On the Algebraic Degree of Iterated Power Functions

Clémence Bouvier [♪,♫]
joint work with Anne Canteaut [♫] and Léo Perrin [♫]

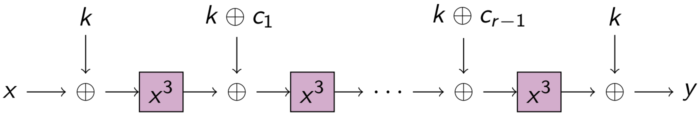
[♪] Sorbonne Université, [♫] Inria Paris, team COSMIQ

WCC, March 7th, 2022

A bit of context

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



A bit of context

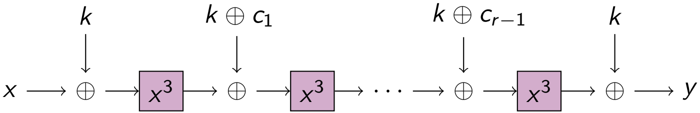
The block cipher MiMC

- 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.



A bit of context

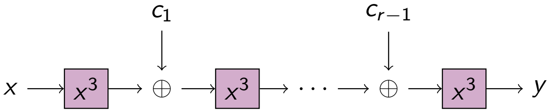
The block cipher MiMC

- 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.



Content

On the Algebraic Degree of Iterated Power Functions

1. Background
   - Emerging uses in symmetric cryptography
   - Definition of algebraic degree

2. On the algebraic degree of MiMC_3
   - First plateau
   - Bounding the degree
   - Exact degree

3. Other permutations
   - Quadratic functions
   - Algebraic degree of MiMC_3^{-1}

4. Integral attack
   - Secret-key 0-sum distinguisher
   - Comparison to previous work

Emerging uses in symmetric cryptography

$\boxed{\textbf{Problem}\text{: Analyzing the security of new symmetric primitives}}$

Protocols requiring new primitives:

- multiparty computation (MPC)
- systems of zero-knowledge proofs (zk-SNARK, zk-STARK)

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

Emerging uses in symmetric cryptography

Problem: Analyzing the security of new symmetric primitives

Protocols requiring new primitives:

- multiparty computation (MPC)
- systems of zero-knowledge proofs (zk-SNARK, zk-STARK)

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

"Usual" case

- operations on $\mathbb{F}_{2^n}$, where $n \simeq 4, 8$.
- based on CPU instructions and hardware components

Arithmetization-friendly

- operations on $\mathbb{F}_q$, where $q \in \{2^n, p\}, p \simeq 2^n, n \geq 64$.
- based on large finite-field arithmetic

Algebraic degree

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, 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 $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$:

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

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

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

Algebraic degree

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, 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 $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$:

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

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

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

First Plateau

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

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$_3$: $x \mapsto x^3 + c_{i+1}$.

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: $B_3^1 = 2$

$$\mathcal{P}_1(x) = x^3$$

$$3 = [11]_2$$

First Plateau

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

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: $B_3^1 = 2$

$$\mathcal{P}_1(x) = x^3$$

$$3 = [11]_2$$

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

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: $\boxed{B_3^1 = 2}$

$$\mathcal{P}_1(x) = x^3$$

$$3 = [11]_2$$

- Round 2: $\boxed{B_3^2 = 2}$

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

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

First Plateau

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

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: $\boxed{B_3^1 = 2}$

$$\mathcal{P}_1(x) = x^3$$

$$3 = [11]_2$$

- Round 2: $\boxed{B_3^2 = 2}$

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

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

First Plateau

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

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: $\boxed{B_3^1 = 2}$

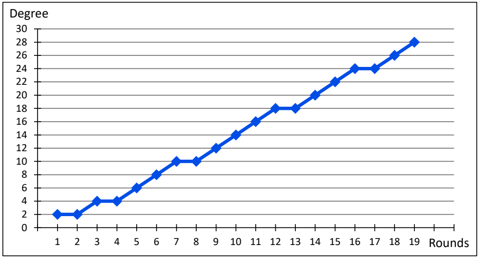
$$\mathcal{P}_1(x) = x^3$$

$$3 = [11]_2$$

- Round 2: $\boxed{B_3^2 = 2}$

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

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



Algebraic degree observed for $n = 31$.

First Plateau

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

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: $\boxed{B_3^1 = 2}$

$$\mathcal{P}_1(x) = x^3$$

$$3 = [11]_2$$

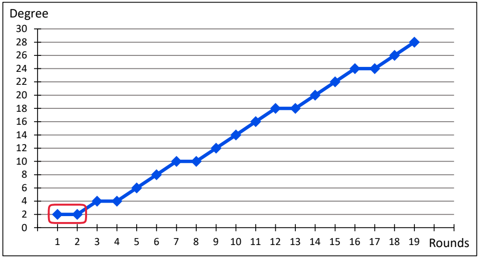
- Round 2: $\boxed{B_3^2 = 2}$

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

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

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: $x \mapsto x^3 + c_{i+1}$.

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: $\boxed{B_3^1 = 2}$

$$\mathcal{P}_1(x) = x^3$$

$$3 = [11]_2$$

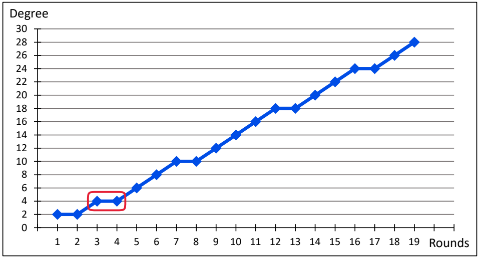
- Round 2: $\boxed{B_3^2 = 2}$

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

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

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: $x \mapsto x^3 + c_{i+1}$.

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: $\boxed{B_3^1 = 2}$

$$\mathcal{P}_1(x) = x^3$$

$$3 = [11]_2$$

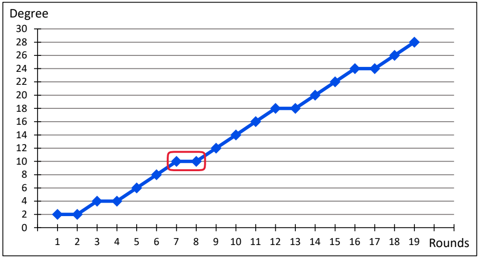
- Round 2: $\boxed{B_3^2 = 2}$

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

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

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$_3$: $x \mapsto x^3 + c_{i+1}$.

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: $\boxed{B_3^1 = 2}$

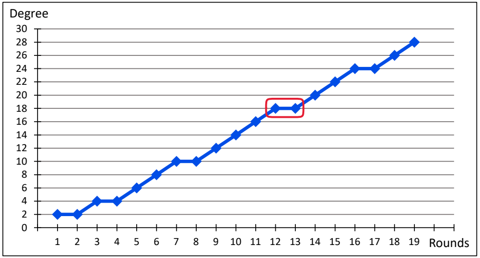
$$\mathcal{P}_1(x) = x^3$$

$$3 = [11]_2$$

- Round 2: $\boxed{B_3^2 = 2}$

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

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



Algebraic degree observed for $n = 31$.

First Plateau

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

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: $\boxed{B_3^1 = 2}$

$$\mathcal{P}_1(x) = x^3$$

$$3 = [11]_2$$

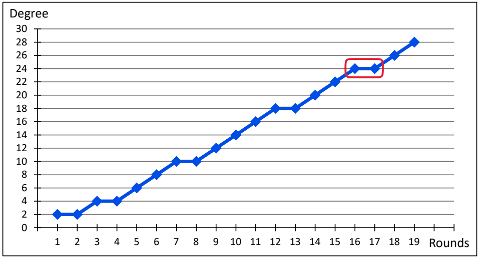
- Round 2: $\boxed{B_3^2 = 2}$

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

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

Definition

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



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:

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

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

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

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 $2^{2k} - 1$

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

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

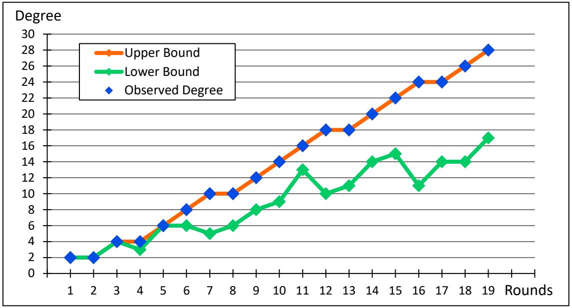
Theorem

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

$\forall r \in \{4, \ldots, 16265\} \backslash \mathcal{F}$ 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,

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

Exact degree

Maximum-weight exponents:

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

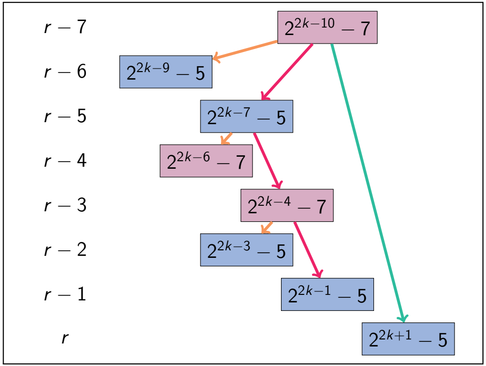
$\forall r \in \{4, \ldots, 16265\} \backslash \mathcal{F}$ with $\mathcal{F} = \{465, 571, \ldots\}$:

- if k_r is odd,

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

- if k_r is even,

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



Constructing exponents.

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

Exact degree

Maximum-weight exponents:

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

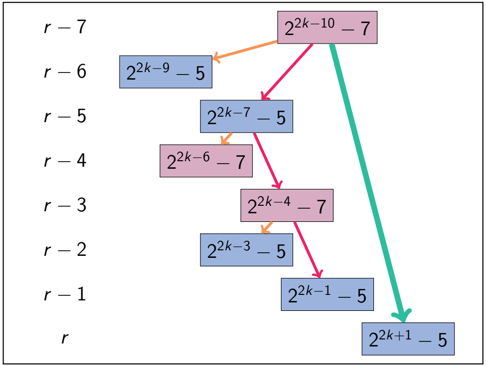
$\forall r \in \{4, \ldots, 16265\} \backslash \mathcal{F}$ with $\mathcal{F} = \{465, 571, \ldots\}$:

- if k_r is odd,

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

- if k_r is even,

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



Constructing exponents.

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

Exact degree

Maximum-weight exponents:

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

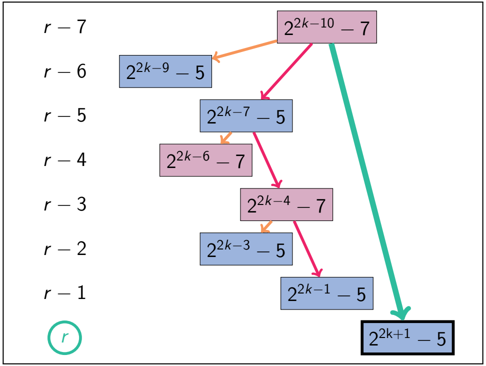
$\forall r \in \{4, \dots, 16265\} \backslash \mathcal{F}$ with $\mathcal{F} = \{465, 571, \dots\}$:

- if k_r is odd,

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

- if k_r is even,

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



Constructing exponents.

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

Exact degree

Maximum-weight exponents:

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

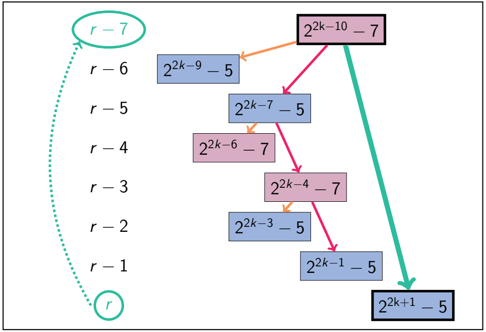
$\forall r \in \{4, \dots, 16265\} \backslash \mathcal{F}$ with $\mathcal{F} = \{465, 571, \dots\}$:

- if k_r is odd,

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

- if k_r is even,

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



Constructing exponents.

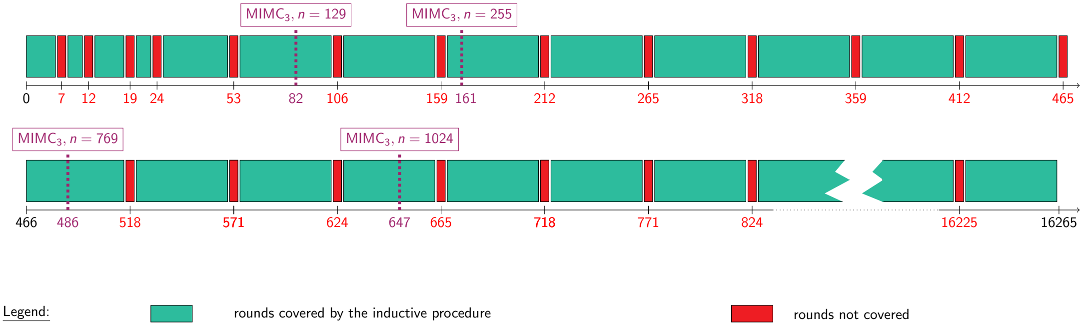
$$\boxed{\exists\, \ell \text{ s.t. } \quad \omega_{r-\ell} \in \mathcal{E}_{r-\ell} \Rightarrow \omega_r \in \mathcal{E}_r}$$

Covered rounds

Idea of the proof:

- inductive proof: existence of "good" ℓ

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

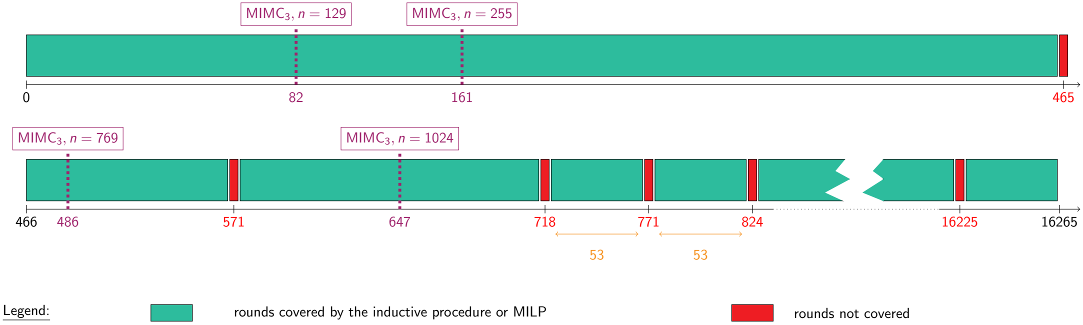


Covered rounds

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.

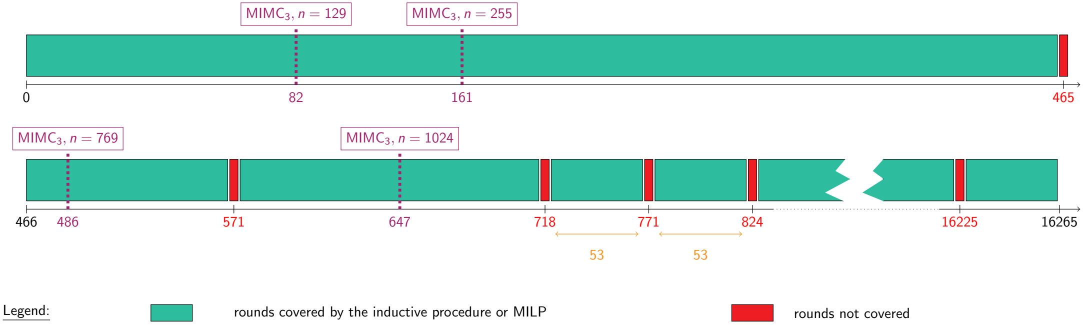


Covered rounds

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.

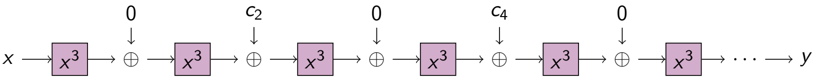


$\Rightarrow$ plateau when $k_r = \lfloor r \log_2 3 \rfloor$ is odd and $k_{r+1} = \lfloor (r+1) \log_2 3 \rfloor$ is even

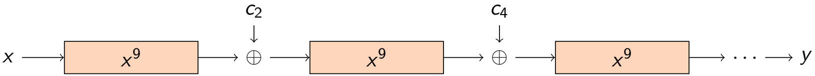
1. Background
   - Emerging uses in symmetric cryptography
   - Definition of algebraic degree
2. On the algebraic degree of MiMC_3
   - First plateau
   - Bounding the degree
   - Exact degree
3. Other permutations
   - Quadratic functions
   - Algebraic degree of MiMC_3^{-1}
4. Integral attack
   - Secret-key 0-sum distinguisher
   - Comparison to previous work

$MiMC_9$ and form of coefficients

- $MIMC_3[2r]$

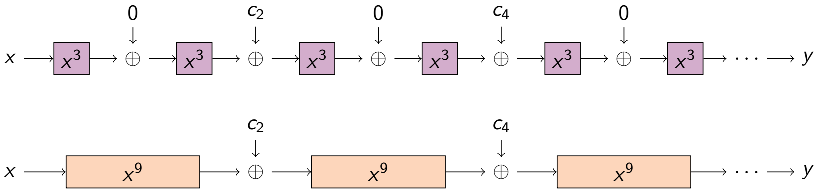


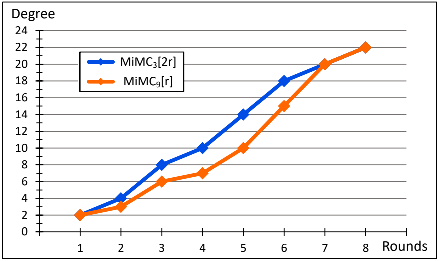
- $MIMC_9[r]$



MiMC_9 and form of coefficients

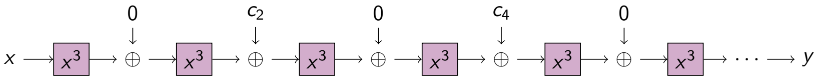
- $\text{MIMC}_3[2r]$
- $\text{MIMC}_9[r]$



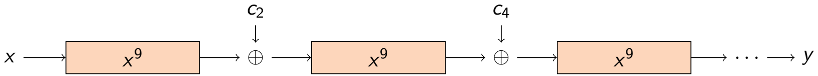


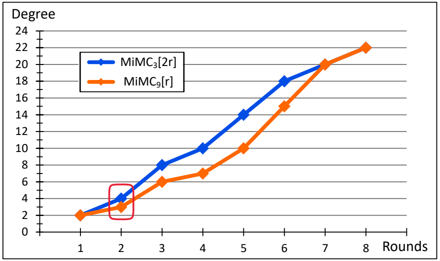
MiMC_9 and form of coefficients

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



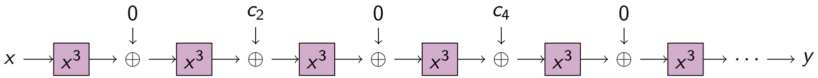
- $\mathrm{MIMC}_9[r]$



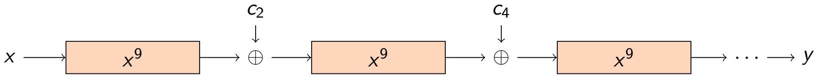


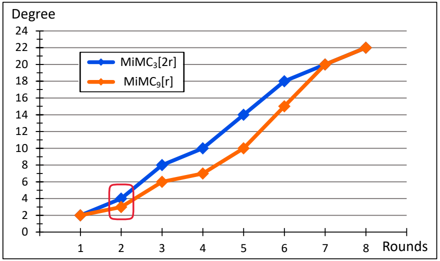
MiMC$_9$ and form of coefficients

- MIMC$_3[2r]$



- MIMC$_9[r]$





Example: coefficients of maximum weight exponent monomials at round 4

$$
\begin{array}{ll}
27 : c_1^{18} + c_3^2 & 57 : c_1^8 \\
30 : c_1^{17} & 75 : c_1^2 \\
51 : c_1^{10} & 78 : c_1 \\
54 : c_1^9 + c_3 &
\end{array}
$$

Other Quadratic functions

Proposition

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

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

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

$$x \longrightarrow \boxed{x^d} \longrightarrow \overset{\displaystyle c_1 \atop \displaystyle \downarrow}{\oplus} \longrightarrow \boxed{x^d} \longrightarrow \cdots \longrightarrow \overset{\displaystyle c_{r-1} \atop \displaystyle \downarrow}{\oplus} \longrightarrow \boxed{x^d} \longrightarrow y$$

Proposition

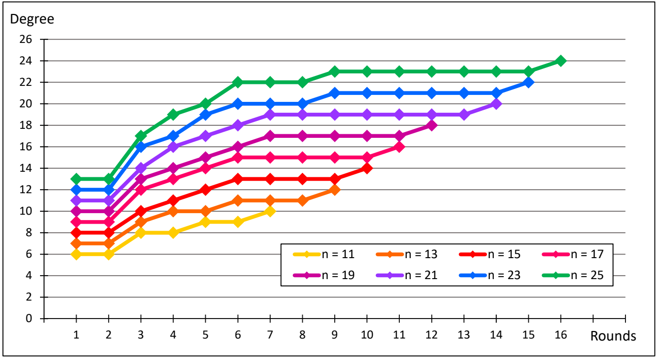
Let $\mathcal{E}_r$ be the set of exponents in the univariate form of $\mathrm{MIMC}_d[r]$, where $d = 2^j + 1$. Then:

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

Study of MiMC_3^{-1}

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

$$x \longrightarrow \boxed{x^s} \longrightarrow \overset{c_{r-1}}{\overset{\downarrow}{\oplus}} \longrightarrow \boxed{x^s} \longrightarrow \cdots \longrightarrow \overset{c_1}{\overset{\downarrow}{\oplus}} \longrightarrow \boxed{x^s} \longrightarrow y$$



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 $n - 2$?

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

1. Background
   - Emerging uses in symmetric cryptography
   - Definition of algebraic degree
2. On the algebraic degree of MiMC_3
   - First plateau
   - Bounding the degree
   - Exact degree
3. Other permutations
   - Quadratic functions
   - Algebraic degree of MiMC_3^{-1}
4. Integral attack
   - Secret-key 0-sum distinguisher
   - Comparison to previous work

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 $= n - 1$

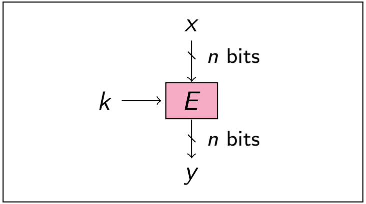
Higher-order differential attack

Exploiting a low algebraic degree

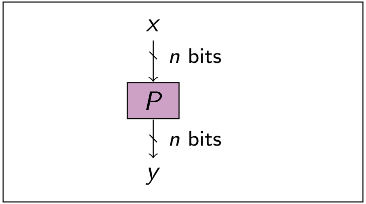
For any affine subspace $\mathcal{V} \subset \mathbb{F}_2^n$ with $\dim \mathcal{V} \geq \deg^a(F) + 1$, we have a 0-sum distinguisher:

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

Random permutation: degree $= n - 1$



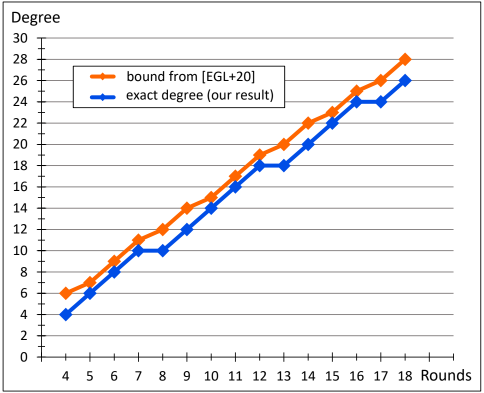
Block cipher



Random permutation

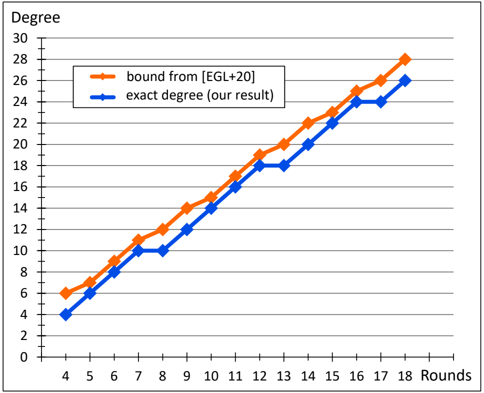
Comparison to previous work

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



For $n = 129$, $\mathrm{MIMC}_3 = 82$ 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 ($n = 129$)

Conclusions

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

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

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

Conclusions

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

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

  - bound tight, up to 16265 rounds.
- minimal complexity for higher-order differential attack
- application in music for semiconvergents of $\log_2(3)$

Conclusions

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

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

  - bound tight, up to 16265 rounds.
- minimal complexity for higher-order differential attack
- application in music for semiconvergents of $\log_2(3)$

Thanks for your attention

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

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

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

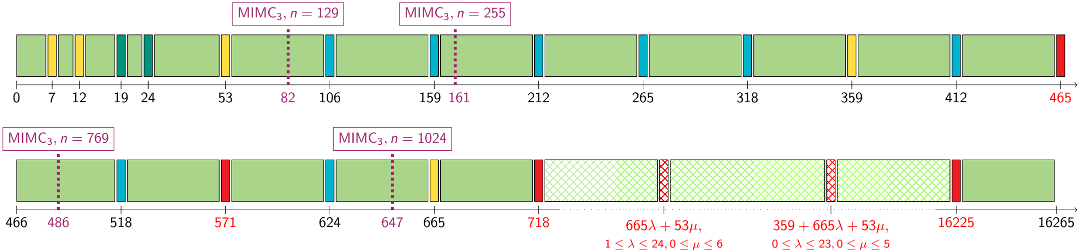
Let $r \geq 4$, and $\ell \in \mathcal{L}_r$ s.t.:

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

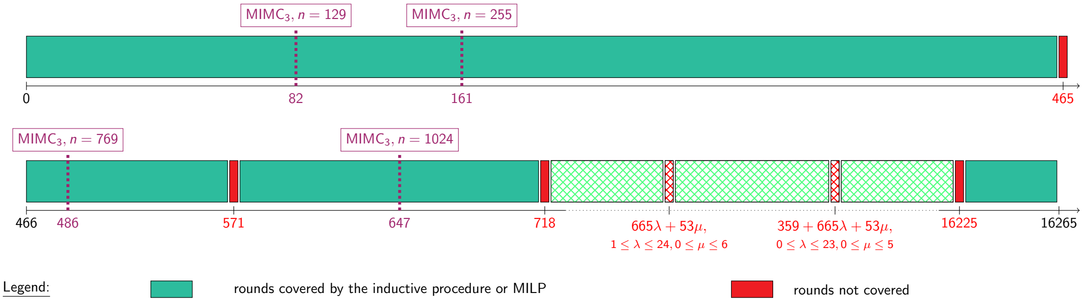
- semiconvergents of $\log_2(3)$: MILP
- "good" ℓ
- no "good" ℓ: MILP
- no "good" ℓ ($\ell \geq 53$): MILP

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:

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

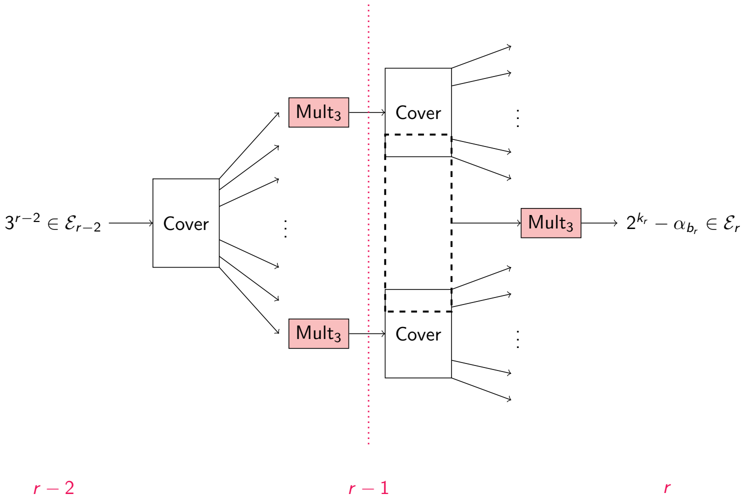
$\Rightarrow$ MILP problem solved using `PySCIPOpt`

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

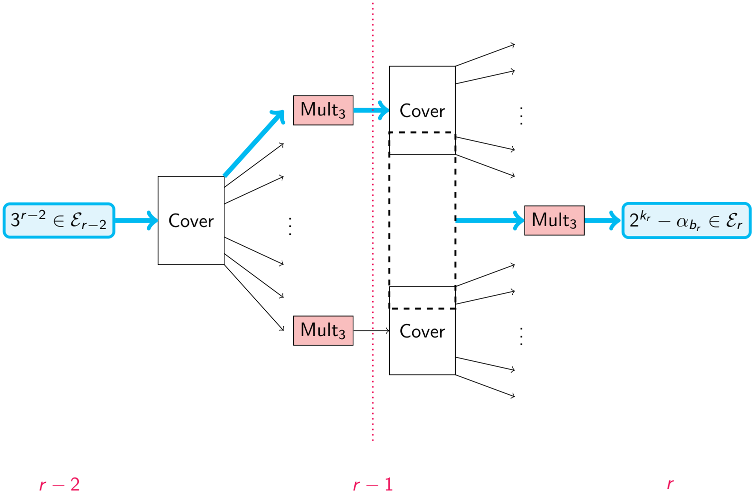
With $\ell = 1$:

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

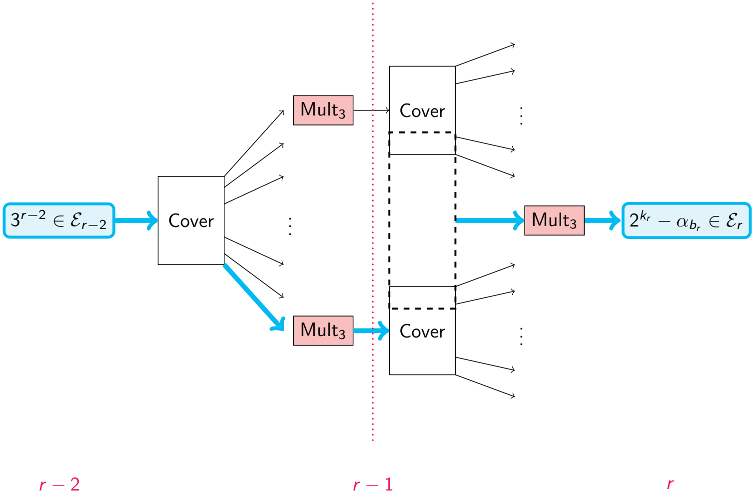
MILP Solver (2 rounds)



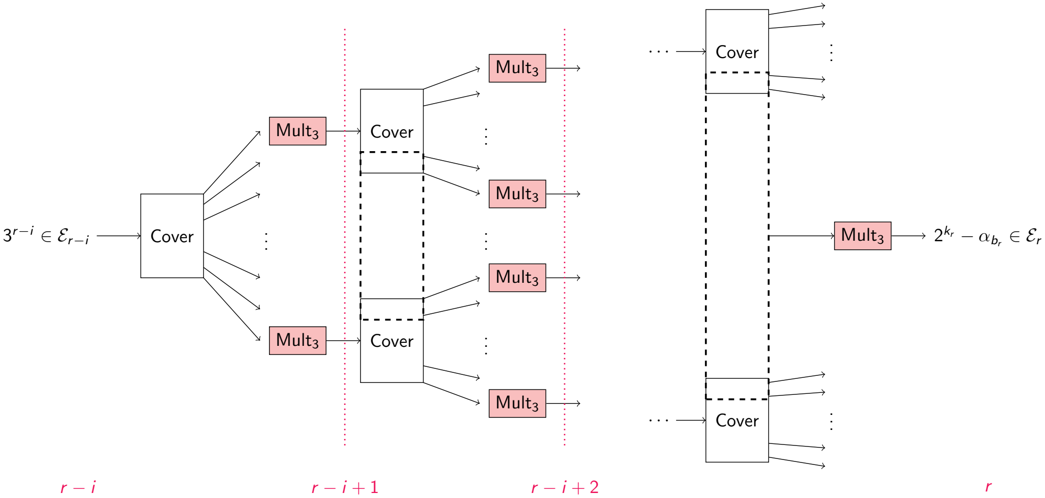
MILP Solver (2 rounds)



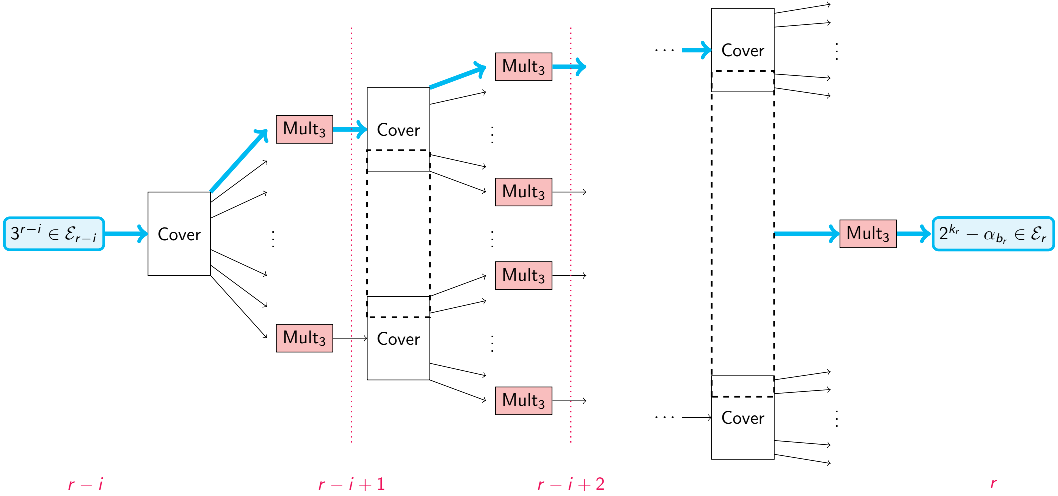
MILP Solver (2 rounds)



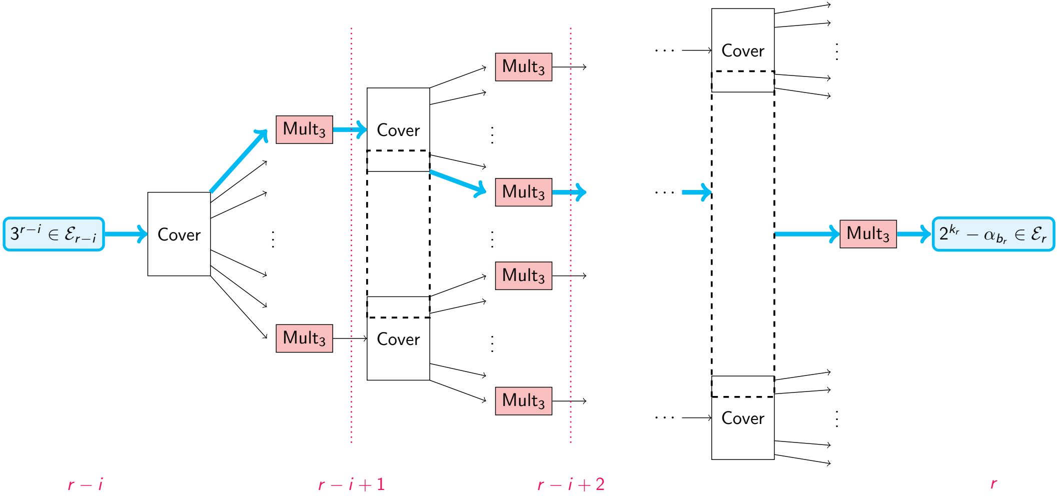
MILP Solver (i rounds)



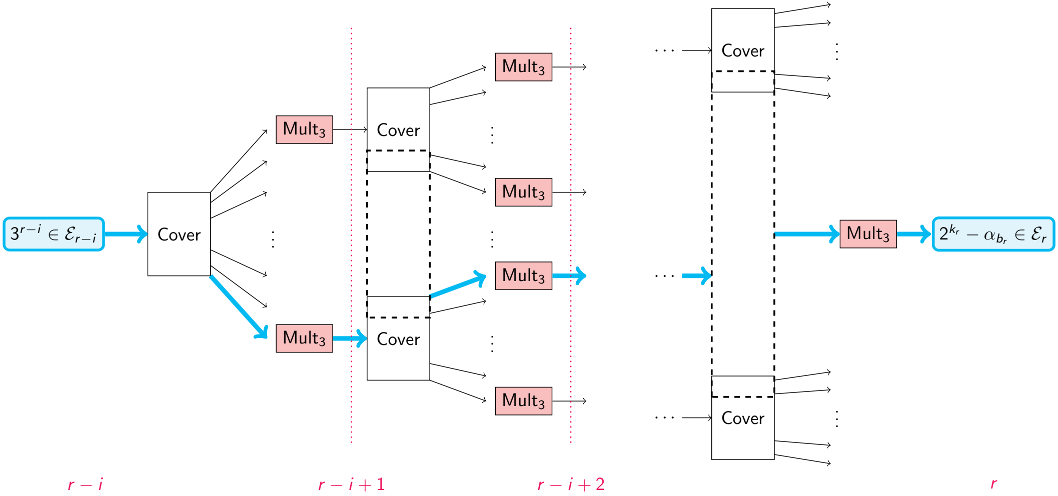
MILP Solver (i rounds)



MILP Solver (i rounds)



MILP Solver (i rounds)



MILP Solver (i rounds)