New uses in Symmetric Cryptography:
An equation between Practical needs and Mathematical concepts

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

June 23rd, 2022

SORBONNE UNIVERSITÉ

Inria

Some definitions

Definition

Cryptology: science of secret messages.
Eth. from the Greek kryptós *(hidden) and* lógos *(word).*

$$\text{Cryptology} = \text{Cryptography} + \text{Cryptanalysis}$$

Definition

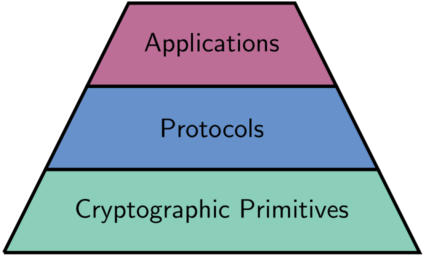
Cryptography: methods used to transform a plaintext in an unintelligible one.

Definition

Cryptanalysis: methods used to recover the plaintext from the ciphertext.

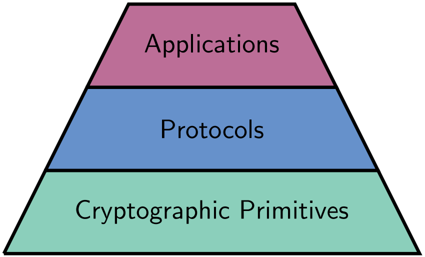
Cryptographic primitives

A primitive is the building block of security



Cryptographic primitives

A primitive is the building block of security



Applications in everyday life!

Example:

- ⋆ Encrypting email communications: PGP
- ⋆ Securing a website: HTTPS
- ⋆ Internet of Things (IoT)
- ⋆ ...

Lifecycle of a primitive

Conception

- ⋆ Specification of the algorithm
- ⋆ Justification of design choices
- ⋆ First security analysis

Publication

Analysis

- ⋆ Trying to break algorithms

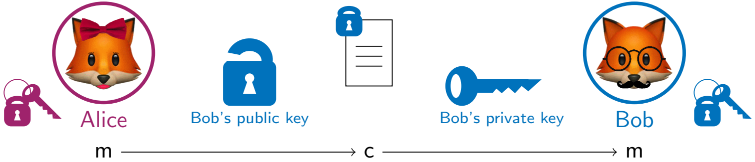
Standardization

Deployment

- ⋆ Implementation of algorithms

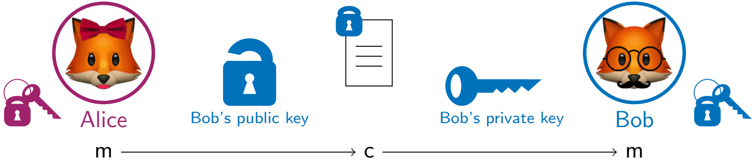
Asymmetric VS Symmetric

⋆ Asymmetric: RSA, Diffie-Hellman, . . .

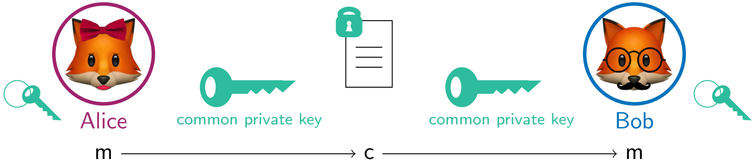


Asymmetric VS Symmetric

⋆ Asymmetric: RSA, Diffie-Hellman, ...



⋆ Symmetric: AES, DES, Triple-DES, ...



Symmetric cryptography

We assume that a key is already shared.

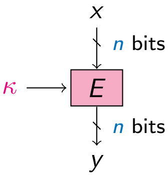
- Stream cipher
- Block cipher

Symmetric cryptography

We assume that a key is already shared.

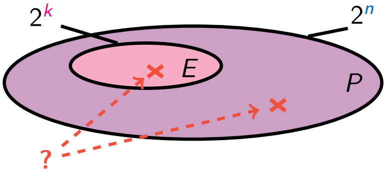
- Stream cipher
- Block cipher

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



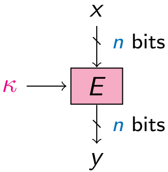
Block cipher

Symmetric cryptography

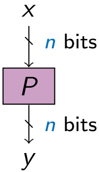


We assume that a key is already shared.

- ⋆ Stream cipher
- ⋆ Block cipher



Block cipher



Random permutation

- ⋆ 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

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

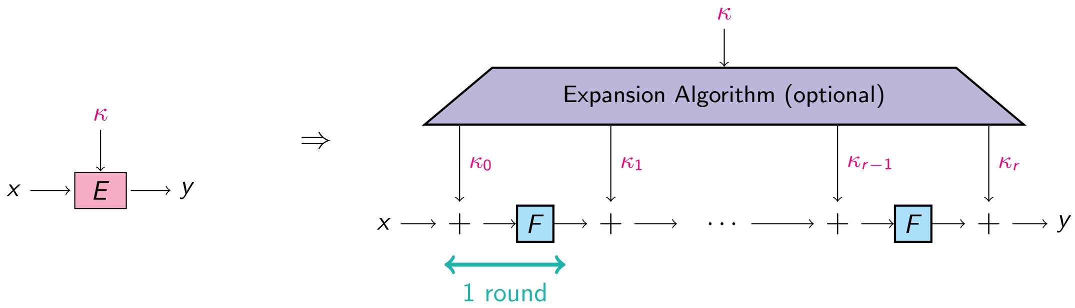
Content

New uses in Symmetric Cryptography:
An equation between Practical needs and Mathematical concepts.

Iterated constructions

$\Rightarrow$ How to build a block cipher?

By iterating a round function.



Performance constraints! The primitive must be fast.

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

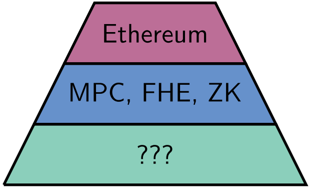
  Example: SNARKs, STARKs, Bulletproofs

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



$\Rightarrow$ 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:
  $$y \leftarrow E(x)$$
- 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

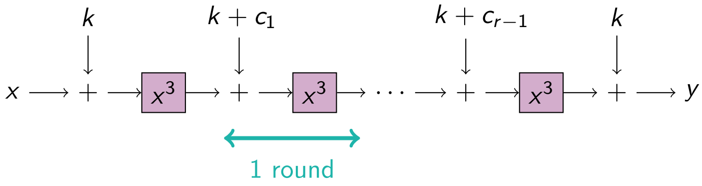
- Operations:
  $$y \leftarrow E(x)$$
- Efficiency:
  implementation in software/hardware

Arithmetization-friendly

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

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 $s = (2^{n+1} - 1)/3$



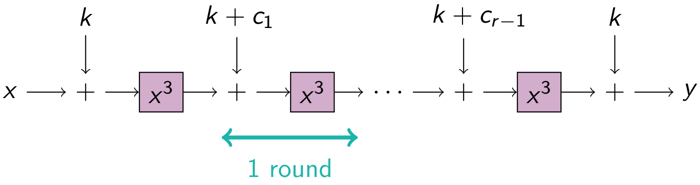
The block cipher MiMC

- 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.



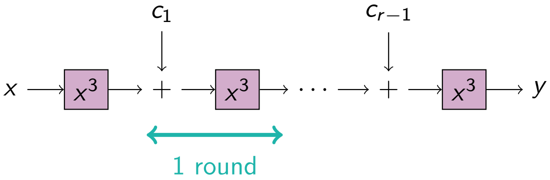
The block cipher MiMC

- 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.



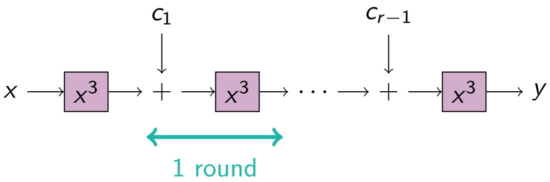
The block cipher MiMC

- 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.



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

Algebraic degree

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

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

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

Definition

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

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

Algebraic degree

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

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

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

Definition

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

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

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

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

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

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

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

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

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

Higher-order differential 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 $= n - 1$

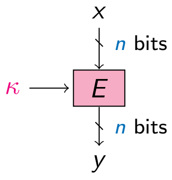
Higher-order differential attack

Exploiting a low algebraic degree

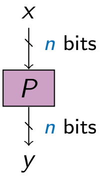
For any affine subspace $\mathcal{V} \subset \mathbb{F}_2^n$ with $\dim \mathcal{V} \geq \deg^a(F) + 1$, we have a 0-sum distinguisher:

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

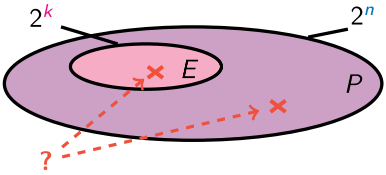
Random permutation: degree $= n - 1$



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

First Plateau

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

For r rounds:

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

⋆ Round 1: $B_3^1 = 2$

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

$$3 = [11]_2$$

First Plateau

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

For r rounds:

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

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

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

Definition

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

⋆ Round 1: $B_3^1 = 2$

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

$$3 = [11]_2$$

⋆ Round 2: $B_3^2 = 2$

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

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

First Plateau

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

For r rounds:

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

Definition

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

⋆ Round 1: $B_3^1 = 2$

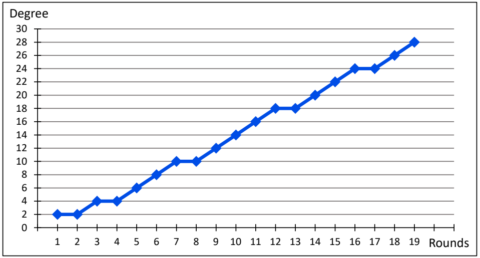
$$\mathcal{P}_1(x) = x^3, \quad (c_0 = 0)$$

$$3 = [11]_2$$

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

⋆ Round 1: $B_3^1 = 2$

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

$$3 = [11]_2$$

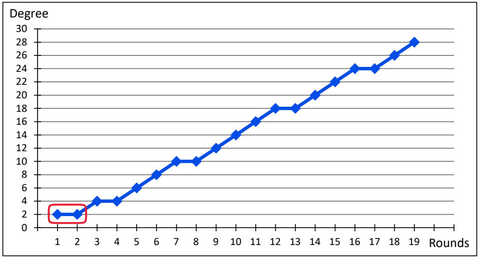
⋆ Round 2: $B_3^2 = 2$

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

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

Definition

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



Algebraic degree observed for $n = 31$.

First Plateau

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

For r rounds:

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

Definition

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

⋆ Round 1: $B_3^1 = 2$

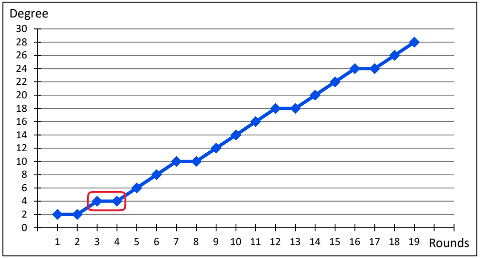
$$\mathcal{P}_1(x) = x^3, \quad (c_0 = 0)$$

$$3 = [11]_2$$

⋆ 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: $B_3^1 = 2$

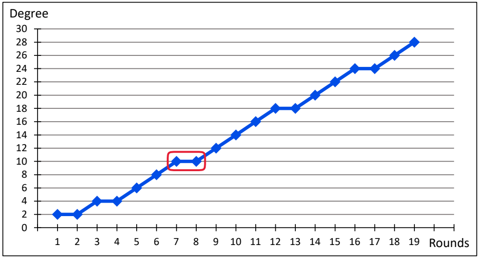
$$\mathcal{P}_1(x) = x^3, \quad (c_0 = 0)$$

$$3 = [11]_2$$

- ⋆ 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 $B_3^r = B_3^{r-1}$.

- ⋆ Round 1: $B_3^1 = 2$

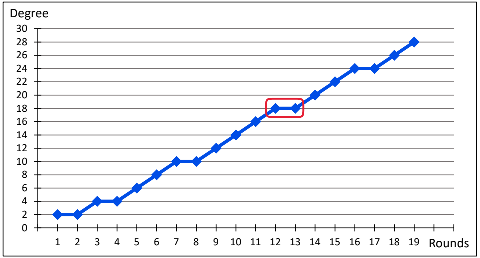
$$\mathcal{P}_1(x) = x^3, \quad (c_0 = 0)$$

$$3 = [11]_2$$

- ⋆ 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: $B_3^1 = 2$

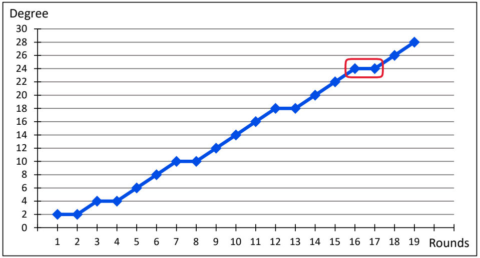
$$\mathcal{P}_1(x) = x^3, \quad (c_0 = 0)$$

$$3 = [11]_2$$

⋆ 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 $n = 31$.

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 $2^{2k} - 1$

$$\mathcal{E}_r \subseteq \{ \begin{array}{cccccccc} 0 & 3 & 6 & 9 & 12 & \cancel{15} & 18 & \cancel{21} \\ 24 & 27 & 30 & 33 & 36 & \cancel{39} & 42 & \cancel{45} \\ 48 & 51 & 54 & 57 & 60 & \cancel{63} & 66 & \cancel{69} \\ \ldots & 3^r\} \end{array}$$

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

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

Bounding the degree

Theorem

After r rounds of MiMC, the algebraic degree is

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

Bounding the degree

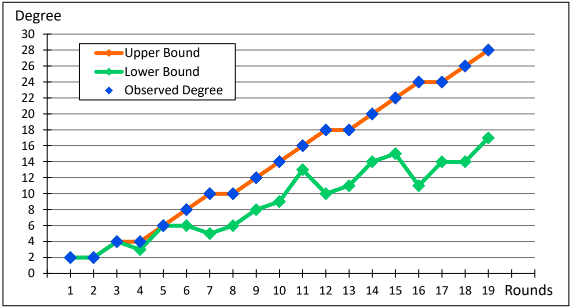
Theorem

After r rounds of MiMC, the algebraic degree is

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

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

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



Exact degree

Maximum-weight exponents:

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

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

- if $k_r = 1 \bmod 2$,

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

- if $k_r = 0 \bmod 2$,

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

Example:

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

Exact degree

Maximum-weight exponents:

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

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

- ⋆ if $k_r = 1 \bmod 2$,

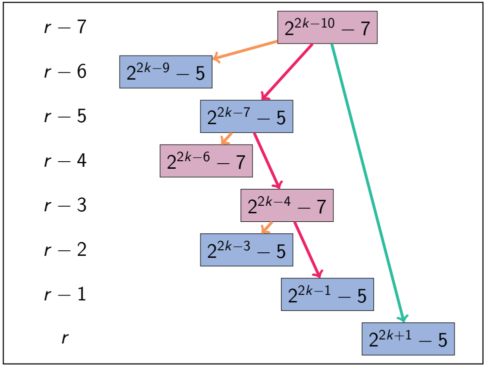
$$\omega_r = 2^{k_r} - 5 \in \mathcal{E}_r,$$

- ⋆ if $k_r = 0 \bmod 2$,

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

Example:

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



Constructing exponents.

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

Exact degree

Maximum-weight exponents:

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

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

- if $k_r = 1 \bmod 2$,

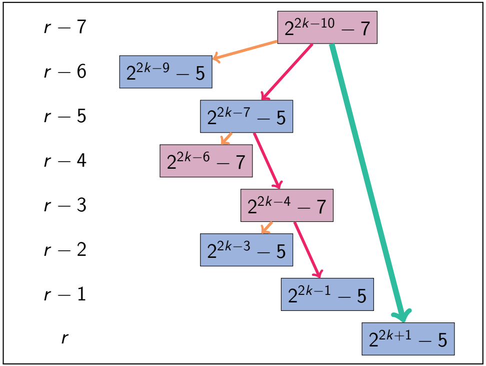
$$\omega_r = 2^{k_r} - 5 \in \mathcal{E}_r,$$

- if $k_r = 0 \bmod 2$,

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

Example:

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



Constructing exponents.

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

Exact degree

Maximum-weight exponents:

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

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

- ⋆ if $k_r = 1 \bmod 2$,

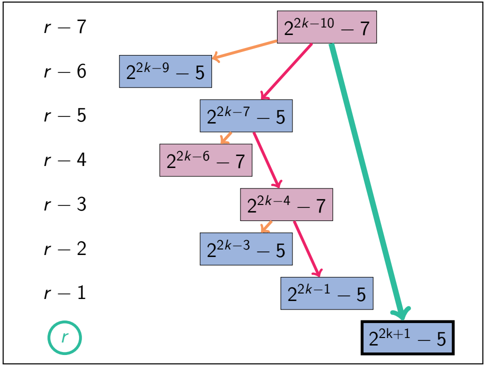
$$\omega_r = 2^{k_r} - 5 \in \mathcal{E}_r,$$

- ⋆ if $k_r = 0 \bmod 2$,

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

Example:

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



Constructing exponents.

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

Exact degree

Maximum-weight exponents:

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

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

- ⋆ if $k_r = 1 \bmod 2$,

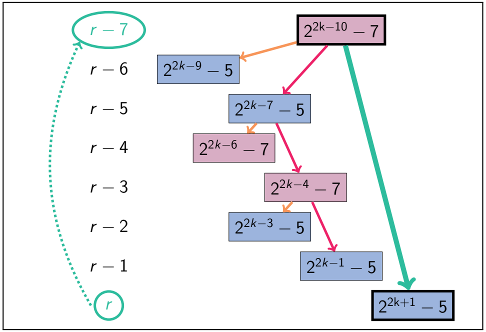
$$\omega_r = 2^{k_r} - 5 \in \mathcal{E}_r,$$

- ⋆ 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.

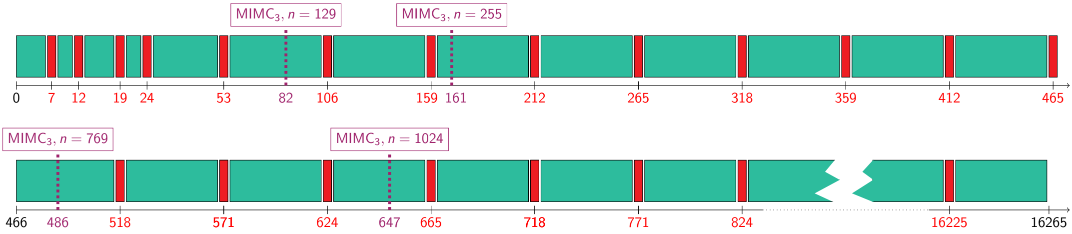
$$\exists\, \ell \text{ s.t. } \quad \omega_{r-\ell} \in \mathcal{E}_{r-\ell} \Rightarrow \omega_r \in \mathcal{E}_r$$

Covered rounds

Idea of the proof:

⋆ inductive proof: existence of "good" ℓ

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



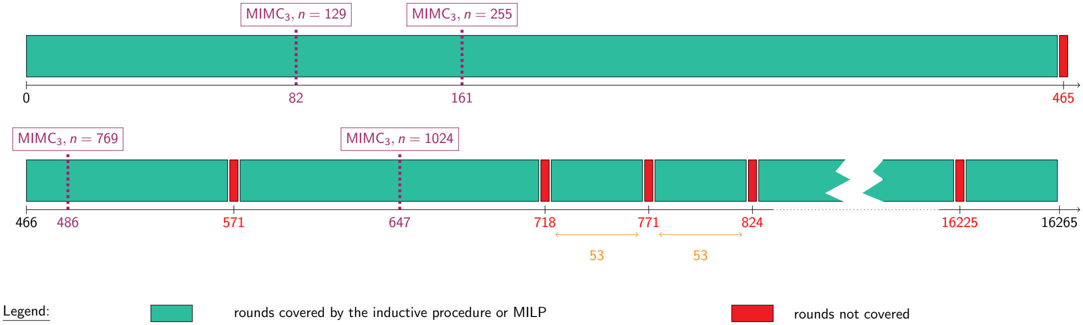
Legend: rounds covered by the inductive procedure; rounds not covered

Covered rounds

Idea of the proof:

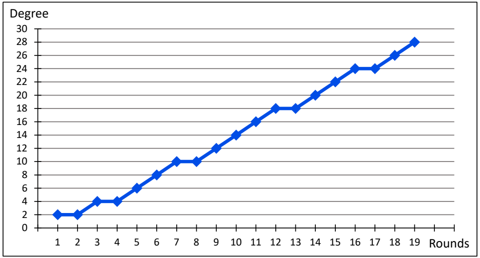
- ⋆ inductive proof: existence of "good" ℓ
- ⋆ MILP solver (`PySCIPOpt`)

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

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

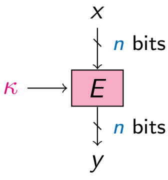
Higher-order differential attack

Exploiting a low algebraic degree

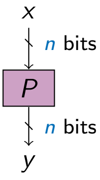
For any affine subspace $\mathcal{V} \subset \mathbb{F}_2^n$ with $\dim \mathcal{V} \geq \deg^a(F) + 1$, we have a 0-sum distinguisher:

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

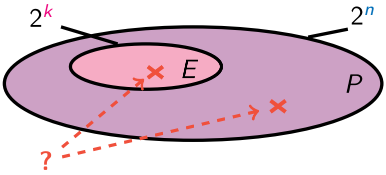
Random permutation: degree $= n - 1$



Block cipher

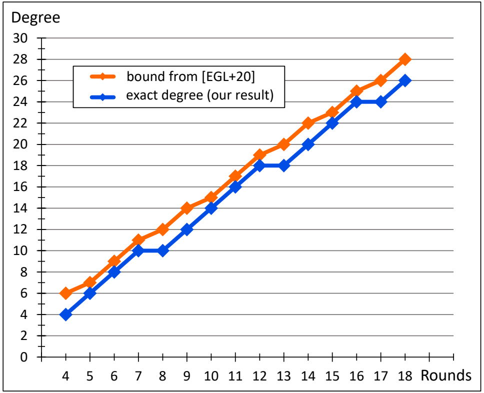


Random permutation



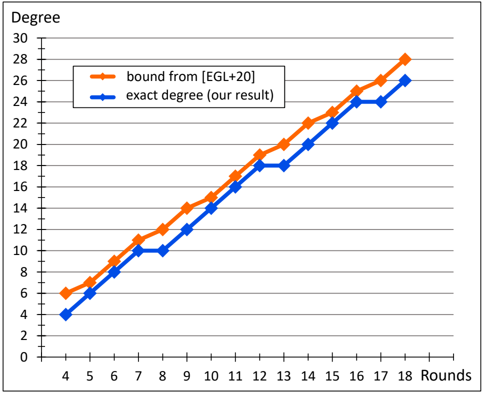
Comparison to previous work

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

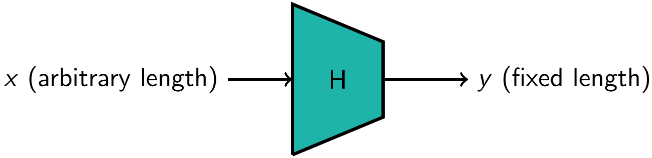
Rounds	Time	Data	Source
80/82	2^{128}XOR	2^{128}	[EGL+20]
81/82	2^{128}XOR	2^{128}	New
80/82	2^{125}XOR	2^{125}	New

Secret-key distinguishers ($n = 129$)

Hash Functions

Definition

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



- ⋆ Preimage resistance: Given y it must be *infeasible* to find x s.t.

$$H(x) = y \ .$$

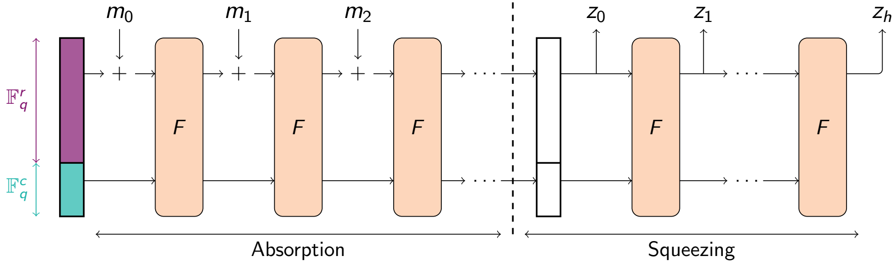
- ⋆ Collision resistance: It must be *infeasible* to find $x \neq x'$ s.t.

$$H(x) = H(x') \ .$$

Sponge construction

Parameters:

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



Hash function in sponge framework.

Some values of p

Parameter p given by Standardized Elliptic Curves.

Example:

- ⋆ Curve BLS12-381 $\log_2 p = 381$

$$p = 4002409555221667393417789825735904156556882819939007885332 \\ 058136124031650490837864442687629129015664037894272559787$$

- ⋆ Curve BLS12-377 $\log_2 p = 377$

$$p = 2586644260129690940106527336948935335363935127549146605398 \\ 842626667204683483408227749688881395733601244403214581 77$$

Substitution-Permutation Network (SPN)

- S-Box layer → Confusion

  Example:

$$\begin{pmatrix} x_0 & x_1 & \dots & x_{m-1} \end{pmatrix} \mapsto \begin{pmatrix} x_0^d & x_1^d & \dots & x_{m-1}^d \end{pmatrix}.$$

- Linear layer → Diffusion

  Example:

$$\begin{pmatrix} x_0 & x_1 & \dots & x_{m-1} \end{pmatrix} \mapsto \begin{pmatrix} x_0 & x_1 & \dots & x_{m-1} \end{pmatrix} \times M.$$

- Constants addition

  Example:

$$\begin{pmatrix} x_0 & x_1 & \dots & x_{m-1} \end{pmatrix} \mapsto \begin{pmatrix} x_0 & x_1 & \dots & x_{m-1} \end{pmatrix} + \begin{pmatrix} c_0 & c_1 & \dots & c_{m-1} \end{pmatrix}.$$

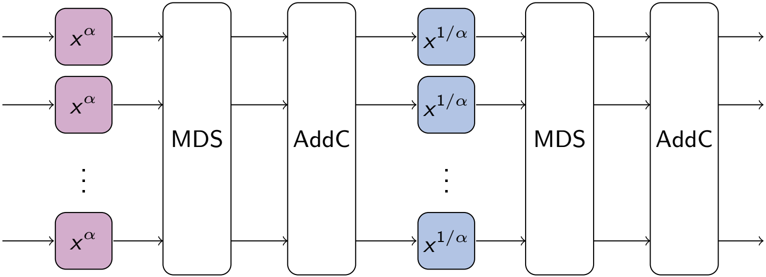
Rescue

[Aly et al., ToSC20]

- S-Box layer
- Linear layer: MDS
- Round constants addition: AddC

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

$R \approx 10$



The 2 steps of round i of Rescue.

Rescue

[Aly et al., ToSC20]

- S-Box layer
- Linear layer: MDS
- Round constants addition: AddC

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

$R \approx 10$

Curve BLS12-381:

$$p = 4002409555221667393417789825735904156556882819939007885332 \\ 058136124031650490837864442687629129015664037894272559787$$

$$\alpha = 5$$

$$\alpha^{-1} = 3201927644177333914734231860588723325245506255951206308265 \\ 646508899225320392670291554150103303212531230315418047829$$

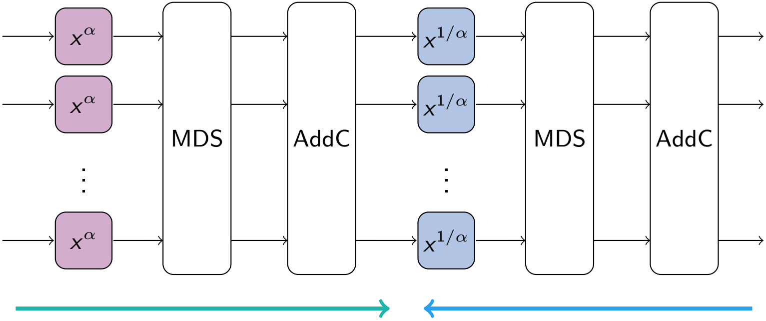
Rescue

[Aly et al., ToSC20]

- S-Box layer
- Linear layer: MDS
- Round constants addition: AddC

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

$R \approx 10$



The 2 steps of round i of Rescue.

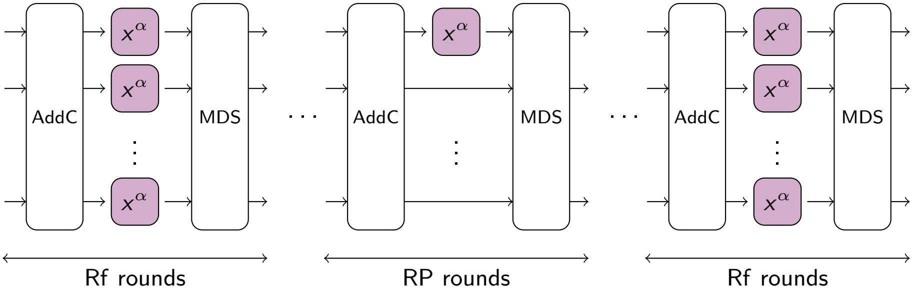
Poseidon

[Grassi et al., USENIX21]

- S-Box layer
- Linear layer: MDS
- Round constants addition: AddC

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

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



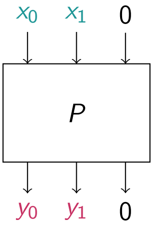
Overview of Poseidon.

Ethereum Challenges

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

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

Tricks for SPN

⋆ Solving Univariate systems:

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

Tricks 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 $X_i \in \mathbb{F}_p$:

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

compute a Gröbner basis...

Tricks 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!**

Tricks for SPN

⋆ Solving Univariate systems:

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

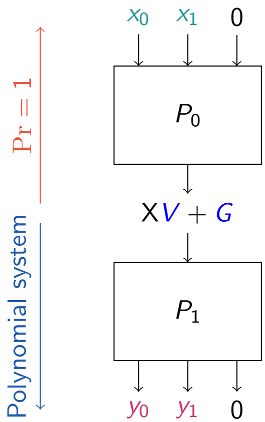
⋆ Solving Multivariate systems:

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...

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



A 2-staged trick.

Consequence for the Challenge

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*

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

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.
- ⋆ Low number of multiplications
- ⋆ Fast and secure

CCZ-equivalence

Definition

$F : \mathbb{F}_q \rightarrow \mathbb{F}_q$ and $G : \mathbb{F}_q \rightarrow \mathbb{F}_q$ 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

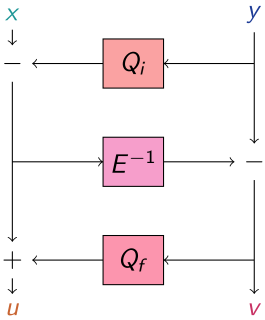
Definition

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

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

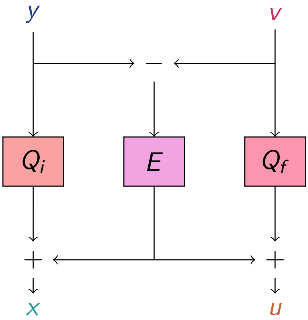
where $\mathcal{A}$ is an affine permutation.

High-degree permutation



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

Low-degree function



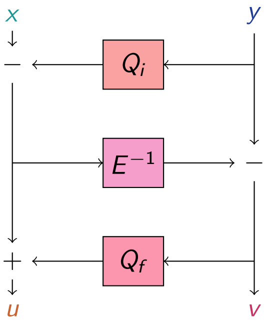
Closed `Flystel` $\mathcal{V}$.

CCZ-equivalence

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

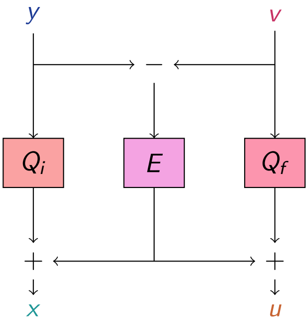
$$\{(x, y), (u, v)\} = \mathcal{A}(\{(y, v), (x, u)\})$$

High-degree permutation



Open Flystel $\mathcal{H}$.

Low-degree function

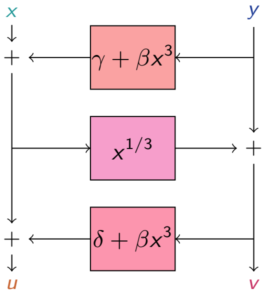


Closed Flystel $\mathcal{V}$.

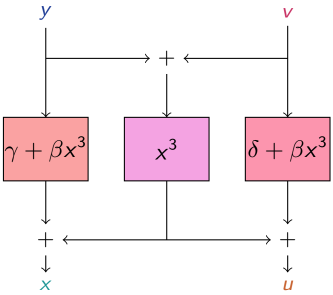
Flystel in $\mathbb{F}_{2^n}$

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

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



Open Flystel$_2$.

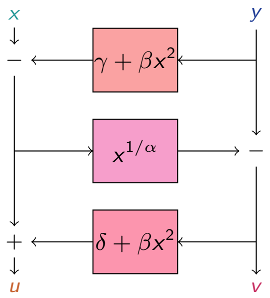


Closed Flystel$_2$.

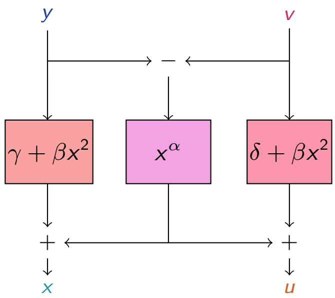
Flystel in $\mathbb{F}_p$

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

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



Open Flystel$_p$.

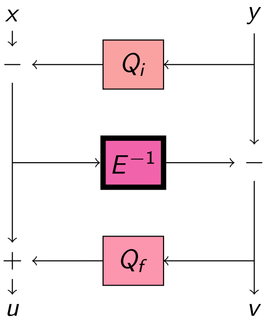


Closed Flystel$_p$.

Advantage of CCZ-equivalence

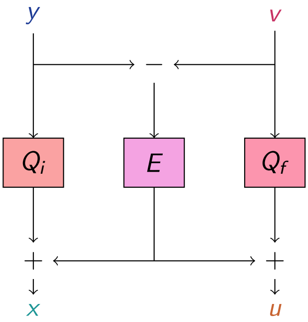
⋆ High Degree Evaluation.

High-degree permutation



Open Flystel $\mathcal{H}$.

Low-degree function



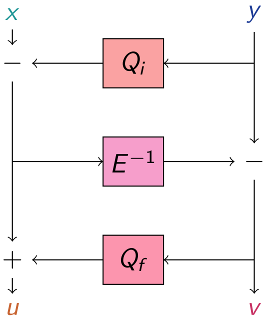
Closed Flystel $\mathcal{V}$.

Advantage of CCZ-equivalence

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

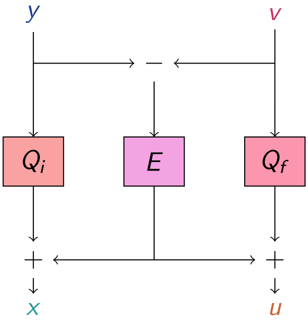
$$(u, v) == \mathcal{H}(x, y) \Leftrightarrow (x, u) == \mathcal{V}(y, v)$$

High-degree permutation



Open Flystel $\mathcal{H}$.

Low-degree function



Closed Flystel $\mathcal{V}$.

The SPN Structure

Let

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

The internal state of `Anemoi` can be represented as:

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

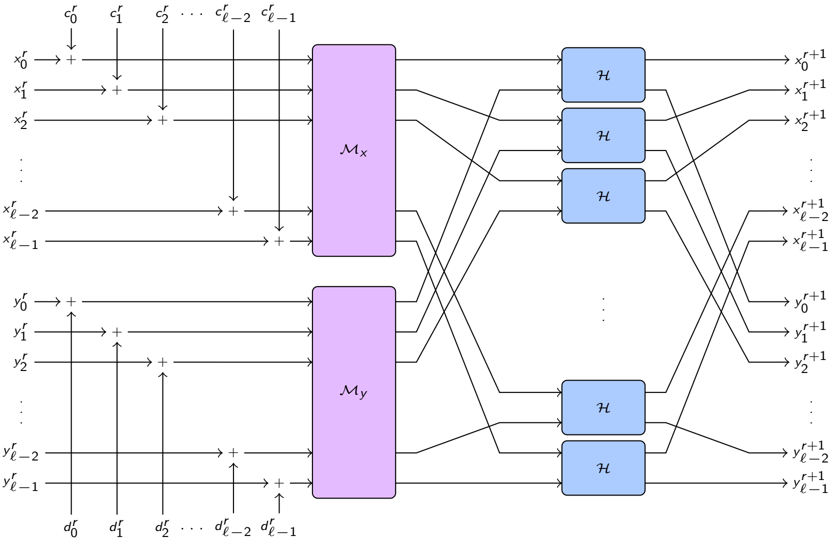
Addition of constants and the linear layer as:

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

And the S-Box layer as:

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

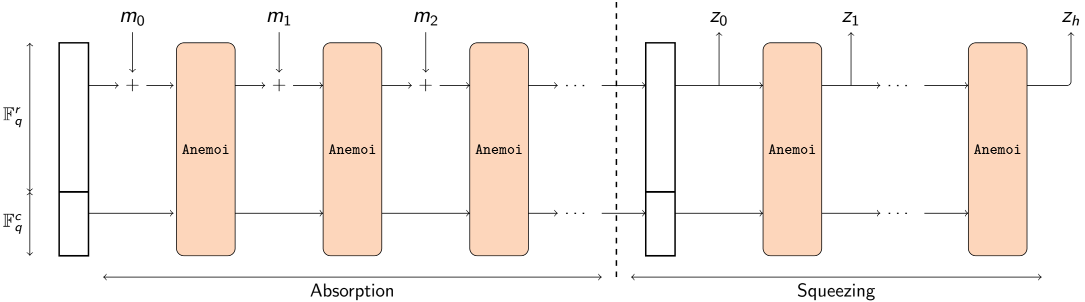
The SPN Structure



Overview of `Anemoi`*.*

New Mode

- Hash function:
  - input: arbitrary length
  - ouput: fixed length

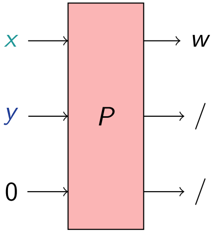


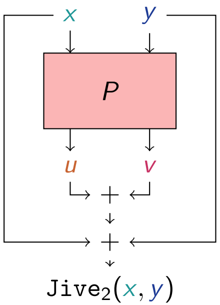
New Mode

- Hash function:
  - input: arbitrary length
  - ouput: fixed length
- Compression function:
  - input: fixed length
  - output: length 1

Dedicated mode $\Rightarrow$ 2 words in 1

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





Comparison to previous work

s	$\log_2 q$	m	Rescue	Poseidon	Anemoi
128	192	8	384	363	**200**
	256	6	288	315	**150**
	384	4	216	264	**120**
256	192	8	432	450	**280**
	256	6	432	495	**225**
	384	4	432	444	**200**

(a) *for R1CS.*

s	$\log_2 q$	m	Rescue	Poseidon	Anemoi
128	192	8	1280	4003	**560**
	256	6	768	2265	**360**
	384	4	432	1032	**240**
256	192	8	1440	5714	**784**
	256	6	1152	4245	**540**
	384	4	864	1932	**784**

(b) *for Plonk.*

Number of constraints for Rescue, Poseidon and Anemoi when $\alpha = 5$.

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
and to appear in *Designs, Codes and Cryptography*

Conclusions

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

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

- 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
and to appear in *Designs, Codes and Cryptography*

- 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
  - new observations of fundamental interest

Open Problem

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

And the opinion of mathematicians would be of great help to us!

Open Problem

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

And the opinion of mathematicians would be of great help to us!

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?

Open Problem

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

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?

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

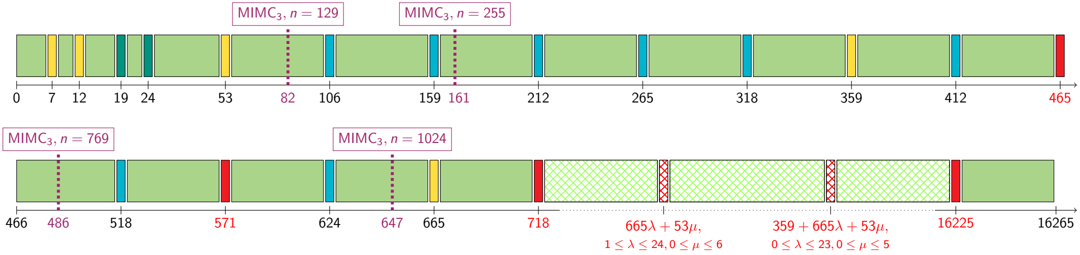
Let $r \geq 4$, and $\ell \in \mathcal{L}_r$ s.t.:

- $\ell = 1, 2,$
- $2 < \ell \leq 22$ 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.

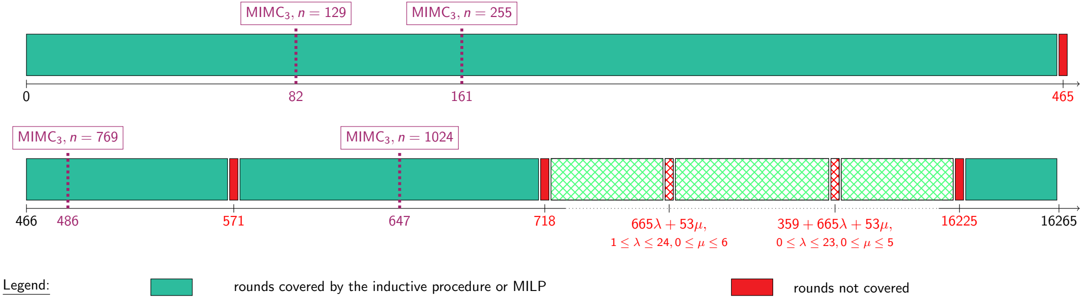
- semiconvergents of $\log_2(3)$: MILP
- "good" ℓ
- no "good" ℓ: MILP
- no "good" ℓ ($\ell \geq 53$): MILP

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

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

and

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

So that:

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

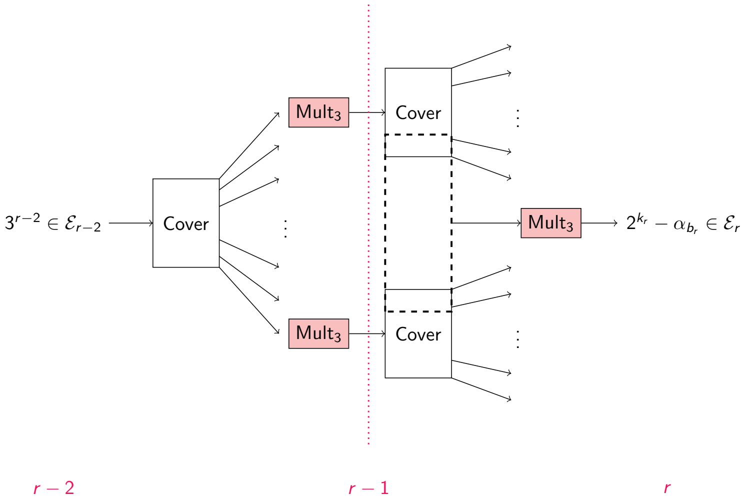
$\Rightarrow$ MILP problem solved using PySCIPOpt

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

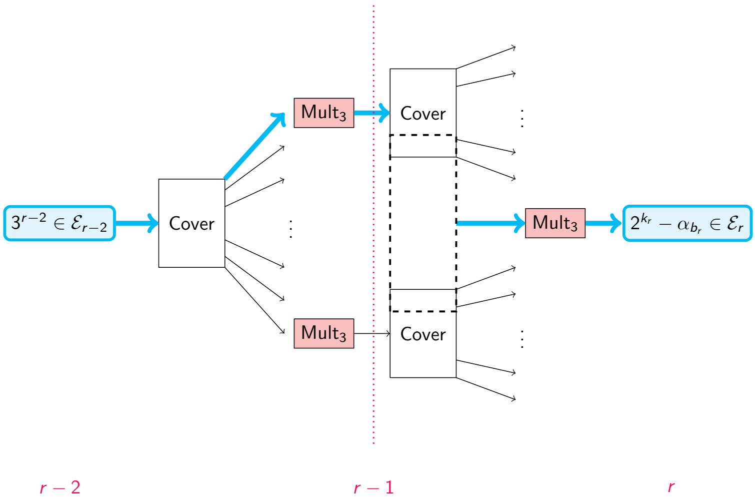
With $\ell = 1$:

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

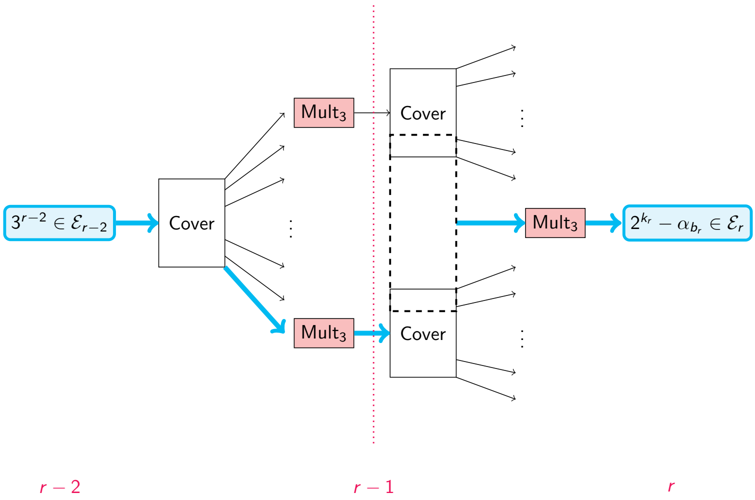
MILP Solver (2 rounds)



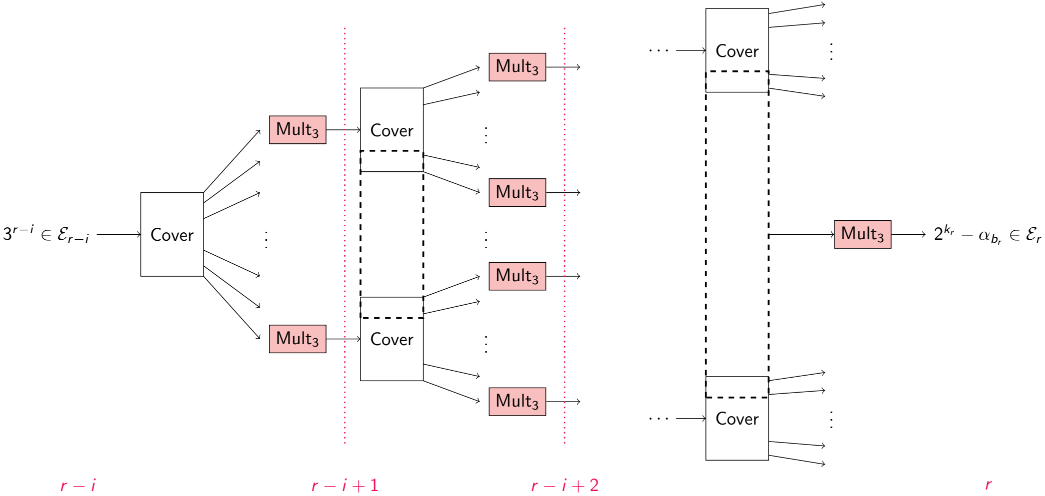
MILP Solver (2 rounds)



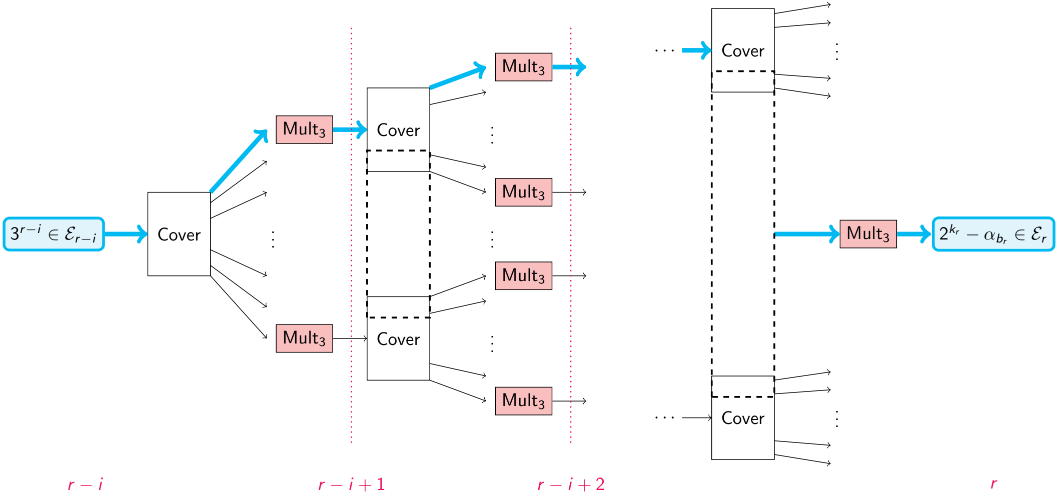
MILP Solver (2 rounds)



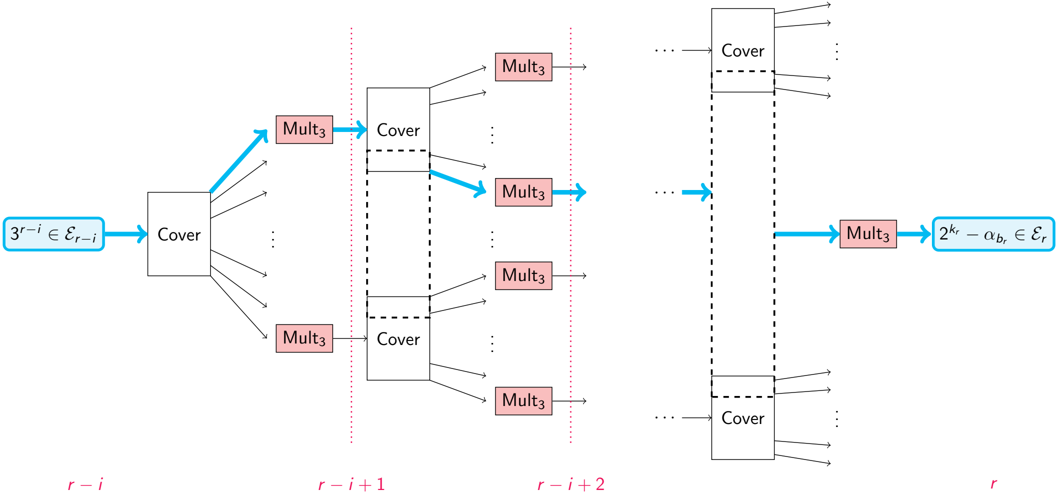
MILP Solver (i rounds)



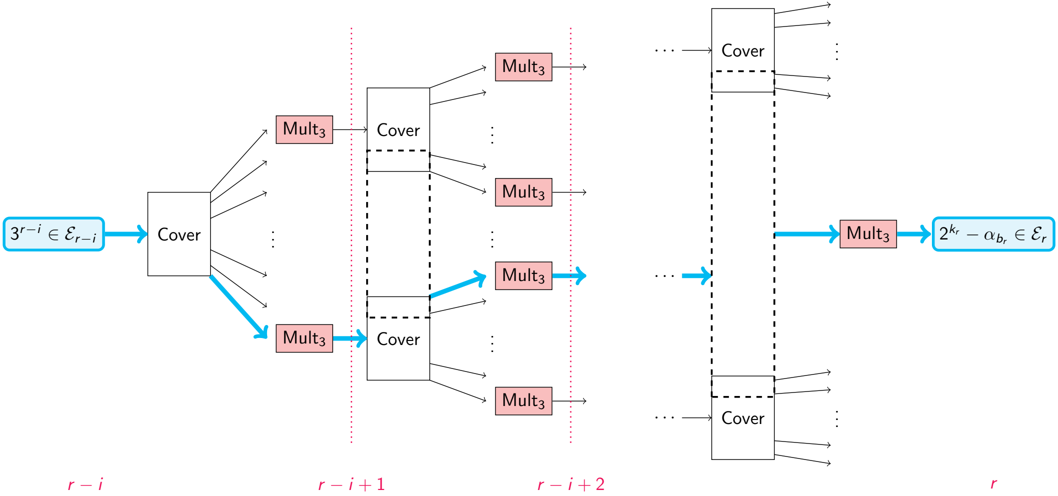
MILP Solver (i rounds)



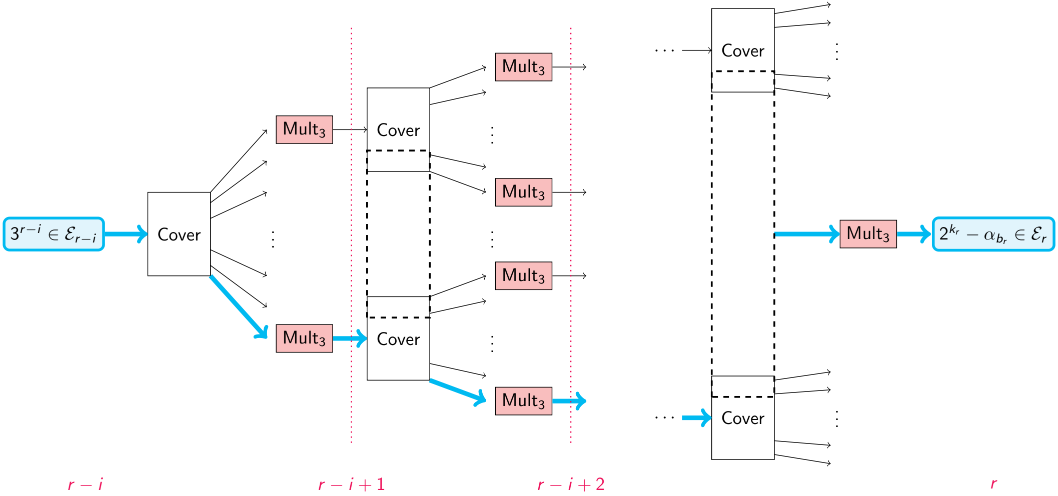
MILP Solver (i rounds)



MILP Solver (i rounds)

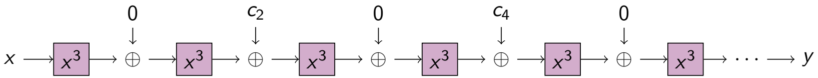


MILP Solver (i rounds)

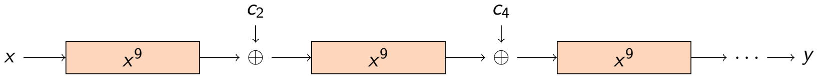


$MiMC_9$ and form of coefficients

- $MIMC_3[2r]$

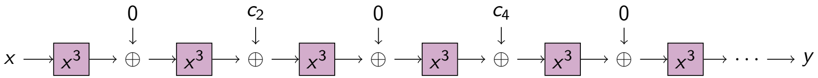


- $MIMC_9[r]$

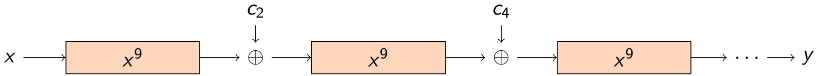


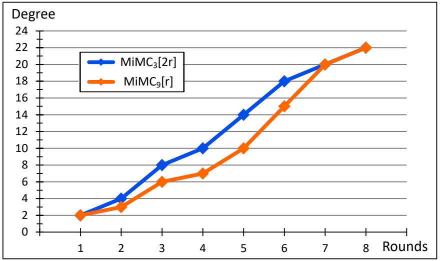
$MiMC_9$ and form of coefficients

- $MIMC_3[2r]$



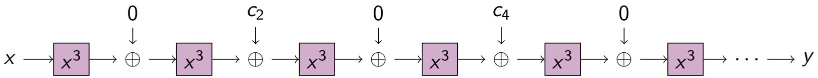
- $MIMC_9[r]$



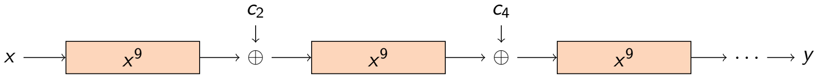


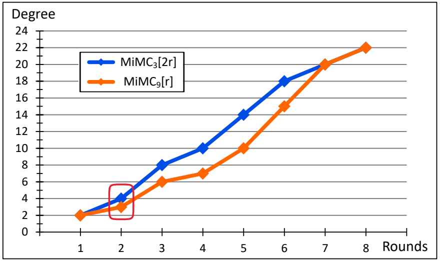
MiMC_9 and form of coefficients

- $\text{MIMC}_3[2r]$



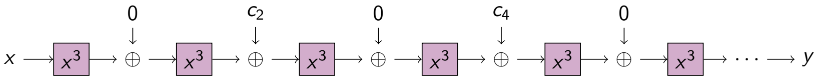
- $\text{MIMC}_9[r]$



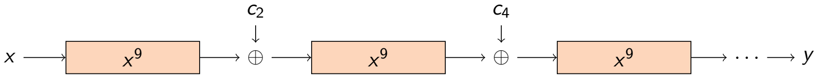


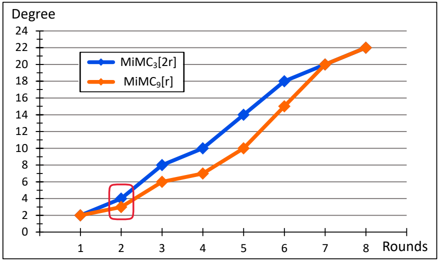
$MiMC_9$ and form of coefficients

- ⋆ $MIMC_3[2r]$



- ⋆ $MIMC_9[r]$





Example: coefficients of maximum weight exponent monomials at round 4

$$27 : c_1^{18} + c_3^2 \qquad 57 : c_1^8$$
$$30 : c_1^{17} \qquad 75 : c_1^2$$
$$51 : c_1^{10} \qquad 78 : c_1$$
$$54 : c_1^9 + c_3$$

Other Quadratic functions

Proposition

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

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

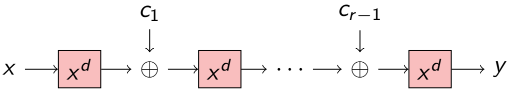
Other Quadratic functions

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, $\ldots$



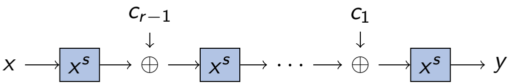
Proposition

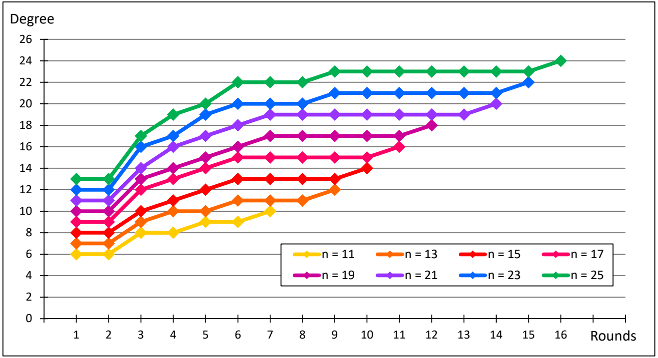
Let $\mathcal{E}_r$ be the set of exponents in the univariate form of MIMC$_d[r]$, where $d = 2^j + 1$. Then:

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

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 $n-2$?

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