minimal complexity for higher-order differential attack

☞ More details on eprint.iacr.org/2022/366
and to appear in *Designs, Codes and Cryptography*

Conclusions

- Algebraic degree of MIMC_3
  - A tight upper bound, up to 16265 rounds: $2 \times \lceil \lfloor \log_2(3^r) \rfloor /2 - 1 \rceil$.
  - The minimal complexity for higher-order differential attack

☞ More details on eprint.iacr.org/2022/366
and to appear in *Designs, Codes and Cryptography*

- Anemoi
  - A new family of ZK-friendly hash functions efficient accross proof system
  - New observations of fundamental interest:
    - Standalone component: Flystel
    - Identify a link between AO and CCZ-equivalence

☞ More details on eprint.iacr.org/2022/840

Future Work

Cryptanalysis and designing of arithmetization-oriented primitives remain to be explored!
And the opinion of mathematicians would be of great help to us!

Future Work

Cryptanalysis and designing of arithmetization-oriented primitives remain to be explored!
And the opinion of mathematicians would be of great help to us!

- On MIMC
  - solve the conjecture for maximum-weight exponents
  - extend the analysis to MIMC_d for any d, to SPN constructions, ...

Future Work

Cryptanalysis and designing of arithmetization-oriented primitives remain to be explored!
And the opinion of mathematicians would be of great help to us!

- On MIMC
  - solve the conjecture for maximum-weight exponents
  - extend the analysis to MIMC_d for any d, to SPN constructions, ...
- On `Anemoi`:
  - explaining linear properties of the `Flystel`.
  - pushing further the use of CCZ-equivalence for AO primitives

Future Work

Cryptanalysis and designing of arithmetization-oriented primitives remain to be explored!
And the opinion of mathematicians would be of great help to us!

- On MIMC
  - solve the conjecture for maximum-weight exponents
  - extend the analysis to MIMC_d for any d, to SPN constructions, ...
- On `Anemoi`:
  - explaining linear properties of the `Flystel`.
  - pushing further the use of CCZ-equivalence for AO primitives

Thanks for your attention!