New uses in Symmetric Cryptography:
From Cryptanalysis to Designing

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] and Vesselin Velichkov[4,5]

[1]Sorbonne Université, [2]Inria Paris,
[3]National & Kapodistrian University of Athens, [4]University of Edinburgh, [5]Clearmatics, London

May 20th, 2022

Some motivations

A Cryptanalysis Challenge for ZK-friendly Hash Functions!
In November 2021, by the Ethereum Fundation.

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

(a) *Feistel-MiMC*

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

(b) *Rescue Prime*

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

(c) *Poseidon*

☞ *Bariant, Bouvier, Leurent, Perrin*
Practical Algebraic Attacks against some Arithmetization-oriented Hash Functions

Total Bounty Budget: $200 000

Some motivations

A Cryptanalysis Challenge for ZK-friendly Hash Functions!
In November 2021, by the Ethereum Fundation.

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

(a) *Feistel-MiMC*

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

(b) *Rescue Prime*

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

(c) *Poseidon*

☞ *Bariant, Bouvier, Leurent, Perrin*
Practical Algebraic Attacks against some Arithmetization-oriented Hash Functions

Total Bounty Budget: $200 000

More and more primitives

Some motivations

A Cryptanalysis Challenge for ZK-friendly Hash Functions!
In November 2021, by the Ethereum Fundation.

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

(a) *Feistel-MiMC*

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

(b) *Rescue Prime*

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

(c) *Poseidon*

☞ *Bariant, Bouvier, Leurent, Perrin*
Practical Algebraic Attacks against some Arithmetization-oriented Hash Functions

Total Bounty Budget: $200 000

More and more primitives that need to be better understood!

Content

New uses in Symmetric Cryptography:
From Cryptanalysis to Designing.

1. Emerging uses in symmetric cryptography
   - A need of new primitives
   - Comparison with “usual” case
2. On the algebraic degree of $MiMC_3$
   - Preliminaries
   - Exact degree
   - Integral attacks
3. Practical Attacks
4. Anemoi
   - CCZ-equivalence
   - New Mode

Background

Symmetric cryptography: we assume that a key is already shared.

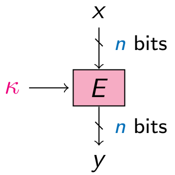
- ⋆ Stream cipher
- ⋆ Block cipher

Background

Symmetric cryptography: we assume that a key is already shared.

- ⋆ Stream cipher
- ⋆ Block cipher

- ⋆ input: n-bit block x
- ⋆ parameter: k-bit key κ
- ⋆ output: n-bit block $y = E_\kappa(x)$
- ⋆ symmetry: E and E^{-1} use the same κ



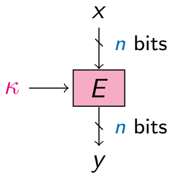
Block cipher

Background

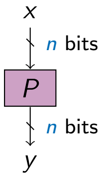
Symmetric cryptography: we assume that a key is already shared.

- Stream cipher
- Block cipher

- input: n-bit block x
- parameter: k-bit key κ
- output: n-bit block $y = E_\kappa(x)$
- symmetry: E and E^{-1} use the same κ



Block cipher



Random permutation

A need of new primitives

Problem: Analyzing the security of new symmetric primitives

Protocols requiring new primitives:

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

Primitives designed to minimize the number of multiplications in finite fields.

A need of new primitives

Problem: Analyzing the security of new symmetric primitives

Protocols requiring new primitives:

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

Primitives designed to minimize the number of multiplications in finite fields.

$\Rightarrow$ 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

New properties

"Usual" case

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

Arithmetization-friendly

- Operations:
  $$y == R(x)$$
- 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:

$$y \leftarrow R(x)$$

- Efficiency:
  implementation in software/hardware

Arithmetization-friendly

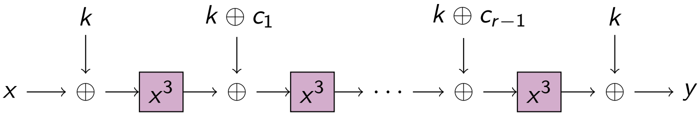
- Operations:

$$y == R(x)$$

- Efficiency:
  integration within advanced protocols

The block cipher MiMC

- Minimize the number of multiplications in $\mathbb{F}_{2^n}$.
- Construction of MiMC_3 [Albrecht et al., EC16]:
  - n-bit blocks (n odd ≈ 129)
  - n-bit key k
  - decryption : replacing x^3 by x^s where $s = (2^{n+1} - 1)/3$



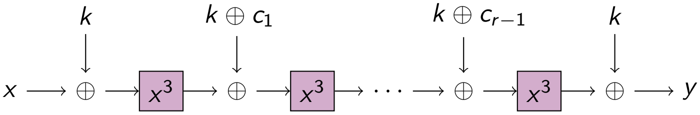
The block cipher MiMC

- Minimize the number of multiplications in $\mathbb{F}_{2^n}$.
- Construction of MiMC_3 [Albrecht et al., EC16]:
  - n-bit blocks (n odd ≈ 129)
  - n-bit key k
  - 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 instances.



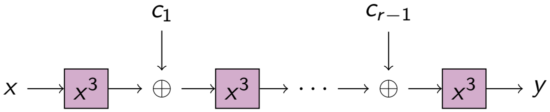
The block cipher MiMC

- Minimize the number of multiplications in $\mathbb{F}_{2^n}$.
- Construction of MiMC$_3$ [Albrecht et al., EC16]:
  - n-bit blocks (n odd ≈ 129)
  - n-bit key k
  - 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 instances.



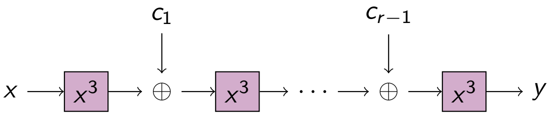
The block cipher MiMC

- Minimize the number of multiplications in $\mathbb{F}_{2^n}$.
- Construction of MiMC$_3$ [Albrecht et al., EC16]:
  - n-bit blocks (n odd ≈ 129)
  - n-bit key k
  - 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 instances.



☞ *Bouvier, Canteaut, Perrin*
On the Algebraic Degree of Iterated Power Functions

Algebraic degree

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

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

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

Definition

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

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

Algebraic degree

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

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

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

Definition

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

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

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

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

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

Algebraic degree

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

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

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

Algebraic degree

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

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

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

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

Higher-order differential 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 $= n - 1$

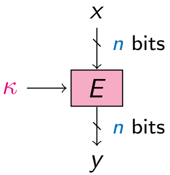
Higher-order differential attack

Exploiting a low algebraic degree

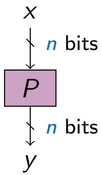
For any affine subspace $\mathcal{V} \subset \mathbb{F}_2^n$ with $\dim \mathcal{V} \geq \deg^a(F) + 1$, we have a 0-sum distinguisher:

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

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., AC20]: $\lceil r \log_2 3 \rceil$.
- ⋆ Aim: determine $B_3^r := \max_c \deg^a \mathrm{MIMC}_{3,c}[r]$.

First Plateau

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

For r rounds:

- ⋆ Upper bound [Eichlseder et al., AC20]: $\lceil r \log_2 3 \rceil$.
- ⋆ Aim: determine $B_3^r := \max_c \deg^a \text{MIMC}_{3,c}[r]$.

⋆ Round 1: $B_3^1 = 2$

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

$$3 = [11]_2$$

First Plateau

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

For r rounds:

- ⋆ Upper bound [Eichlseder et al., AC20]: $\lceil r \log_2 3 \rceil$.
- ⋆ Aim: determine $B_3^r := \max_c \deg^a \text{MIMC}_{3,c}[r]$.

⋆ <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> $B_3^2 = 2$

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

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

First Plateau

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

For r rounds:

- ⋆ Upper bound [Eichlseder et al., AC20]: $\lceil r \log_2 3 \rceil$.
- ⋆ 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., AC20]: $\lceil r \log_2 3 \rceil$.
- ⋆ 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: $B_3^2 = 2$

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

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

First Plateau

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

For r rounds:

- ⋆ Upper bound [Eichlseder et al., AC20]: $\lceil r \log_2 3 \rceil$.
- ⋆ Aim: determine $B_3^r := \max_c \deg^a \mathrm{MIMC}_{3,c}[r]$.

⋆ Round 1: $B_3^1 = 2$

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

$$3 = [11]_2$$

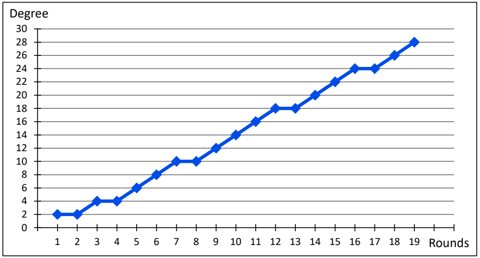
⋆ Round 2: $B_3^2 = 2$

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

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

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., AC20]: $\lceil r \log_2 3 \rceil$.
- ⋆ Aim: determine $B_3^r := \max_c \deg^a \mathrm{MIMC}_{3,c}[r]$.

⋆ Round 1: $B_3^1 = 2$

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

$$3 = [11]_2$$

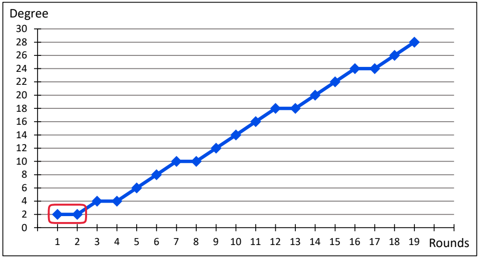
⋆ Round 2: $B_3^2 = 2$

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

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

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., AC20]: $\lceil r \log_2 3 \rceil$.
- ⋆ Aim: determine $B_3^r := \max_c \deg^a \text{MIMC}_{3,c}[r]$.

⋆ Round 1: $B_3^1 = 2$

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

$$3 = [11]_2$$

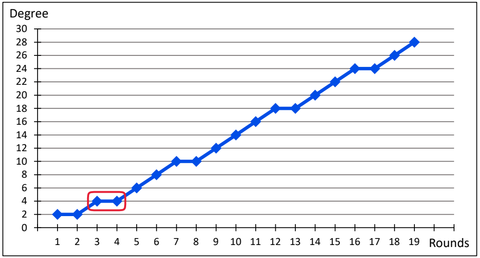
⋆ Round 2: $B_3^2 = 2$

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

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

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., AC20]: $\lceil r \log_2 3 \rceil$.
- ⋆ Aim: determine $B_3^r := \max_c \deg^a \mathrm{MIMC}_{3,c}[r]$.

⋆ <u>Round 1:</u> $B_3^1 = 2$

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

$$3 = [11]_2$$

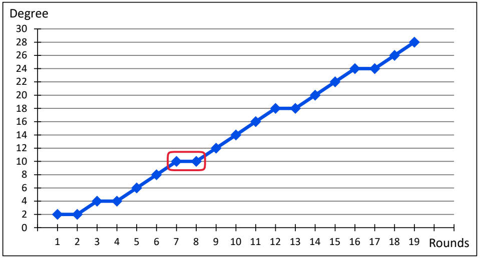
⋆ <u>Round 2:</u> $B_3^2 = 2$

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

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

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., AC20]: $\lceil r \log_2 3 \rceil$.
- ⋆ Aim: determine $B_3^r := \max_c \deg^a \text{MIMC}_{3,c}[r]$.

⋆ Round 1: $B_3^1 = 2$

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

$$3 = [11]_2$$

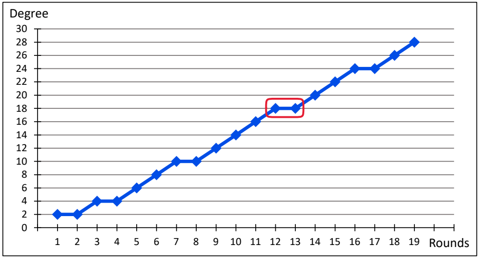
⋆ Round 2: $B_3^2 = 2$

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

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

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., AC20]: $\lceil r \log_2 3 \rceil$.
- ⋆ 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: $B_3^1 = 2$

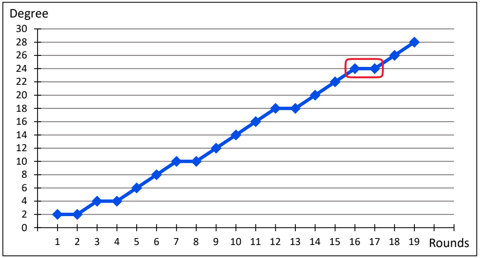
$$\mathcal{P}_1(x) = x^3, \quad (c_0 = 0)$$

$$3 = [11]_2$$

⋆ 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

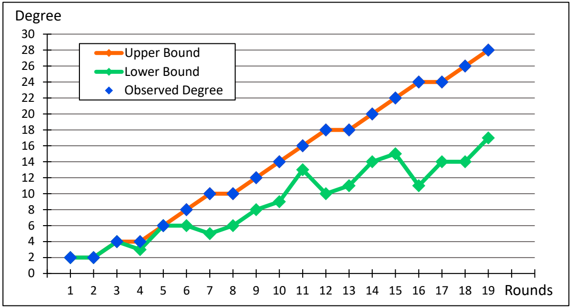
Theorem

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

$$B_3^r \geq wt(3^r)$$



Exact degree

Maximum-weight exponents:

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

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

- ⋆ if k_r is odd,

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

- ⋆ if k_r is even,

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

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

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

- if k_r is odd,

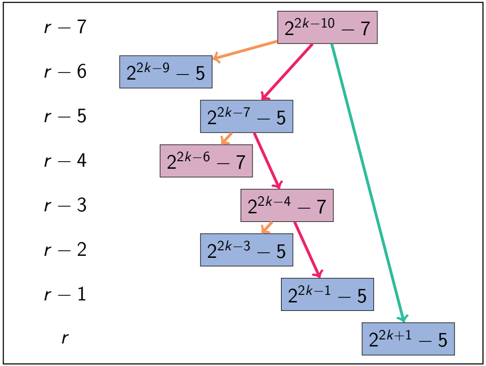
$$\omega_r = 2^{k_r} - 5 \in \mathcal{E}_r ,$$

- if k_r is even,

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

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

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

- if k_r is odd,

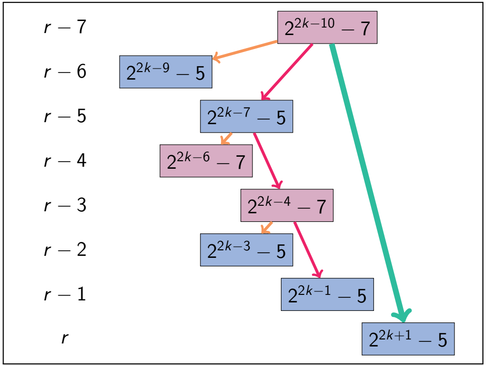
$$\omega_r = 2^{k_r} - 5 \in \mathcal{E}_r,$$

- if k_r is even,

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

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

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

- if k_r is odd,

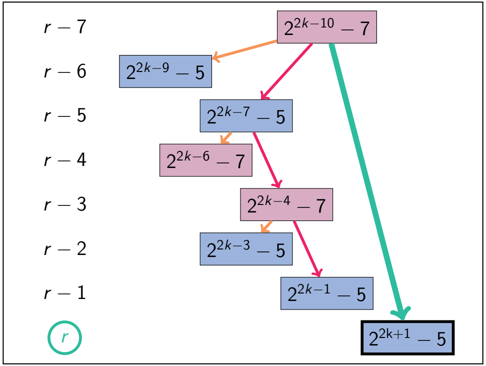
$$\omega_r = 2^{k_r} - 5 \in \mathcal{E}_r,$$

- if k_r is even,

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

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:

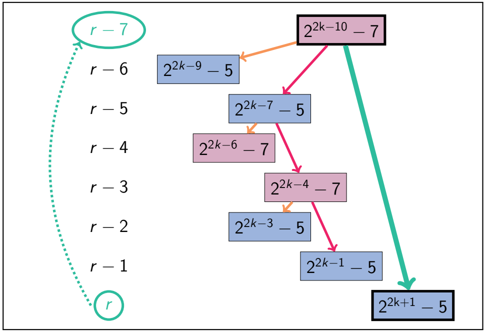
Let $k_r = \lfloor r \log_2 3 \rfloor$.

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

- if k_r is odd,
$$\omega_r = 2^{k_r} - 5 \in \mathcal{E}_r,$$
- if k_r is even,
$$\omega_r = 2^{k_r} - 7 \in \mathcal{E}_r.$$

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.

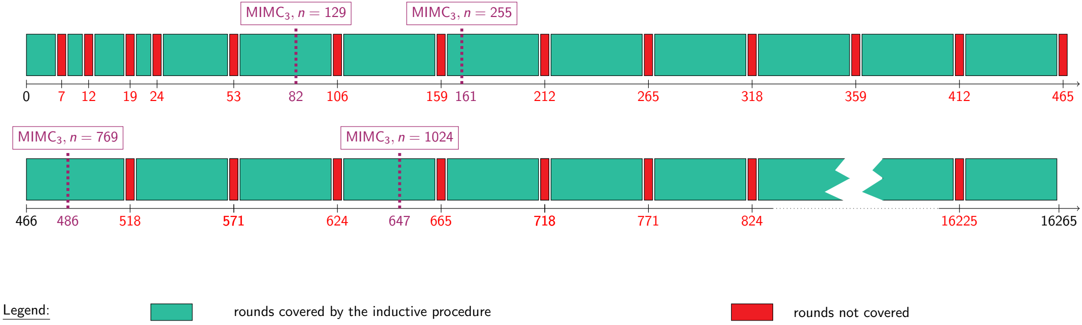
$$\exists \ell \text{ s.t. } \quad \omega_{r-\ell} \in \mathcal{E}_{r-\ell} \Rightarrow \omega_r \in \mathcal{E}_r$$

Covered rounds

Idea of the proof:

- ⋆ inductive proof: existence of "good" ℓ

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

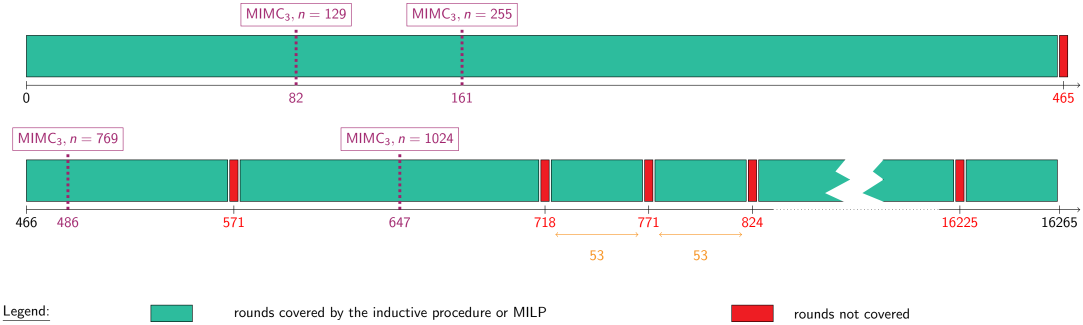


Covered rounds

Idea of the proof:

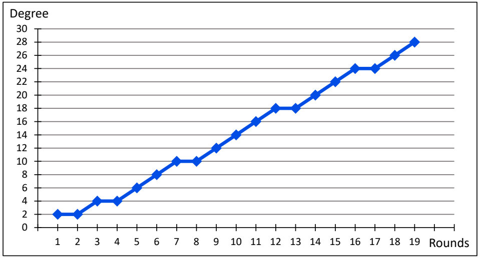
- ⋆ inductive proof: existence of "good" ℓ
- ⋆ MILP solver (`PySCIPOpt`)

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



Plateau

$\Rightarrow$ plateau when $k_r = \lfloor r \log_2 3 \rfloor$ is odd and $k_{r+1} = \lfloor (r+1) \log_2 3 \rfloor$ is even



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

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

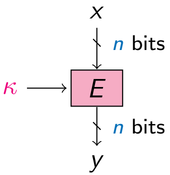
Higher-order differential attack

Exploiting a low algebraic degree

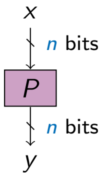
For any affine subspace $\mathcal{V} \subset \mathbb{F}_2^n$ with $\dim \mathcal{V} \geq \deg^a(F) + 1$, we have a 0-sum distinguisher:

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

Random permutation: degree $= n - 1$



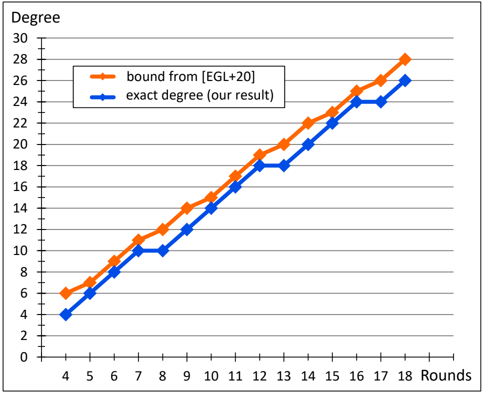
Block cipher



Random permutation

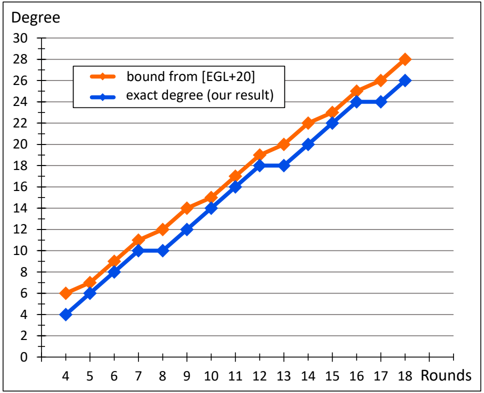
Comparison to previous work

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



For $n = 129$, MIMC$_3$ $= 82$ rounds

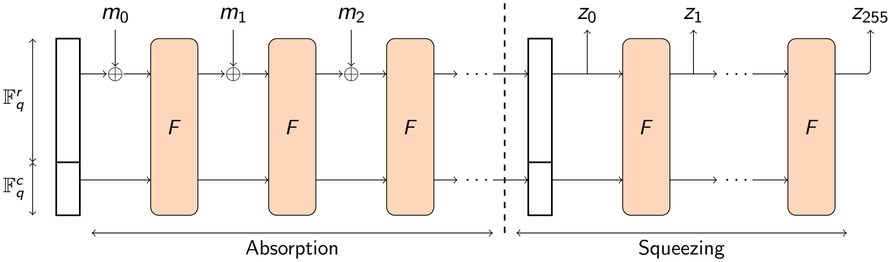
Rounds	Time	Data	Source
80/82	2^{128} XOR	2^{128}	[EGL+20]
81/82	2^{128} XOR	2^{128}	New
80/82	2^{125} XOR	2^{125}	New

Secret-key distinguishers ($n = 129$)

MiMC in a Hash Function

Sponge construction:

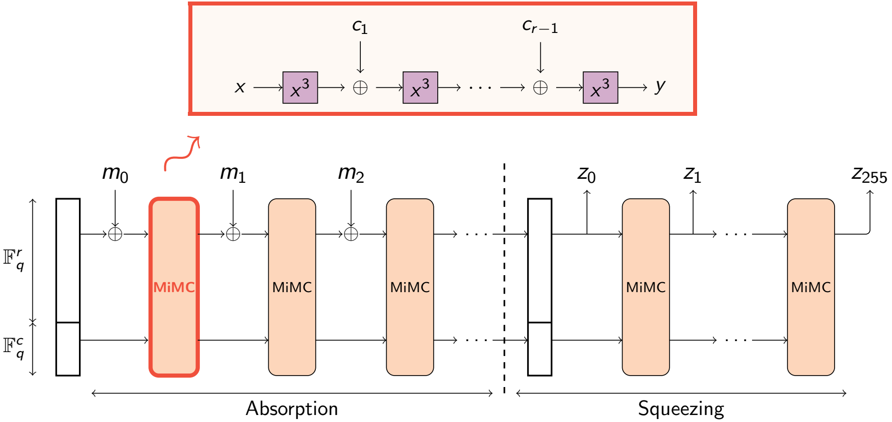
- ⋆ rate $r > 0$
- ⋆ capacity $c > 0$
- ⋆ permutation of $\mathbb{F}_q^r \times \mathbb{F}_q^c$



Hash function in sponge framework.

MiMC in a Hash Function

MiMC-Hash: $MIMC_3$ used as a permutation in a hash function ($\approx$ 90 rounds)



Hash function in sponge framework.

Some values of p

Parameter p given by Elliptic Curves.

Example:

- ⋆ Curve BLS12-381 $\log_2 p = 381$

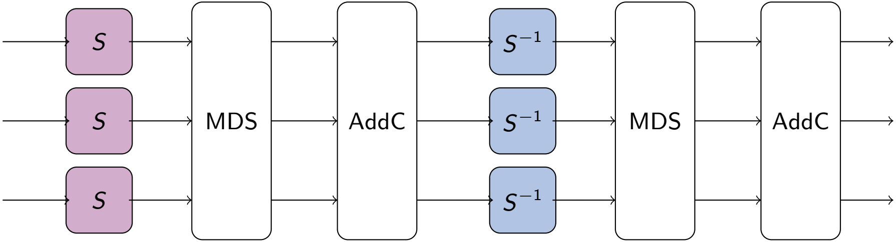
$$p = 4002409555221667393417789825735904156556882819939007885332\\058136124031650490837864442687629129015664037894272559787$$

- ⋆ Curve BLS12-377 $\log_2 p = 377$

$$p = 2586644260129690940106527336948935335363935127549146605398\\842626667204683483408227749688881395733601244403214581 77$$

Rescue

- S-Box layer
- Linear layer
- Constants addition



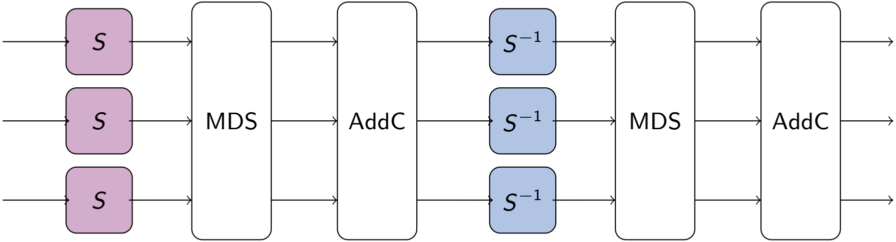
The 2 steps of round i of Rescue.

Rescue

- S-Box layer
- Linear layer
- Constants addition

$S : x \mapsto x^{\alpha}$, and $S^{-1} : x \mapsto x^{1/\alpha}$ $(\alpha = 3)$

$R \approx 10$



The 2 steps of round i of Rescue.

Rescue

- S-Box layer
- Linear layer
- Constants addition

$S : x \mapsto x^{\alpha}$, and $S^{-1} : x \mapsto x^{1/\alpha}$ $(\alpha = 3)$

$R \approx 10$

Curve BLS12−381:

$$p = 4002409555221667393417789825735904156556882819939007885332\\058136124031650490837864442687629129015664037894272559787$$

$$\alpha = 5$$

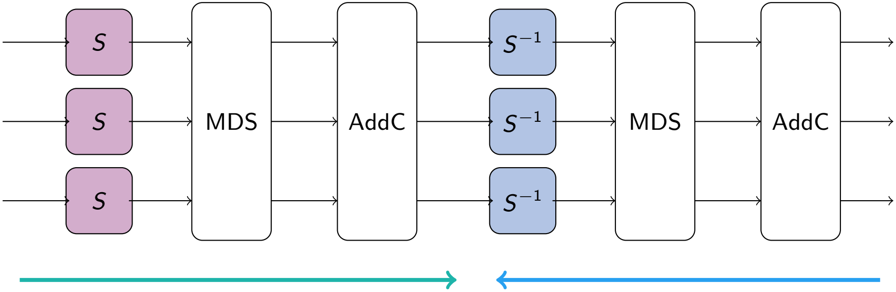
$$\alpha^{-1} = 3201927644177339147342318605887233252455062559512063082656\\4650889922532039267029155415010330321253123031541804782 9$$

Rescue

- S-Box layer
- Linear layer
- Constants addition

$S : x \mapsto x^\alpha$, and $S^{-1} : x \mapsto x^{1/\alpha}$ $(\alpha = 3)$

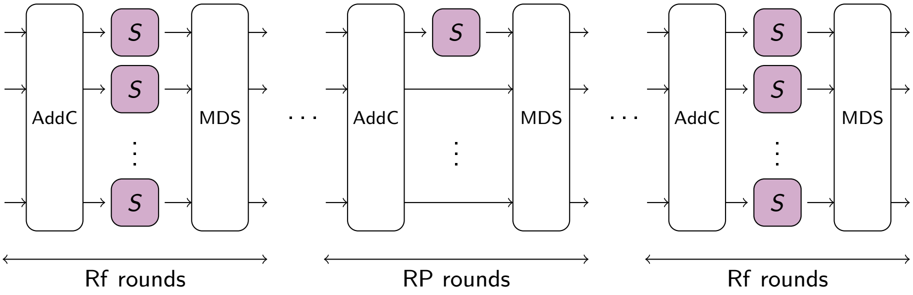
$R \approx 10$



The 2 steps of round i of Rescue.

Poseidon

- S-Box layer
- Linear layer
- Constants addition



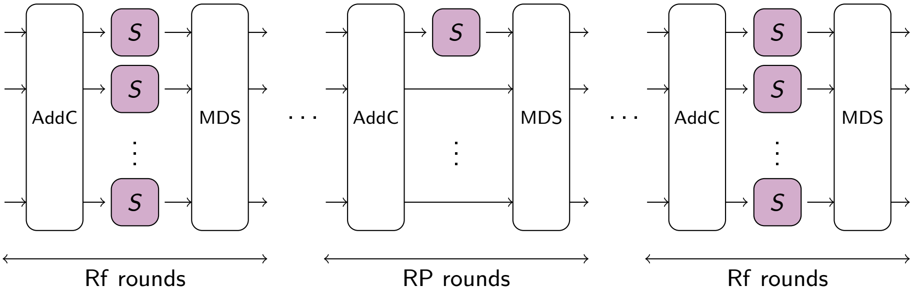
Overview of Poseidon.

Poseidon

- S-Box layer
- Linear layer
- Constants addition

$S : x \mapsto x^{\alpha}$, $(\alpha = 3)$

$R = \text{RF} + \text{RP} \approx 50$



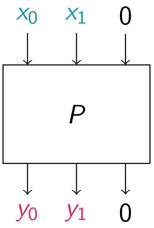
Overview of Poseidon.

CICO Problem

☞ *Bariant, Bouvier, Leurent, Perrin*
Practical Algebraic Attacks against some Arithmetization-oriented Hash Functions

Definition

Constrained Input Constrained Output (CICO) problem:
Find $X, Y \in \mathbb{F}_q^{t-u}$ s.t. $P(X, 0^u) = (Y, 0^u)$.



CICO problem when $t = 3$, $u = 1$.

Trick for SPN

- Solving Univariate systems:

  Find the roots of a polynomial $P \in \mathbb{F}_p[X]$.

Trick for SPN

- Solving Univariate systems:

  Find the roots of a polynomial $P \in \mathbb{F}_p[X]$.

- Solving Multivariate systems:

  From polynomial equations on variables $X_i \in \mathbb{F}_p$:

$$\begin{cases} P_1(X_1, \ldots X_n) = 0 \\ P_2(X_1, \ldots X_n) = 0 \\ \vdots \\ P_n(X_1, \ldots X_n) = 0, \end{cases}$$

  compute a Gröbner basis...

Trick for SPN

- Solving Univariate systems:

  Find the roots of a polynomial $P \in \mathbb{F}_p[X]$.

- Solving Multivariate systems:

  From polynomial equations on variables $X_i \in \mathbb{F}_p$:

$$\begin{cases} P_1(X_1, \dots X_n) = 0 \\ P_2(X_1, \dots X_n) = 0 \\ \vdots \\ P_n(X_1, \dots X_n) = 0, \end{cases}$$

compute a Gröbner basis...

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

Trick for SPN

- Solving Univariate systems:

  Find the roots of a polynomial $P \in \mathbb{F}_p[X]$.

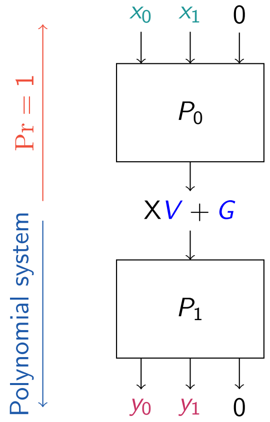
- Solving Multivariate systems:

  From polynomial equations on variables $X_i \in \mathbb{F}_p$:

$$\begin{cases} P_1(X_1, \dots X_n) = 0 \\ P_2(X_1, \dots X_n) = 0 \\ \vdots \\ P_n(X_1, \dots X_n) = 0, \end{cases}$$

  compute a Gröbner basis...

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



A 2-staged trick.

Goals and Principles

Anemoi

Bouvier, Briaud, Chaidos, Perrin, Velichkov

A family of hash functions exploiting the link between arithmetization-friendliness and CCZ-equivalence.

Goals and Principles

Anemoi

Bouvier, Briaud, Chaidos, Perrin, Velichkov

A family of hash functions exploiting the link between arithmetization-friendliness and CCZ-equivalence.

Design goals:

- ⋆ Compatibility with Various Proof Systems.
- ⋆ Different Algorithms for Different Purposes.
- ⋆ Design Consistency.

Goals and Principles

Anemoi
Bouvier, Briaud, Chaidos, Perrin, Velichkov

A family of hash functions exploiting the link between arithmetization-friendliness and CCZ-equivalence.

Design goals:

- ⋆ Compatibility with Various Proof Systems. → not as Reinforced Concrete!
- ⋆ Different Algorithms for Different Purposes.
- ⋆ Design Consistency.

Goals and Principles

Anemoi

Bouvier, Briaud, Chaidos, Perrin, Velichkov

A family of hash functions exploiting the link between arithmetization-friendliness and CCZ-equivalence.

Design goals:

- ⋆ Compatibility with Various Proof Systems. → not as Reinforced Concrete!
- ⋆ Different Algorithms for Different Purposes. → hash function ≠ compression function
- ⋆ Design Consistency.

Goals and Principles

Anemoi

Bouvier, Briaud, Chaidos, Perrin, Velichkov

A family of hash functions exploiting the link between arithmetization-friendliness and CCZ-equivalence.

Design goals:

- ⋆ Compatibility with Various Proof Systems. → not as Reinforced Concrete!
- ⋆ Different Algorithms for Different Purposes. → hash function ≠ compression function
- ⋆ Design Consistency. → same structure for all uses

CCZ-equivalence

Definition

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

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

where $\mathcal{A}$ is an affine permutation.

CCZ-equivalence

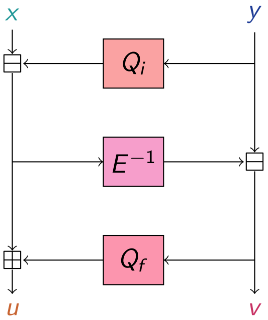
Definition

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

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

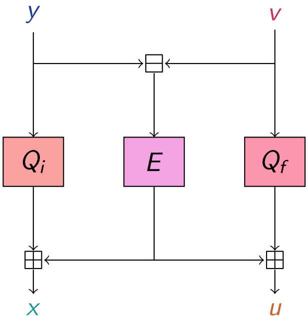
where $\mathcal{A}$ is an affine permutation.

High-degree permutation



Open Flystel $\mathcal{H}$.

Low-degree function



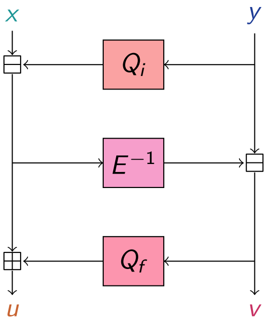
Closed Flystel $\mathcal{V}$.

CCZ-equivalence

$$\Gamma_{\mathcal{H}} = \mathcal{A}(\Gamma_{\mathcal{V}})$$

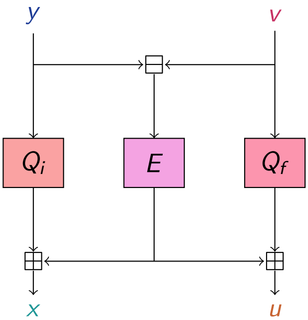
$$\{(x, y), (u, v)\} = \mathcal{A}\left(\{(y, v), (x, u)\}\right)$$

High-degree permutation



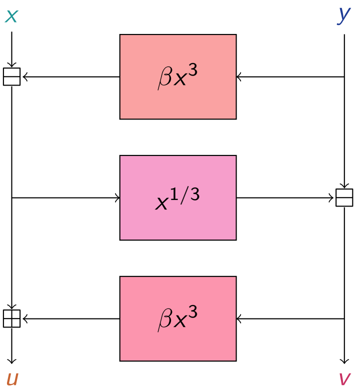
Open Flystel $\mathcal{H}$.

Low-degree function

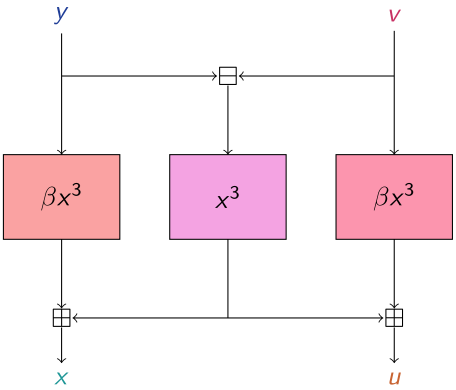


Closed Flystel $\mathcal{V}$.

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

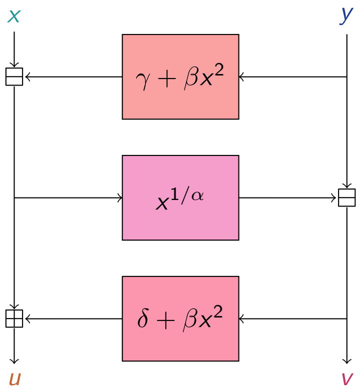


Open Flystel$_2$.

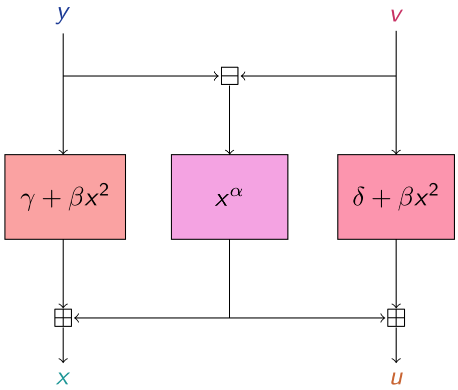


Closed Flystel$_2$.

Flystel in $\mathbb{F}_p$



Open $\texttt{Flystel}_p$.

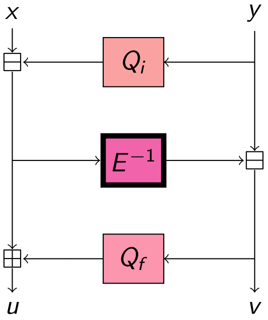


Closed $\texttt{Flystel}_p$.

Advantage of CCZ-equivalence

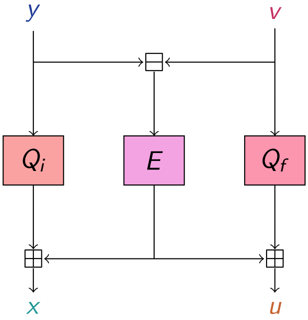
⋆ High Degree Evaluation.

High-degree permutation



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

Low-degree function



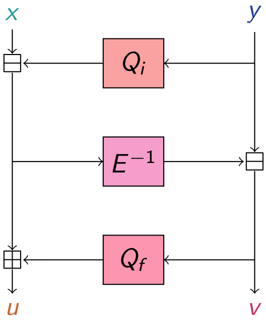
Closed `Flystel` $\mathcal{V}$.

Advantage of CCZ-equivalence

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

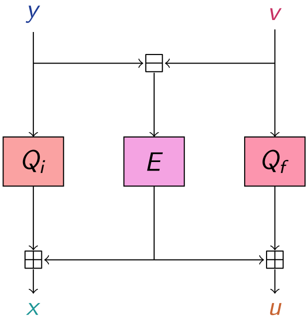
$$(u, v) == \mathcal{H}(x, y) \Leftrightarrow (x, u) == \mathcal{V}(y, v)$$

High-degree permutation



Open Flystel $\mathcal{H}$.

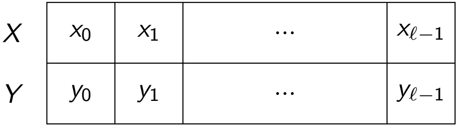
Low-degree function



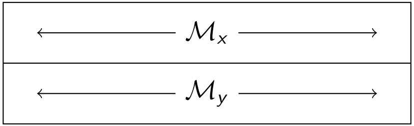
Closed Flystel $\mathcal{V}$.

The SPN Structure

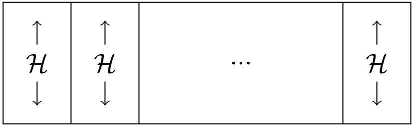
The internal state of `Anemoi` and its basic operations.



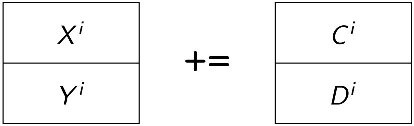
(a) *Internal state*



(b) *The diffusion layer $\mathcal{M}$.*



(c) *The S-box layer $\mathcal{S}$.*



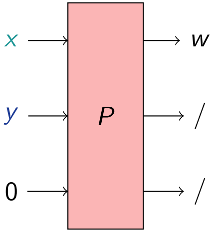
(d) *The constant addition $\mathcal{A}$.*

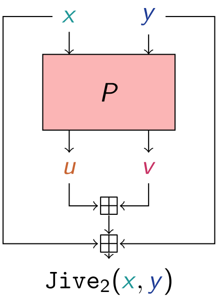
New Mode

- ⋆ Random oracle replacement: `AnemoiRO`
- ⋆ Collision resistant compression function for Merkle-trees: `AnemoiMC`

  Dedicated mode ⇒ 2 words in 1

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





Conclusions

- Algebraic degree of MIMC_3
  - a tight upper bound, up to 16265 rounds:

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

  - minimal complexity for higher-order differential attack

☞ More details on eprint.iacr.org/2022/366

Conclusions

- Algebraic degree of MIMC$_3$
  - a tight upper bound, up to 16265 rounds:

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

  - minimal complexity for higher-order differential attack
- ☞ More details on eprint.iacr.org/2022/366
- Practical attacks against arithmetization-oriented hash functions
- ☞ More details on https://hal.inria.fr/hal-03518757

Conclusions

- Algebraic degree of $MIMC_3$
  - a tight upper bound, up to 16265 rounds:
  $$2 \times \lceil \lfloor \log_2(3^r) \rfloor / 2 - 1 \rceil \ .$$
  - minimal complexity for higher-order differential attack
  - ☞ More details on eprint.iacr.org/2022/366
- Practical attacks against arithmetization-oriented hash functions
  - ☞ More details on https://hal.inria.fr/hal-03518757
- Anemoi
  - a new family of ZK-friendly hash functions
  - contributions of fundamental interest

Conclusions

- Algebraic degree of MIMC_3
  - a tight upper bound, up to 16265 rounds:

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

  - minimal complexity for higher-order differential attack
  - ☞ More details on eprint.iacr.org/2022/366
- Practical attacks against arithmetization-oriented hash functions
  - ☞ More details on https://hal.inria.fr/hal-03518757
- Anemoi
  - a new family of ZK-friendly hash functions
  - contributions of fundamental interest

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

Conclusions

- Algebraic degree of MIMC$_3$
  - a tight upper bound, up to 16265 rounds:

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

  - minimal complexity for higher-order differential attack
  - ☞ More details on eprint.iacr.org/2022/366
- Practical attacks against arithmetization-oriented hash functions
  - ☞ More details on https://hal.inria.fr/hal-03518757
- Anemoi
  - a new family of ZK-friendly hash functions
  - contributions of fundamental interest

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

Thanks for your attention

Sporadic Cases

Bound on ℓ

Observation

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

Let: $k_r = \lfloor r \log_2 3 \rfloor$, $b_r = k_r \bmod 2$ and

$$\mathcal{L}_r = \{\ell,\ 1 \leq \ell < r,\ \text{s.t. } k_{r-\ell} = k_r - k_\ell\}\ .$$

Proposition

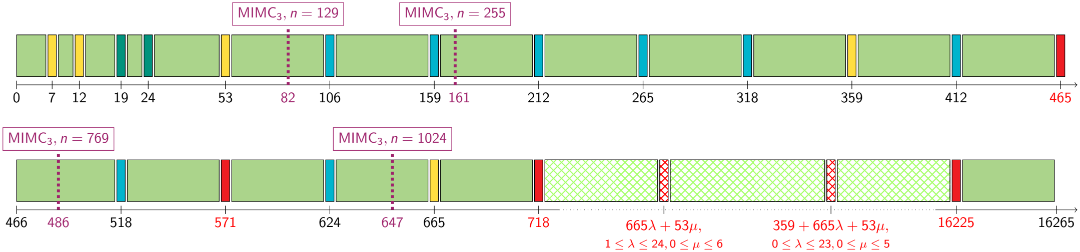
Let $r \geq 4$, and $\ell \in \mathcal{L}_r$ s.t.:

- $\ell = 1, 2$,
- $2 < \ell \leq 22$ s.t. $k_r \geq k_\ell + 3\ell + b_r + 1$, and ℓ is even, or ℓ is odd, with $b_{r-\ell} = \overline{b_r}$;
- $2 < \ell \leq 22$ is odd s.t. $k_r \geq k_\ell + 3\ell + \overline{b_r} + 5$

Then $\omega_{r-\ell} \in \mathcal{E}_{r-\ell}$ implies that $\omega_r \in \mathcal{E}_r$.

Covered Rounds

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



Legend:

Rounds for which we are able to construct an exponent.

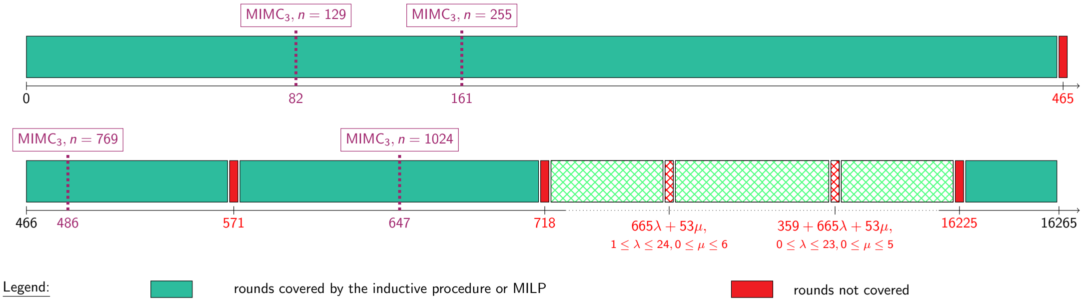
- semiconvergents of $\log_2(3)$: MILP
- "good" ℓ
- no "good" ℓ: MILP
- no "good" ℓ ($\ell \geq 53$): MILP

Rounds likely to be covered by solving the conjecture.

- no "good" ℓ: no result with MILP

Covered Rounds

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



MILP Solver

Let

$$\mathrm{Mult}_3 : \begin{cases} \mathbb{N}^{\mathbb{N}} & \to \mathbb{N}^{\mathbb{N}} \\ \{j_0, \ldots, j_{\ell-1}\} & \mapsto \{(3j_0) \bmod (2^n - 1), \ldots, (3j_{\ell-1}) \bmod (2^n - 1)\} \end{cases},$$

and

$$\mathrm{Cover} : \begin{cases} \mathbb{N}^{\mathbb{N}} & \to \mathbb{N}^{\mathbb{N}} \\ \{j_0, \ldots, j_{\ell-1}\} & \mapsto \{k \preceq j_i, i \in \{0, \ldots, \ell - 1\}\} \end{cases}.$$

So that:

$$\mathcal{E}_r = \mathrm{Mult}_3\big(\mathrm{Cover}(\mathcal{E}_{r-1})\big) .$$

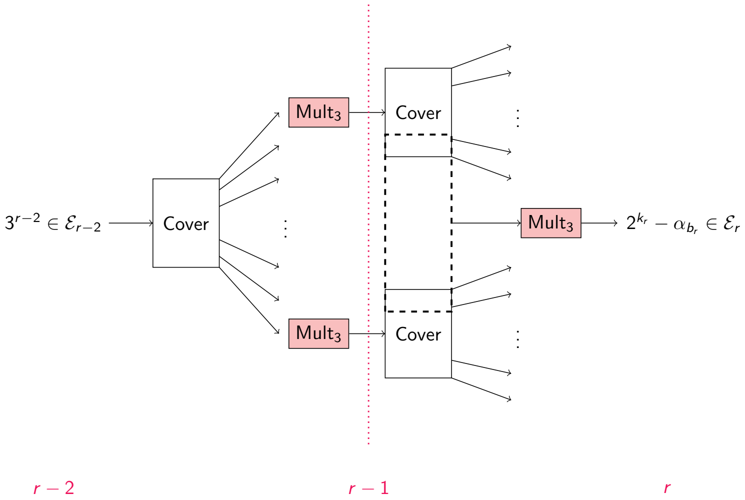
$\Rightarrow$ MILP problem solved using `PySCIPOpt`

$$\boxed{\text{existence of a solution} \quad \Leftrightarrow \quad \omega_r \in (\mathrm{Mult}_3 \circ \mathrm{Cover})^{\ell}(\{3^{r-\ell}\})}$$

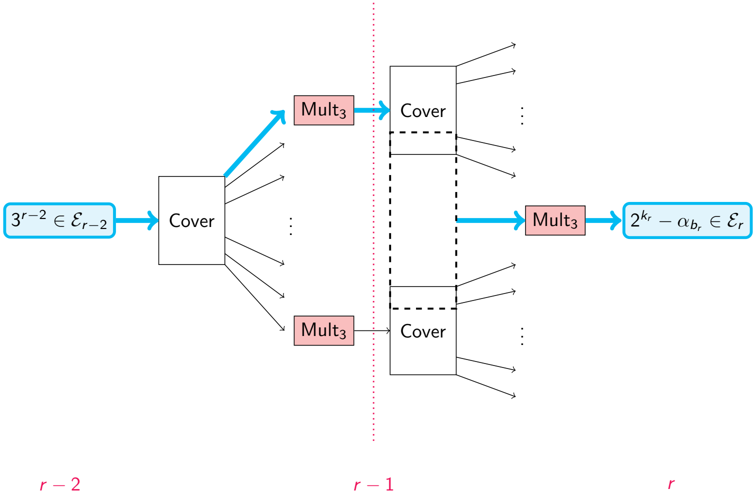
<u>With $\ell = 1$</u>:

$$3^{r-1} \in \mathcal{E}_{r-1} \longrightarrow \boxed{\mathrm{Cover}} \longrightarrow \boxed{\mathrm{Mult}_3} \longrightarrow 2^{k_r} - \alpha_{b_r} \in \mathcal{E}_r$$

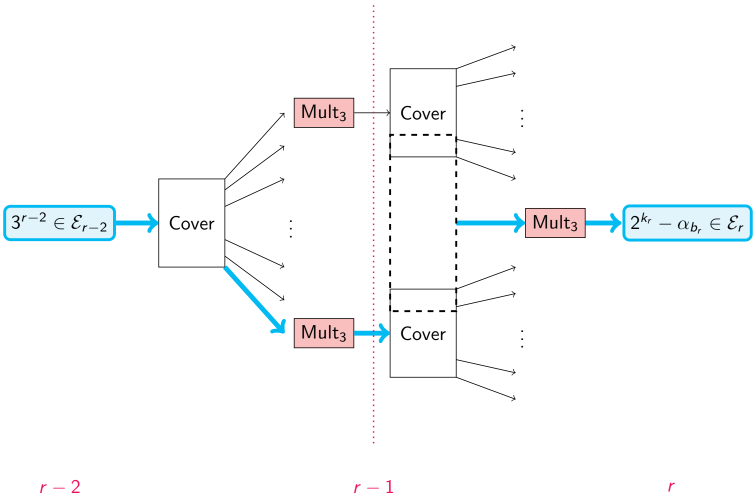
MILP Solver (2 rounds)



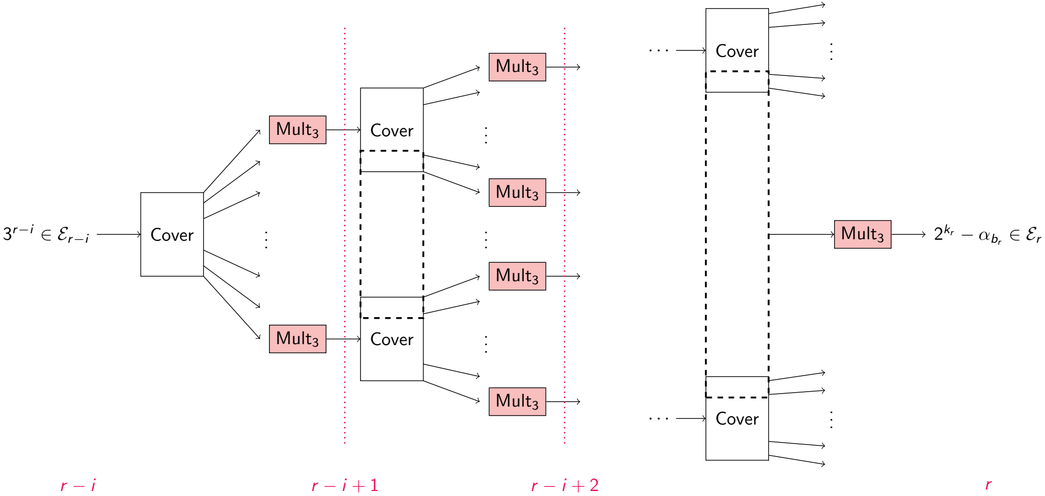
MILP Solver (2 rounds)



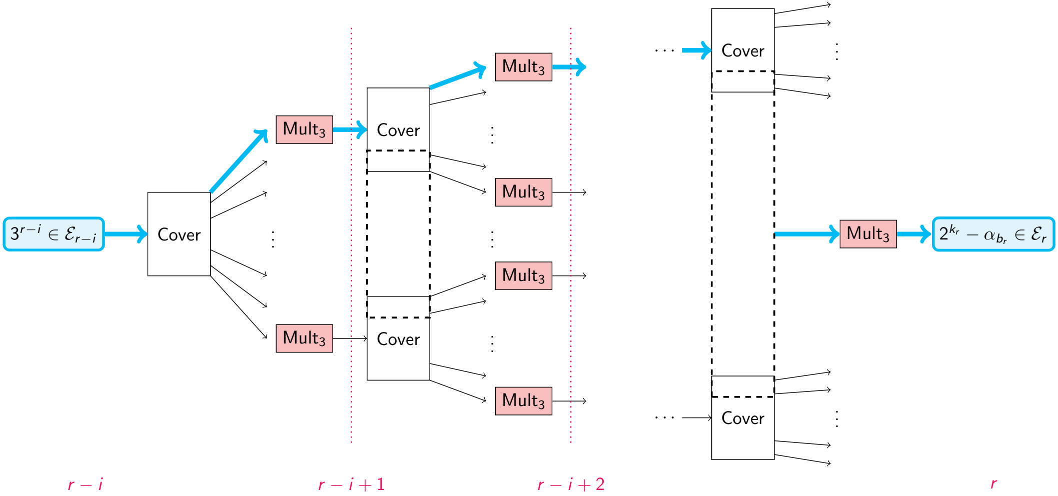
MILP Solver (2 rounds)



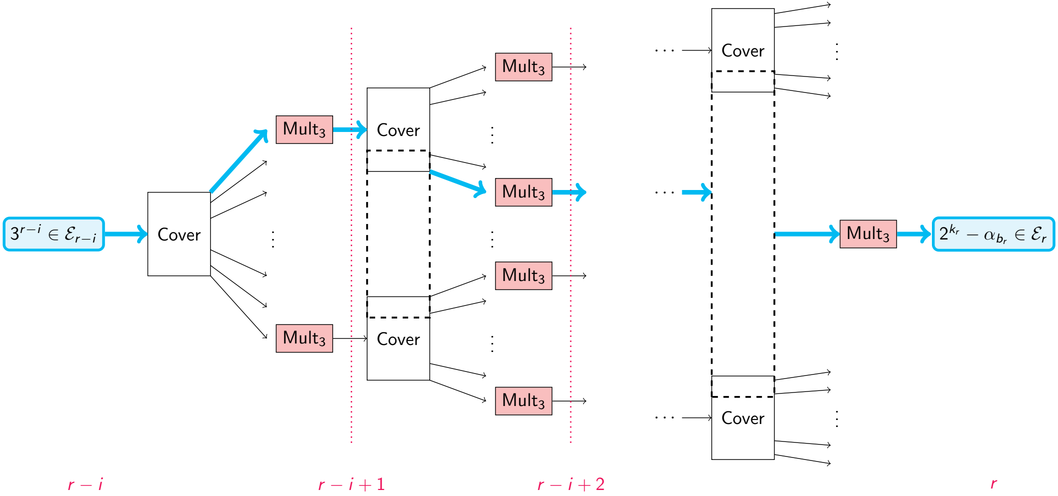
MILP Solver (i rounds)



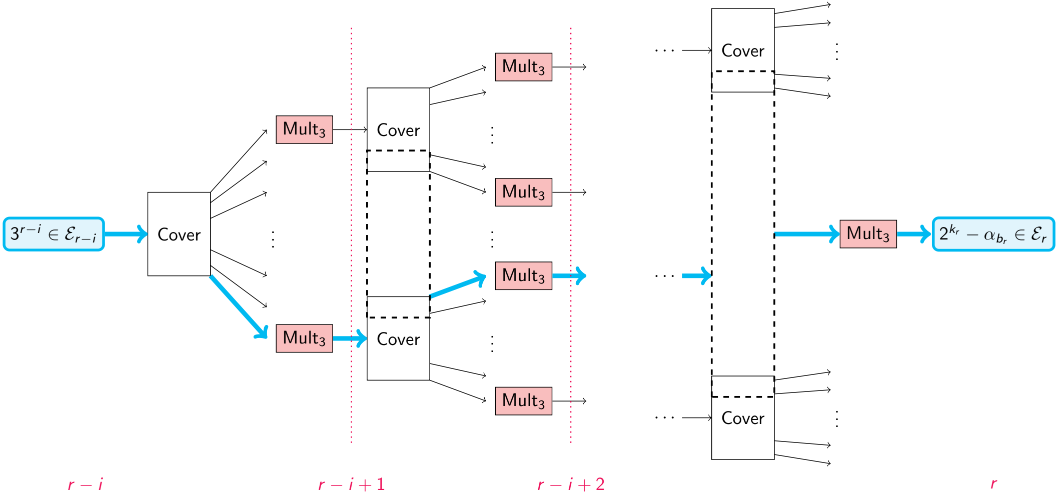
MILP Solver (i rounds)



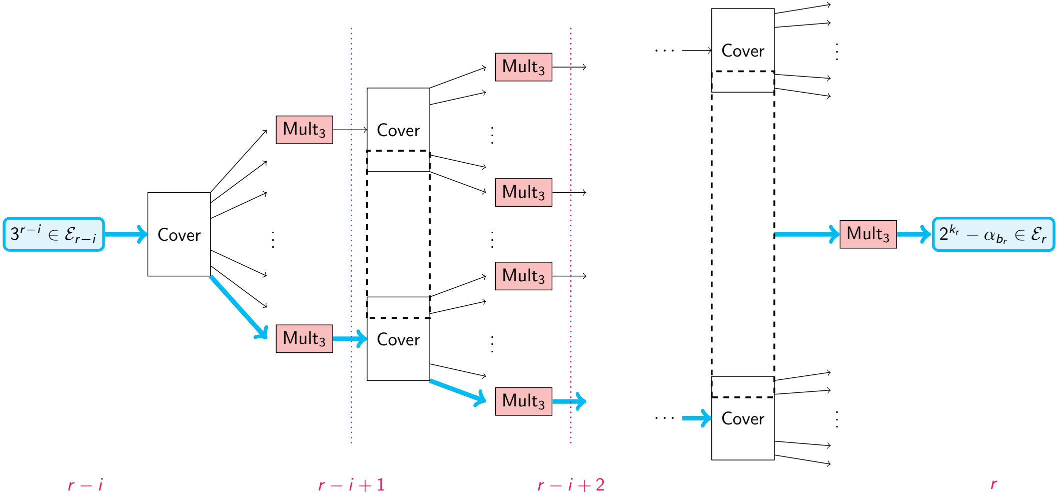
MILP Solver (i rounds)



MILP Solver (i rounds)

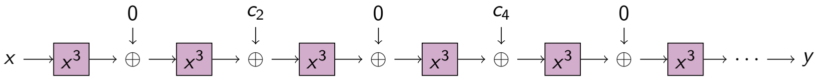


MILP Solver (i rounds)

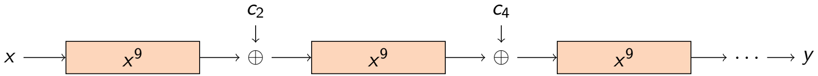


$MiMC_9$ and form of coefficients

- $MIMC_3[2r]$

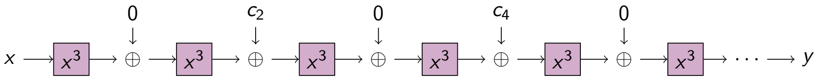


- $MIMC_9[r]$

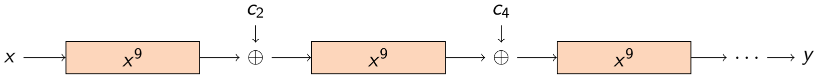


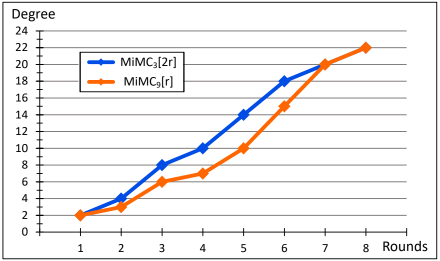
MiMC$_9$ and form of coefficients

- MIMC$_3[2r]$



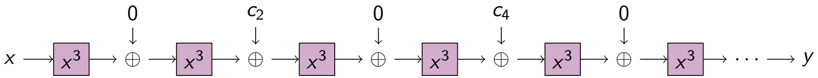
- MIMC$_9[r]$



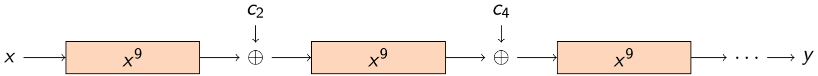


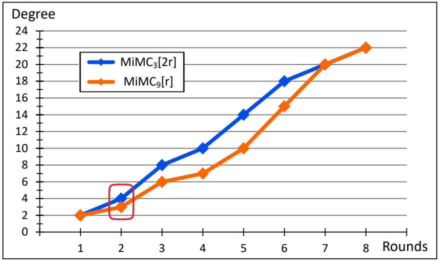
MiMC$_9$ and form of coefficients

- MIMC$_3[2r]$



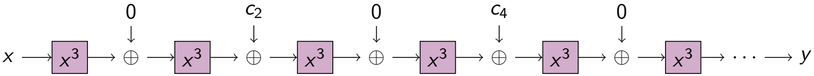
- MIMC$_9[r]$



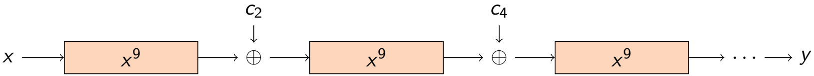


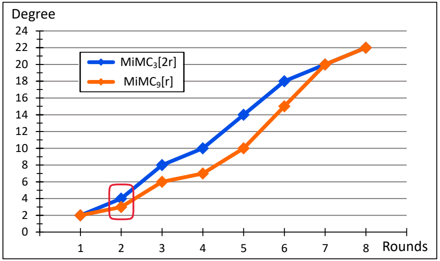
MiMC$_9$ and form of coefficients

- MIMC$_3[2r]$



- MIMC$_9[r]$





Example: coefficients of maximum weight exponent monomials at round 4

$27 : c_1^{18} + c_3^{2}$

$30 : c_1^{17}$

$51 : c_1^{10}$

$54 : c_1^{9} + c_3$

$57 : c_1^{8}$

$75 : c_1^{2}$

$78 : c_1$

Other Quadratic functions

Proposition

Let $\mathcal{E}_r$ be the set of exponents in the univariate form of MIMC$_9[r]$. Then:

$$\forall\, i \in \mathcal{E}_r,\ i \bmod 8 \in \{0, 1\}\ .$$

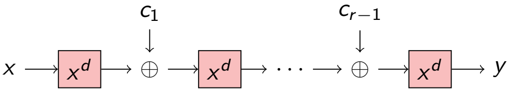
Other Quadratic functions

Proposition

Let $\mathcal{E}_r$ be the set of exponents in the univariate form of MIMC$_9[r]$. Then:

$$\forall\, i \in \mathcal{E}_r,\ i \bmod 8 \in \{0, 1\}\ .$$

Gold Functions: x^3, x^9, ...



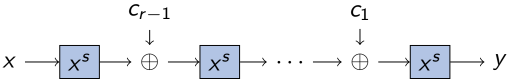
Proposition

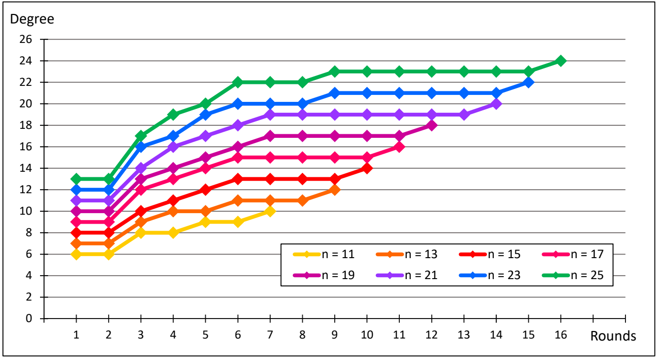
Let $\mathcal{E}_r$ be the set of exponents in the univariate form of MIMC$_d[r]$, where $d = 2^j + 1$. Then:

$$\forall\, i \in \mathcal{E}_r,\ i \bmod 2^j \in \{0, 1\}\ .$$

Algebraic degree of MiMC_3^{-1}

Inverse: $F : x \mapsto x^s, s = (2^{n+1} - 1)/3 = [101..01]_2$





Some ideas studied

Plateau between rounds 1 and 2, for $s = (2^{n+1} - 1)/3 = [101..01]_2$:

- Round 1: $B_s^1 = wt(s) = (n+1)/2$
- Round 2: $B_s^2 = \max\{wt(is), \text{ for } i \preceq s\} = (n+1)/2$

Proposition

For $i \preceq s$ such that $wt(i) \geq 2$:

$$wt(is) \in \begin{cases} [wt(i) - 1, (n-1)/2] & \text{if } \; wt(i) \equiv 2 \bmod 3 \\ [wt(i), (n-1)/2] & \text{if } \; wt(i) \equiv 0 \bmod 3 \\ [wt(i), (n+1)/2] & \text{if } \; wt(i) \equiv 1 \bmod 3 \end{cases}$$

Some ideas studied

Plateau between rounds 1 and 2, for $s = (2^{n+1} - 1)/3 = [101..01]_2$:

- Round 1: $B_s^1 = wt(s) = (n+1)/2$
- Round 2: $B_s^2 = \max\{wt(is), \text{ for } i \preceq s\} = (n+1)/2$

Proposition

For $i \preceq s$ such that $wt(i) \geq 2$:

$$wt(is) \in \begin{cases} [wt(i) - 1, (n-1)/2] & \text{if } \; wt(i) \equiv 2 \bmod 3 \\ [wt(i), (n-1)/2] & \text{if } \; wt(i) \equiv 0 \bmod 3 \\ [wt(i), (n+1)/2] & \text{if } \; wt(i) \equiv 1 \bmod 3 \end{cases}$$

Next rounds: another plateau at $n-2$?

$$\boxed{r_{n-2} \geq \left\lceil \frac{1}{\log_2 3} \left(2 \left\lceil \frac{n-1}{4} \right\rceil + 1\right) \right\rceil}$$