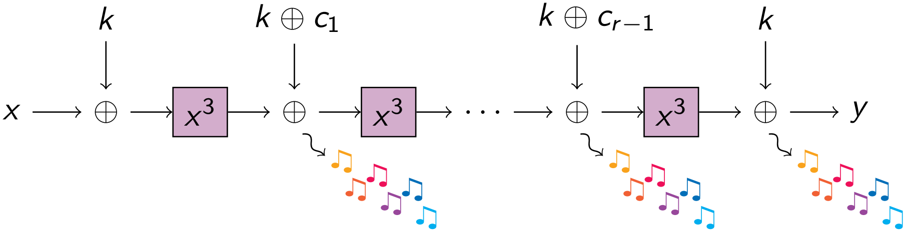
Iterated Power Functions: from Univariate Polynomial Representation to Multivariate Degree

Clémence Bouvier [1,2]
joint work with Anne Canteaut[2] and Léo Perrin[2]

[1]Sorbonne Université, [2]Inria Paris

Fq15, June 20th, 2023

Introduction



Content

Iterated Power Functions:
from Univariate Polynomial Representation to Multivariate Degree

Content

Iterated Power Functions:
from Univariate Polynomial Representation to Multivariate Degree

Block ciphers

- input: n-bit block

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

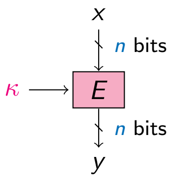
- parameter: k-bit key

$$\kappa \in \mathbb{F}_{2^k}$$

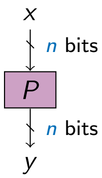
- output: n-bit block

$$y = E_\kappa(x) \in \mathbb{F}_{2^n}$$

- symmetry: E and E^{-1} use the same κ



Block cipher



Random permutation

Block ciphers

- ⋆ input: n-bit block

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

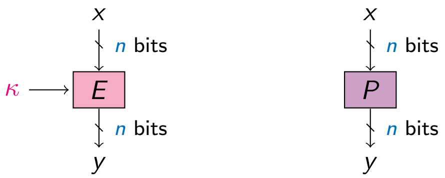
- ⋆ parameter: k-bit key

$$\kappa \in \mathbb{F}_{2^k}$$

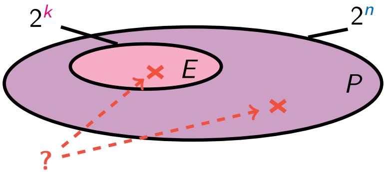
- ⋆ output: n-bit block

$$y = E_\kappa(x) \in \mathbb{F}_{2^n}$$

- ⋆ symmetry: E and E^{-1} use the same κ



Block cipher *Random permutation*



A block cipher is a family of 2^k permutations of n bits.

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.

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

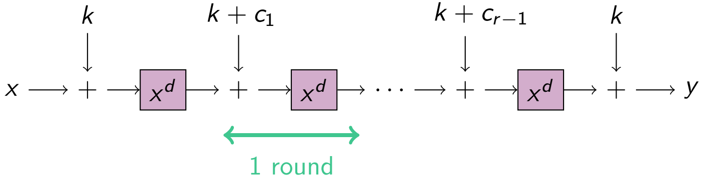
- ⋆ operations on $\mathbb{F}_{2^n}$, where $n \simeq 4, 8$.
- ⋆ based on CPU instructions and hardware components

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

The block cipher MiMC

- Minimize the number of multiplications in $\mathbb{F}_{2^n}$.
- Construction of MiMC_3 [Albrecht et al., AC16]:
  - n-bit blocks: $x \in \mathbb{F}_{2^n}$ (n odd ≈ 129)
  - n-bit key k: $k \in \mathbb{F}_{2^n}$
  - decryption: e.g. replacing x^3 by x^s where $s = (2^{n+1} - 1)/3$



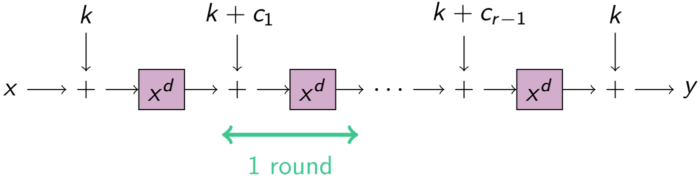
The block cipher MiMC

- Minimize the number of multiplications in $\mathbb{F}_{2^n}$.
- Construction of MiMC$_3$ [Albrecht et al., AC16]:
  - n-bit blocks: $x \in \mathbb{F}_{2^n}$ (n odd ≈ 129)
  - n-bit key k: $k \in \mathbb{F}_{2^n}$
  - decryption: e.g. 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$_3$.



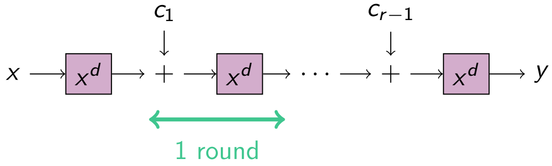
The block cipher MiMC

- Minimize the number of multiplications in $\mathbb{F}_{2^n}$.
- Construction of MiMC_3 [Albrecht et al., AC16]:
  - n-bit blocks: $x \in \mathbb{F}_{2^n}$ (n odd ≈ 129)
  - n-bit key k: $k \in \mathbb{F}_{2^n}$
  - decryption: e.g. 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_3.



Multivariate degree - 1st definition

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

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

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

Definition

Multivariate Degree (aka **Algebraic Degree**) of $f : \mathbb{F}_2^n \to \mathbb{F}_2$:

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

Multivariate degree - 1st definition

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

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

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

Definition

Multivariate Degree (aka **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 $F(x) = (f_1(x), \dots f_m(x))$.

Multivariate degree - 1st definition

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

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

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

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

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

$$\begin{aligned}
(&x_0x_{10} + x_0 + x_1x_5 + x_1x_9 + x_2x_7 + x_2x_9 + x_2x_{10} + x_3x_4 + x_3x_5 + x_4x_8 + x_4x_9 + x_5x_{10} + x_6x_7 + x_6x_{10} + x_7x_8 + x_9x_{10},\\
&x_0x_1 + x_0x_6 + x_2x_5 + x_2x_8 + x_3x_6 + x_3x_9 + x_3x_{10} + x_4 + x_5x_8 + x_5x_9 + x_6x_9 + x_7x_8 + x_7x_9 + x_7 + x_{10},\\
&x_0x_1 + x_0x_2 + x_0x_{10} + x_1x_5 + x_1x_6 + x_1x_9 + x_2x_7 + x_3x_4 + x_3x_7 + x_4x_5 + x_4x_8 + x_4x_{10} + x_5x_{10} + x_6x_7 + x_6x_8 + x_6x_9 + x_7x_{10} + x_8 + x_9x_{10},\\
&x_0x_3 + x_0x_6 + x_0x_7 + x_1 + x_2x_5 + x_2x_6 + x_2x_8 + x_2x_{10} + x_3x_6 + x_3x_8 + x_3x_9 + x_4x_5 + x_4x_6 + x_4 + x_5x_8 + x_5x_{10} + x_6x_9 + x_7x_9 + x_7 + x_8x_9 + x_{10},\\
&x_0x_2 + x_0x_4 + x_1x_2 + x_1x_6 + x_1x_7 + x_2x_9 + x_2x_{10} + x_3x_5 + x_3x_6 + x_3x_7 + x_3x_9 + x_4x_5 + x_4x_7 + x_4x_9 + x_5 + x_6x_8 + x_7x_8 + x_8x_9 + x_8x_{10},\\
&x_0x_5 + x_0x_7 + x_0x_8 + x_1x_2 + x_1x_3 + x_2x_6 + x_2x_7 + x_2x_{10} + x_3x_8 + x_4x_5 + x_4x_8 + x_5x_6 + x_5x_9 + x_7x_8 + x_7x_9 + x_7x_{10} + x_9,\\
&x_0x_3 + x_0x_6 + x_1x_4 + x_1x_7 + x_1x_8 + x_2 + x_3x_6 + x_3x_7 + x_3x_9 + x_4x_7 + x_4x_9 + x_4x_{10} + x_5x_6 + x_5x_7 + x_5 + x_6x_9 + x_7x_{10} + x_8x_{10} + x_8 + x_9x_{10},\\
&x_0x_7 + x_0x_8 + x_0x_9 + x_1x_3 + x_1x_5 + x_2x_3 + x_2x_7 + x_2x_8 + x_3x_{10} + x_4x_6 + x_4x_7 + x_4x_8 + x_4x_{10} + x_5x_6 + x_5x_8 + x_5x_{10} + x_6 + x_7x_9 + x_8x_9 + x_9x_{10},\\
&x_0x_4 + x_0x_8 + x_1x_6 + x_1x_8 + x_1x_9 + x_2x_3 + x_2x_4 + x_3x_7 + x_3x_8 + x_4x_9 + x_5x_6 + x_5x_9 + x_6x_7 + x_6x_{10} + x_8x_9 + x_8x_{10} + x_{10},\\
&x_0x_{10} + x_1x_4 + x_1x_7 + x_2x_5 + x_2x_8 + x_2x_9 + x_3 + x_4x_7 + x_4x_8 + x_4x_{10} + x_5x_8 + x_5x_{10} + x_6x_7 + x_6x_8 + x_6 + x_7x_{10} + x_9,\\
&x_0x_5 + x_0x_{10} + x_1x_8 + x_1x_9 + x_1x_{10} + x_2x_4 + x_2x_6 + x_3x_4 + x_3x_8 + x_3x_9 + x_5x_7 + x_5x_8 + x_5x_9 + x_6x_7 + x_6x_9 + x_7 + x_8x_{10} + x_9x_{10}) \; .
\end{aligned}$$

Multivariate degree - 2nd definition

Let $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$. Then using the isomorphism $\mathbb{F}_2^n \simeq \mathbb{F}_{2^n}$,
there is **a unique univariate polynomial representation** on $\mathbb{F}_{2^n}$ of degree at most $2^n - 1$:

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

Definition

Multivariate Degree (aka **Algebraic Degree**) of $F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$:

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

Multivariate degree - 2nd definition

Let $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$. Then using the isomorphism $\mathbb{F}_2^n \simeq \mathbb{F}_{2^n}$,
there is **a unique univariate polynomial representation** on $\mathbb{F}_{2^n}$ of degree at most $2^n - 1$:

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

Definition

Multivariate Degree (aka **Algebraic Degree**) of $F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$:

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

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

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

Content

Iterated Power Functions:
from Univariate Polynomial Representation to Multivariate Degree

First Plateau

Polynomial representing r rounds of MiMC$_d$:

$$\mathcal{P}_{d,r}(x) = F_r \circ \ldots F_1(x) \ , \ \text{where } F_i = (x + c_{i-1})^d \ .$$

Aim: determine

$$B_d^r := \max_c \deg^a(\mathcal{P}_{d,r}) \ .$$

First Plateau

Polynomial representing r rounds of MiMC$_d$:

$$\mathcal{P}_{d,r}(x) = F_r \circ \ldots F_1(x) \text{ , where } F_i = (x + c_{i-1})^d \text{ .}$$

Aim: determine

$$B_d^r := \max_c \deg^a(\mathcal{P}_{d,r}) \text{ .}$$

- ⋆ Round 1: $B_3^1 = 2$

$$\mathcal{P}_{3,1}(x) = x^3$$

$$3 = [11]_2$$

First Plateau

Polynomial representing r rounds of MiMC$_d$:

$$\mathcal{P}_{d,r}(x) = F_r \circ \ldots F_1(x) \ , \ \text{where } F_i = (x + c_{i-1})^d \ .$$

Aim: determine

$$B_d^r := \max_c \deg^a(\mathcal{P}_{d,r}) \ .$$

- ⋆ Round 1: $B_3^1 = 2$

$$\mathcal{P}_{3,1}(x) = x^3$$

$$3 = [11]_2$$

- ⋆ Round 2: $B_3^2 = 2$

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

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

First Plateau

Polynomial representing r rounds of MiMC$_d$:

$$\mathcal{P}_{d,r}(x) = F_r \circ \dots F_1(x) \ , \ \text{where } F_i = (x + c_{i-1})^d \ .$$

Aim: determine

$$B_d^r := \max_c \deg^a(\mathcal{P}_{d,r}) \ .$$

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

$$\mathcal{P}_{3,1}(x) = x^3$$

$$3 = [11]_2$$

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

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

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

First Plateau

Polynomial representing r rounds of MiMC$_d$:

$$\mathcal{P}_{d,r}(x) = F_r \circ \ldots F_1(x) \ , \ \text{where } F_i = (x + c_{i-1})^d \ .$$

Aim: determine

$$B_d^r := \max_c \deg^a(\mathcal{P}_{d,r}) \ .$$

- ⋆ Round 1: $\boxed{B_3^1 = 2}$

$$\mathcal{P}_{3,1}(x) = x^3$$

$$3 = [11]_2$$

- ⋆ Round 2: $\boxed{B_3^2 = 2}$

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

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

Definition

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

First Plateau

Polynomial representing r rounds of MiMC$_d$:

$$\mathcal{P}_{d,r}(x) = F_r \circ \ldots F_1(x) \ , \ \text{where } F_i = (x + c_{i-1})^d \ .$$

Aim: determine

$$B_d^r := \max_c \deg^a(\mathcal{P}_{d,r}) \ .$$

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

$$\mathcal{P}_{3,1}(x) = x^3$$

$$3 = [11]_2$$

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

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

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

Definition

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

Proposition

If $d = 2^j - 1$, there is always **plateau** between rounds 1 and 2:

$$B_d^2 = B_d^1 \ .$$

Missing exponents

Proposition

Set of exponents that might appear in the polynomial:

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

Missing exponents

Proposition

Set of exponents that might appear in the polynomial:

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

Example:

$$\mathcal{P}_{3,1}(x) = x^3 \quad \Rightarrow \quad \mathcal{E}_{3,1} = \{3\} .$$

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

$$\mathcal{E}_{3,2} = \{0, 3, 6, 9\} ,$$

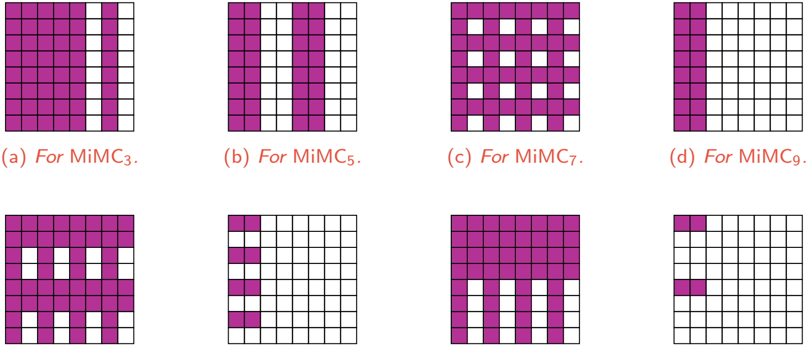
$$\mathcal{P}_{3,2}(x) = x^9 + c_1 x^6 + c_1^2 x^3 + c_1^3 .$$

Missing exponents

Proposition

Set of exponents that might appear in the polynomial:

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



(a) *For* MiMC$_3$. (b) *For* MiMC$_5$. (c) *For* MiMC$_7$. (d) *For* MiMC$_9$.

(a) *For* MiMC$_{15}$. (b) *For* MiMC$_{17}$. (c) *For* MiMC$_{31}$. (d) *For* MiMC$_{33}$.

Missing exponents when $d = 2^j - 1$

Proposition

Let $i \in \mathcal{E}_{d,r}$, where $d = 2^j - 1$. Then:

$$\forall\, i \in \mathcal{E}_{d,r},\ i \bmod 2^{j+1} \in \{0, 1, \ldots 2^j\} \bigcup \{2^j + 2\gamma, \gamma = 1, 2, \ldots 2^{j-1} - 1\}\ .$$

Missing exponents when $d = 2^j - 1$

Proposition

Let $i \in \mathcal{E}_{d,r}$, where $d = 2^j - 1$. Then:

$$\forall\, i \in \mathcal{E}_{d,r},\ i \bmod 2^{j+1} \in \{0, 1, \ldots 2^j\} \bigcup \{2^j + 2\gamma, \gamma = 1, 2, \ldots 2^{j-1} - 1\}\ .$$

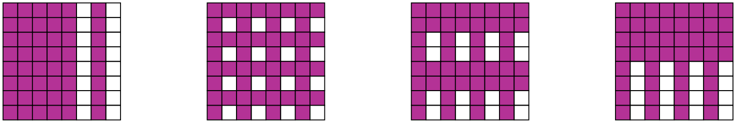
Example:

- ⋆ For MiMC_3

$$\forall\, i \in \mathcal{E}_{3,r},\ i \bmod 8 \notin \{5, 7\}\ .$$

- ⋆ For MiMC_7

$$\forall\, i \in \mathcal{E}_{7,r},\ i \bmod 16 \notin \{9, 11, 13, 15\}\ .$$



(a) *For* MiMC_3. (b) *For* MiMC_7. (c) *For* MiMC_{15}. (d) *For* MiMC_{31}.

Missing exponents when $d = 2^j + 1$

Proposition

Let $i \in \mathcal{E}_{d,r}$ where $d = 2^j + 1$ and $j > 1$. Then:

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

Missing exponents when $d = 2^j + 1$

Proposition

Let $i \in \mathcal{E}_{d,r}$ where $d = 2^j + 1$ and $j > 1$. Then:

$$\forall\, i \in \mathcal{E}_{d,r},\; i \bmod 2^j \in \{0, 1\} .$$

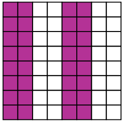
Example:

- For MiMC_5

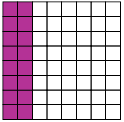
$$\forall\, i \in \mathcal{E}_{5,r},\; i \bmod 4 \in \{0, 1\} .$$

- For MiMC_9

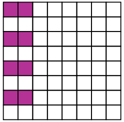
$$\forall\, i \in \mathcal{E}_{9,r},\; i \bmod 8 \in \{0, 1\} .$$



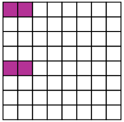
(a) *For* MiMC_5.



(b) *For* MiMC_9.



(c) *For* MiMC_{17}.



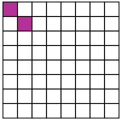
(d) *For* MiMC_{33}.

Missing exponents when $d = 2^j + 1$ (first rounds)

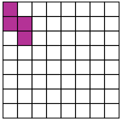
Corollary

Let $i \in \mathcal{E}_{d,r}$ where $d = 2^j + 1$ and $j > 1$. Then:

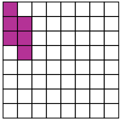
$$\begin{cases} i \bmod 2^{2j} \in \{\{\gamma 2^j, (\gamma+1)2^j + 1\},\ \gamma = 0, \dots r-1\} & \text{if } r \leq 2^j\ , \\ i \bmod 2^j \in \{0, 1\} & \text{if } r \geq 2^j\ . \end{cases}$$



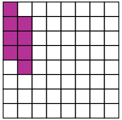
(a) *Round 1*



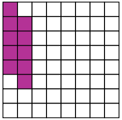
(b) *Round 2*



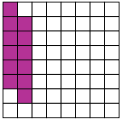
(c) *Round 3*



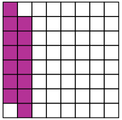
(d) *Round 4*



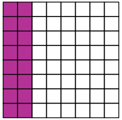
(a) *Round 5*



(b) *Round 6*



(c) *Round 7*



(d) *Round $r \geq 8$*

Content

Iterated Power Functions:
from Univariate Polynomial Representation to Multivariate Degree

Bounding the degree when $d = 2^j - 1$

Note that if $d = 2^j - 1$, then

$$2^i \bmod d \equiv 2^{i \bmod j} .$$

Proposition

Let $d = 2^j - 1$, such that $j \geq 2$. Then,

$$B_d^r \leq \lfloor r \log_2 d \rfloor - (\lfloor r \log_2 d \rfloor \bmod j) .$$

Bounding the degree when $d = 2^j - 1$

Note that if $d = 2^j - 1$, then

$$2^i \bmod d \equiv 2^{i \bmod j} .$$

Proposition

Let $d = 2^j - 1$, such that $j \geq 2$. Then,

$$B_d^r \leq \lfloor r \log_2 d \rfloor - (\lfloor r \log_2 d \rfloor \bmod j) .$$

Note that if $2 \leq j \leq 7$, then

$$2^{\lfloor r \log_2 d \rfloor + 1} - 2^j - 1 > d^r .$$

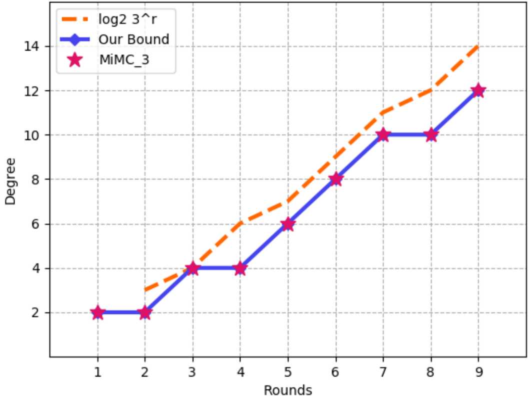
Corollary

Let $d \in \{3, 7, 15, 31, 63, 127\}$. Then,

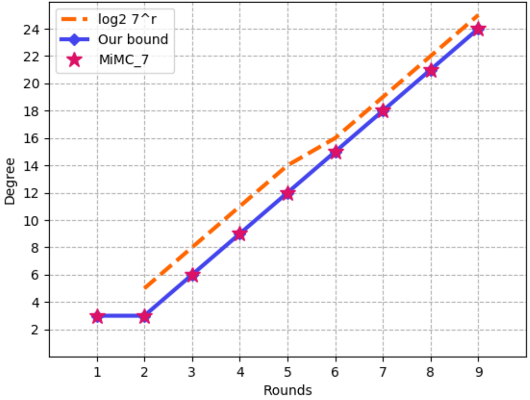
$$B_d^r \leq \begin{cases} \lfloor r \log_2 d \rfloor - j & \text{if } \lfloor r \log_2 d \rfloor \bmod j = 0 , \\ \lfloor r \log_2 d \rfloor - (\lfloor r \log_2 d \rfloor \bmod j) & \text{else} . \end{cases}$$

Bounding the degree when $d = 2^j - 1$

Particularity: Plateau when $\lfloor r \log_2 d \rfloor \bmod j = j - 1$ and $\lfloor (r+1) \log_2 d \rfloor \bmod j = 0$.



Bound for MiMC$_3$



Bound for MiMC$_7$

Bounding the degree when $d = 2^j + 1$

Note that if $d = 2^j + 1$, then

$$2^i \bmod d \equiv \begin{cases} 2^{i \bmod 2j} & \text{if } i \equiv 0, \ldots, j \bmod 2j \ , \\ d - 2^{(i \bmod 2j) - j} & \text{if } i \equiv 0, \ldots, j \bmod 2j \ . \end{cases}$$

Proposition

Let $d = 2^j + 1$ s.t. $j > 1$. Then if $r > 1$:

$$B_d^r \leq \begin{cases} \lfloor r \log_2 d \rfloor - j + 1 & \text{if } \lfloor r \log_2 d \rfloor \bmod 2j \in \{0, j-1, j+1\} \ , \\ \lfloor r \log_2 d \rfloor - j & \text{else } . \end{cases}$$

Bounding the degree when $d = 2^j + 1$

Note that if $d = 2^j + 1$, then

$$2^i \bmod d \equiv \begin{cases} 2^{i \bmod 2j} & \text{if } i \equiv 0, \ldots, j \bmod 2j \ , \\ d - 2^{(i \bmod 2j) - j} & \text{if } i \equiv 0, \ldots, j \bmod 2j \ . \end{cases}$$

Proposition

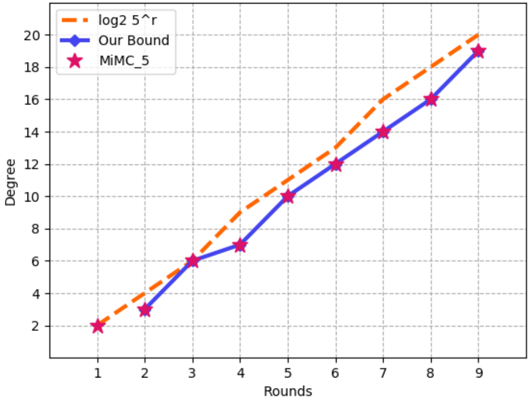
Let $d = 2^j + 1$ s.t. $j > 1$. Then if $r > 1$:

$$B_d^r \leq \begin{cases} \lfloor r \log_2 d \rfloor - j + 1 & \text{if } \lfloor r \log_2 d \rfloor \bmod 2j \in \{0, j-1, j+1\} \ , \\ \lfloor r \log_2 d \rfloor - j & \text{else} \ . \end{cases}$$

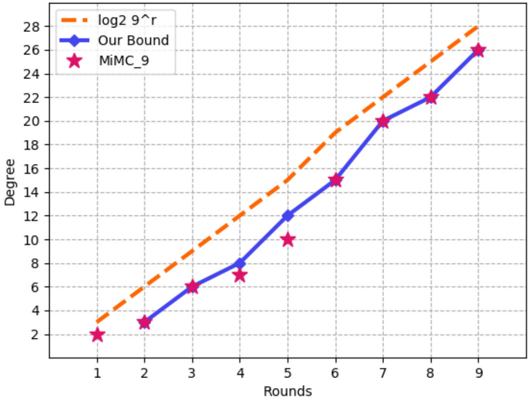
The bound can be refined on the first rounds!

Bounding the degree when $d = 2^j + 1$

Particularity: There is a gap in the first rounds.



Bound for MiMC$_5$



Bound for MiMC$_9$

Music in MiMC_3 and Conjecture

- Patterns in sequence $(\lfloor r \log_2 3 \rfloor)_{r>0}$: denominators of semiconvergents of $\log_2 3 \simeq 1.58496$

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

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

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

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

Music in MiMC_3 and Conjecture

- Patterns in sequence $(\lfloor r \log_2 3 \rfloor)_{r>0}$: denominators of semiconvergents of $\log_2 3 \simeq 1.58496$

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

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

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

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

Observation

Let t be an integer s.t. $1 \le t \le 21$. Then

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

Conclusions and Perspectives

How to set up a distinguisher for MiMC_d using sparse univariate representation?

* missing exponents in the univariate representation of MiMC_d.

Conclusions and Perspectives

How to set up a distinguisher for MiMC_d using sparse univariate representation?

⋆ missing exponents in the univariate representation of MiMC_d.

↓

⋆ bounds on the multivariate degree

Conclusions and Perspectives

How to set up a distinguisher for MiMC_d using sparse univariate representation?

- missing exponents in the univariate representation of MiMC_d.

$\downarrow$

- bounds on the multivariate degree $\longrightarrow$ - Higher-Order differential attacks

Conclusions and Perspectives

How to set up a distinguisher for MiMC_d using sparse univariate representation?

⋆ missing exponents in the univariate representation of MiMC_d. $\longrightarrow$ ⋆ ? ? ?

$\downarrow$

⋆ bounds on the multivariate degree $\longrightarrow$ ⋆ Higher-Order differential attacks

Conclusions and Perspectives

How to set up a distinguisher for MiMC_d using sparse univariate representation?

⋆ missing exponents in the univariate representation of MiMC_d. $\longrightarrow$ ⋆ ? ? ?

$\downarrow$

⋆ bounds on the multivariate degree $\longrightarrow$ ⋆ Higher-Order differential attacks

⋆ tracing exponents: conjecture? $\nearrow$

Conclusions and Perspectives

How to set up a distinguisher for MiMC_d using sparse univariate representation?

⋆ missing exponents in the univariate representation of MiMC_d. → ⋆ ? ? ?

↓

⋆ bounds on the multivariate degree → ⋆ Higher-Order differential attacks

⋆ tracing exponents: conjecture? ↗

☞ More details on eprint.iacr.org/2022/366 (accepted at DCC23)

♪♪♪♪♪♪♪♪♪♪♪♪♪♪♪♪♪♪♪♪♪♪♪♪♪♪♪♪♪♪ *Thanks for your attention*