Arithmetization-Oriented symmetric primitives: from Cryptanalysis to Design.

Clémence Bouvier [1,2]

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

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

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

June 14th, 2023

Content

Arithmetization-Oriented symmetric primitives: from Cryptanalysis to Design.

Comparison with "usual" case

A new environment

"Usual" case

- ⋆ Field size:
  $\mathbb{F}_{2^n}$, with $n \simeq 4, 8$ (AES: $n = 8$).
- ⋆ Operations:
  logical gates/CPU instructions

Arithmetization-friendly

- ⋆ Field size:
  $\mathbb{F}_q$, with $q \in \{2^n, p\}, p \simeq 2^n$, $n \geq 64$
- ⋆ Operations:
  large finite-field arithmetic

Comparison with “usual” case

A new environment

“Usual” case

- ⋆ Field size:
  $\mathbb{F}_{2^n}$, with $n \simeq 4, 8$ (AES: $n = 8$).
- ⋆ Operations:
  logical gates/CPU instructions

Arithmetization-friendly

- ⋆ Field size:
  $\mathbb{F}_q$, with $q \in \{2^n, p\}, p \simeq 2^n,\ n \geq 64$
- ⋆ Operations:
  large finite-field arithmetic

$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, with p given by the order of some elliptic curves

Examples:

- ⋆ Curve BLS12-381 $\quad \log_2 p = 255$

  $p = 52435875175126190479447740508185965837690552500527637822603658699938581184513$

- ⋆ Curve BLS12-377 $\quad \log_2 p = 253$

  $p = 8444461749428370424248824938781546531375899335154063827935233455917409239041$

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

$$y \leftarrow E(x)$$

- Optimized for: implementation in software/hardware

Arithmetization-friendly

$$y \leftarrow E(x) \quad \text{and} \quad y == E(x)$$

- Optimized for: 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 instr

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

Decades of Cryptanalysis

$\leq$ 5 years of Cryptanalysis

N

“U al” case

$$y \leftarrow E(x)$$

- Optimized for: implementation in software/hardware

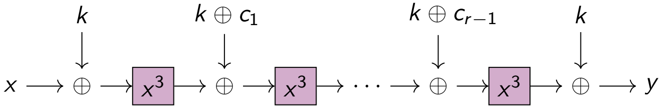
Arit ization-friendly

$$y \leftarrow E(x) \quad \text{and} \quad y == E(x)$$

- Optimized for: 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., Asiacrypt16]:
  - 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 $s = (2^{n+1} - 1)/3$



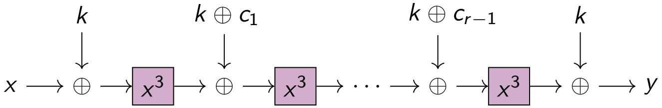
The block cipher MiMC

- Minimize the number of multiplications in $\mathbb{F}_{2^n}$.
- Construction of MiMC_3 [Albrecht et al., Asiacrypt16]:
  - 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.



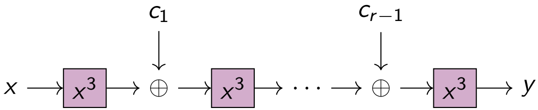
The block cipher MiMC

- Minimize the number of multiplications in $\mathbb{F}_{2^n}$.
- Construction of MiMC$_3$ [Albrecht et al., Asiacrypt16]:
  - n-bit blocks (n odd ≈ 129): $x \in \mathbb{F}_{2^n}$
  - n-bit key: $k \in \mathbb{F}_{2^n}$
  - decryption : replacing x^3 by x^s where $s = (2^{n+1} - 1)/3$

$$R := \lceil n \log_3 2 \rceil .$$

n	129	255	769	1025
R	82	161	486	647

Number of rounds for MiMC.



Algebraic degree - 1st definition

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

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

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

Definition

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

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

Algebraic degree - 1st definition

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

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

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

Definition

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

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

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

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

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

Algebraic degree - 1st definition

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

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

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

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

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

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

Algebraic degree - 2nd definition

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

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

Definition

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

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

Algebraic degree - 2nd definition

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

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

Definition

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

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

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

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

Integral attack

Exploiting a low algebraic degree

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

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

Random permutation: degree $= n - 1$

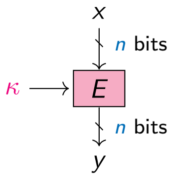
Integral attack

Exploiting a low algebraic degree

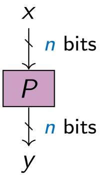
For any affine subspace $\mathcal{V} \subset \mathbb{F}_2^n$ with $\dim \mathcal{V} \geq \deg^a(F) + 1$, we have a 0-sum distinguisher:

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

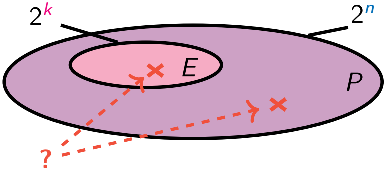
Random permutation: degree $= n - 1$



Block cipher



Random permutation



First Plateau

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

For r rounds:

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

First Plateau

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

For r rounds:

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

- ⋆ Round 1: $B_3^1 = 2$

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

$$3 = [11]_2$$

First Plateau

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

For r rounds:

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

Definition

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

- ⋆ Round 1: $B_3^1 = 2$

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

$$3 = [11]_2$$

- ⋆ Round 2: $B_3^2 = 2$

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

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

First Plateau

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

For r rounds:

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

⋆ Round 1: $B_3^1 = 2$

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

$$3 = [11]_2$$

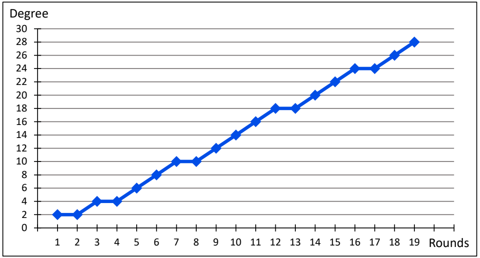
⋆ Round 2: $B_3^2 = 2$

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

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

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

Definition

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

- ⋆ Round 1: $B_3^1 = 2$

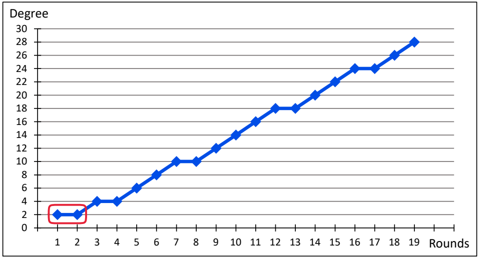
$$\mathcal{P}_1(x) = x^3, \quad (c_0 = 0)$$

$$3 = [11]_2$$

- ⋆ 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: $B_3^1 = 2$

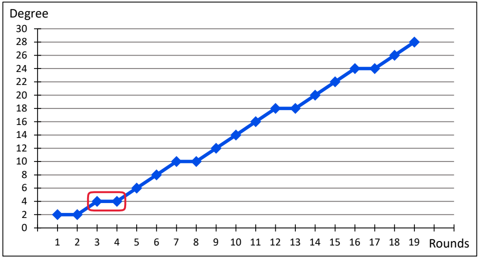
$$\mathcal{P}_1(x) = x^3, \quad (c_0 = 0)$$

$$3 = [11]_2$$

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

Definition

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

⋆ Round 1: $B_3^1 = 2$

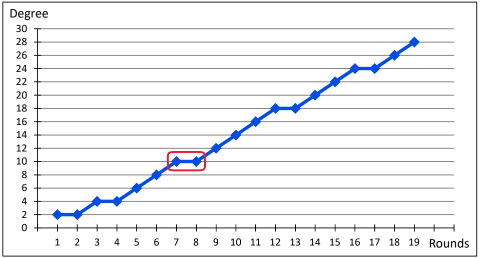
$$\mathcal{P}_1(x) = x^3, \quad (c_0 = 0)$$

$$3 = [11]_2$$

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

⋆ Round 1: $B_3^1 = 2$

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

$$3 = [11]_2$$

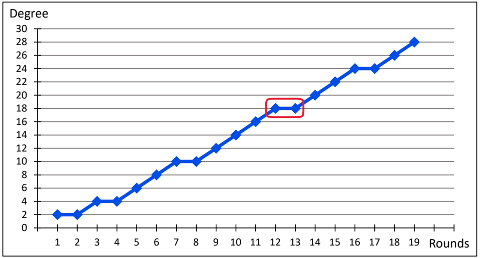
⋆ Round 2: $B_3^2 = 2$

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

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

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

Definition

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

⋆ Round 1: $B_3^1 = 2$

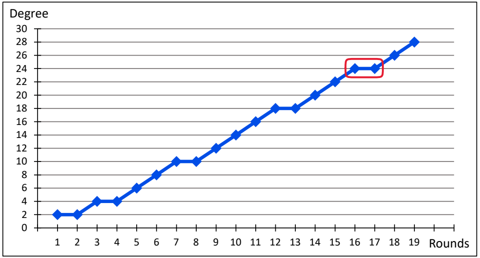
$$\mathcal{P}_1(x) = x^3, \quad (c_0 = 0)$$

$$3 = [11]_2$$

⋆ Round 2: $B_3^2 = 2$

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

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



Algebraic degree observed for $n = 31$.

An upper bound

Proposition

Set of exponents that might appear in the polynomial:

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

An upper bound

Proposition

Set of exponents that might appear in the polynomial:

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

Example:

$$\mathcal{P}_1(x) = x^3 \quad \Rightarrow \quad \mathcal{E}_1 = \{3\}\ .$$

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

$$\mathcal{E}_2 = \{0, 3, 6, 9\}\ ,$$

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

An upper bound

Proposition

Set of exponents that might appear in the polynomial:

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

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

$\mathcal{E}_r \subseteq \{$

0	3	6	9	12	~~15~~	18	~~21~~
24	27	30	33	36	~~39~~	42	~~45~~
48	51	54	57	60	~~63~~	66	~~69~~

$\ldots \quad 3^r\}$

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

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

Bounding the degree

Theorem

After r rounds of MiMC, the algebraic degree is

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

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

$$B_3^r \geq \max\{wt(3^i), i \leq r\}$$

Bounding the degree

Theorem

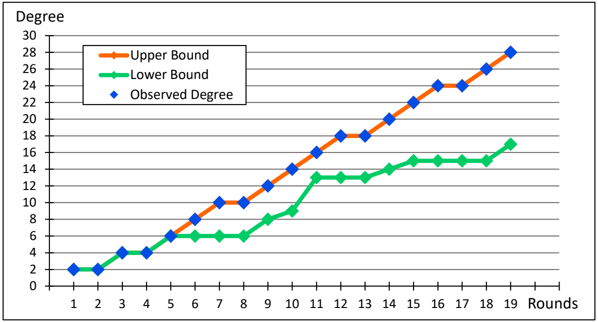
After r rounds of MiMC, the algebraic degree is

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

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

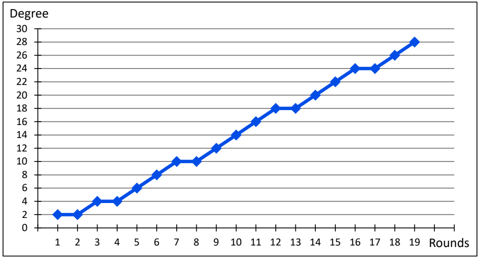
$$B_3^r \geq \max\{wt(3^i), i \leq r\}$$

Upper bound reached for $\sim$ 16265 rounds



Plateau

$\Rightarrow$ plateau when $\lfloor r \log_2 3 \rfloor = 1 \bmod 2$ and $\lfloor (r+1) \log_2 3 \rfloor = 0 \bmod 2$



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 $(\lfloor r \log_2 3 \rfloor)_{r>0}$:

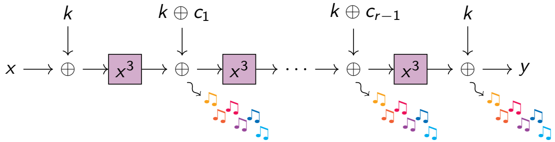
$$\Rightarrow \text{denominators of semiconvergents of } \log_2(3) \simeq 1.5849625$$

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

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

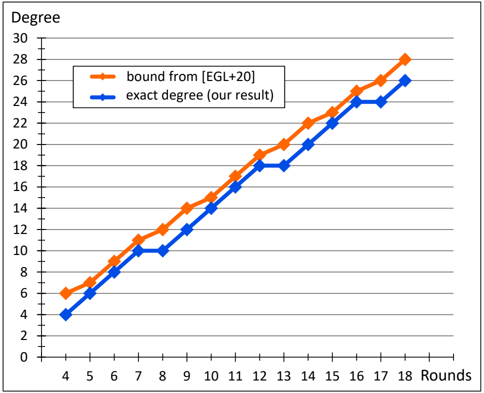
- **Music theory:**
  - perfect octave 2:1
  - perfect fifth 3:2

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



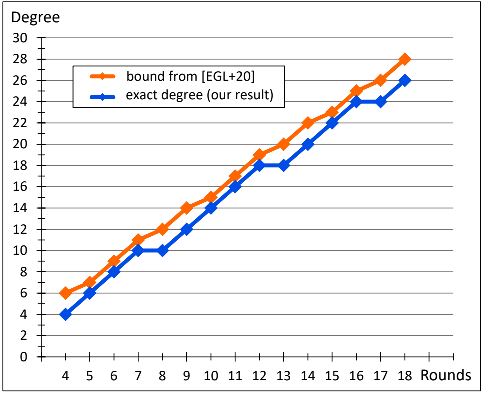
Comparison to previous work

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 $n = 129$, $\text{MIMC}_3 = 82$ rounds

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

Secret-key distinguishers ($n = 129$)

Take-Away

Algebraic Degree of MiMC

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

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

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

Joint work with Anne Canteaut and Léo Perrin

Published in Designs, Codes and Cryptography (2023)

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

Why Anemoi?

- **Anemoi**
  Family of ZK-friendly Hash functions

Why Anemoi?

- Anemoi
  Family of ZK-friendly Hash functions

  ⇓

- Anemoi
  Greek gods of winds

Our approach

Need: verification using few multiplications.

Our approach

Need: verification using few multiplications.

First approach: evaluation also using few multiplications.

$y \leftarrow E(x)$ $\rightsquigarrow$ E: low degree

$y == E(x)$ $\rightsquigarrow$ E: low degree

Our approach

Need: verification using few multiplications.

First approach: evaluation also using few multiplications.

$\boxed{y \leftarrow E(x)}$ $\rightsquigarrow$ E: low degree

$\boxed{y == E(x)}$ $\rightsquigarrow$ E: low degree

$\Rightarrow$ vulnerability to some attacks?

Our approach

Need: verification using few multiplications.

First approach: evaluation also using few multiplications.

$y \leftarrow E(x)$ $\rightsquigarrow E$: low degree

$y == E(x)$ $\rightsquigarrow E$: low degree

$\Rightarrow$ vulnerability to some attacks?

New approach:

using CCZ-equivalence

Our vision

A function is arithmetization-oriented if it is **CCZ-equivalent** to a function that can be verified efficiently.

Our approach

Need: verification using few multiplications.

First approach: evaluation also using few multiplications.

$y \leftarrow E(x)$ $\rightsquigarrow$ E: low degree

$y == E(x)$ $\rightsquigarrow$ E: low degree

$\Rightarrow$ vulnerability to some attacks?

New approach:

using CCZ-equivalence

Our vision

A function is arithmetization-oriented if it is **CCZ-equivalent** to a function that can be verified efficiently.

$y \leftarrow F(x)$ $\rightsquigarrow$ F: high degree

$v == G(u)$ $\rightsquigarrow$ G: low degree

CCZ-equivalence

Definition [Carlet, Charpin, Zinoviev, DCC98]

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

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

where $\mathcal{A}$ is an affine permutation, $\mathcal{A}(x) = \mathcal{L}(x) + c$.

CCZ-equivalence

Definition [Carlet, Charpin, Zinoviev, DCC98]

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

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

where $\mathcal{A}$ is an affine permutation, $\mathcal{A}(x) = \mathcal{L}(x) + c$.

- ⋆ F and G have the same differential properties: $\delta_F = \delta_G$.

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

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

CCZ-equivalence

Definition [Carlet, Charpin, Zinoviev, DCC98]

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

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

where $\mathcal{A}$ is an affine permutation, $\mathcal{A}(x) = \mathcal{L}(x) + c$.

- ⋆ F and G have the same differential properties: $\delta_F = \delta_G$.
- ⋆ F and G have the same linear properties: $\mathcal{W}_F = \mathcal{W}_G$.

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

$$\text{in } \mathbb{F}_{2^n} : \mathcal{W}_F = \max_{a,b \neq 0} \left| \sum_{x \in \mathbb{F}_{2^n}^m} (-1)^{a \cdot x + b \cdot F(x)} \right| \qquad \text{in } \mathbb{F}_p : \mathcal{W}_F = \max_{a,b \neq 0} \left| \sum_{x \in \mathbb{F}_p^m} exp\left(\frac{2\pi i (\langle a, x\rangle - \langle b, F(x)\rangle)}{p} \right) \right|$$

CCZ-equivalence

Definition [Carlet, Charpin, Zinoviev, DCC98]

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

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

where $\mathcal{A}$ is an affine permutation, $\mathcal{A}(x) = \mathcal{L}(x) + c$.

- ⋆ F and G have the same differential properties: $\delta_F = \delta_G$.
- ⋆ F and G have the same linear properties: $\mathcal{W}_F = \mathcal{W}_G$.
- ⋆ Verification is the same: if $y \leftarrow F(x)$, $v \leftarrow G(u)$

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

CCZ-equivalence

Definition [Carlet, Charpin, Zinoviev, DCC98]

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

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

where $\mathcal{A}$ is an affine permutation, $\mathcal{A}(x) = \mathcal{L}(x) + c$.

- ⋆ F and G have the same differential properties: $\delta_F = \delta_G$.
- ⋆ F and G have the same linear properties: $\mathcal{W}_F = \mathcal{W}_G$.
- ⋆ Verification is the same: if $y \leftarrow F(x)$, $v \leftarrow G(u)$

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

- ⋆ The degree is not preserved.

CCZ-equivalence

Definition [Carlet, Charpin, Zinoviev, DCC98]

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

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

where $\mathcal{A}$ is an affine permutation, $\mathcal{A}(x) = \mathcal{L}(x) + c$.

- ⋆ F and G have the same differential properties: $\delta_F = \delta_G$.
- ⋆ F and G have the same linear properties: $\mathcal{W}_F = \mathcal{W}_G$.
- ⋆ Verification is the same: if $y \leftarrow F(x)$, $v \leftarrow G(u)$

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

- ⋆ The degree is not preserved.

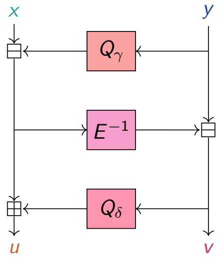
The Flystel

Butterfly + Feistel ⇒ Flystel

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

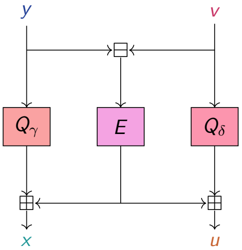
Open Flystel $\mathcal{H}$.

High-degree permutation



Closed Flystel $\mathcal{V}$.

Low-degree function



$$\begin{cases} u &= x - Q_\gamma(y) + Q_\delta(E^{-1}(x - Q_\gamma(y)) - y) \\ y &= E^{-1}(x - Q_\gamma(y)) - y \end{cases}$$

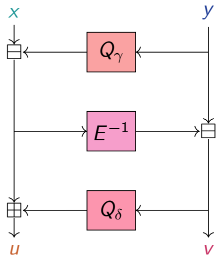
$$\begin{cases} x &= Q_\gamma(y) + E(y - v) \\ u &= Q_\delta(v) + E(y - v) \end{cases}$$

The Flystel

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

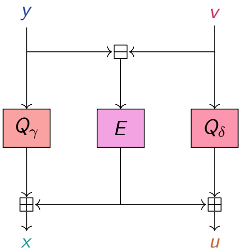
Open Flystel $\mathcal{H}$.

High-degree permutation



Closed Flystel $\mathcal{V}$.

Low-degree function



$$\begin{cases} u &= x - Q_\gamma(y) + Q_\delta(E^{-1}(x - Q_\gamma(y)) - y) \\ y &= E^{-1}(x - Q_\gamma(y)) - y \end{cases}$$

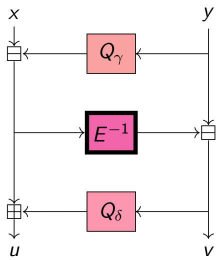
$$\begin{cases} x &= Q_\gamma(y) + E(y - v) \\ u &= Q_\delta(v) + E(y - v) \end{cases}$$

Advantage of CCZ-equivalence

⋆ High Degree Evaluation.

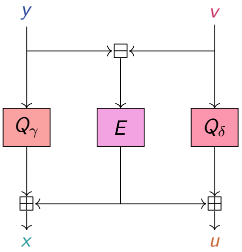
Open Flystel $\mathcal{H}$.

High-degree permutation



Closed Flystel $\mathcal{V}$.

Low-degree function



$$\begin{cases} u &= x - Q_\gamma(y) + Q_\delta(E^{-1}(x - Q_\gamma(y)) - y) \\ y &= E^{-1}(x - Q_\gamma(y)) - y \end{cases}$$

$$\begin{cases} x &= Q_\gamma(y) + E(y - v) \\ u &= Q_\delta(v) + E(y - v) \end{cases}$$

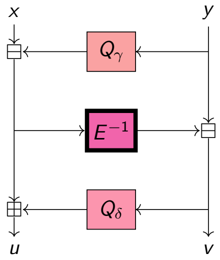
Advantage of CCZ-equivalence

⋆ High Degree Evaluation.

$$\begin{cases} p & = 40024095552216673934177898257359041565568828199390078853320581361240316504908378644426876291290156640378942725597 87 \\ \alpha & = 5 \\ \alpha^{-1} & = 32019276441773339147342318605887233252455062559512063082656465088992253203926702915541501033032125312303154180478 29 \end{cases}$$

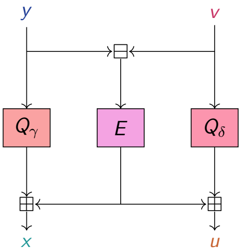
Open `Flystel` $\mathcal{H}$.

High-degree permutation



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

Low-degree function



$$\begin{cases} u & = x - Q_\gamma(y) + Q_\delta(E^{-1}(x - Q_\gamma(y)) - y) \\ y & = E^{-1}(x - Q_\gamma(y)) - y \end{cases}$$

$$\begin{cases} x & = Q_\gamma(y) + E(y - v) \\ u & = Q_\delta(v) + E(y - v) \end{cases}$$

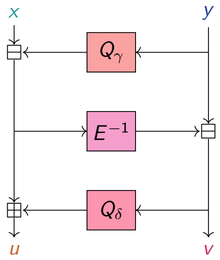
Advantage of CCZ-equivalence

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

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

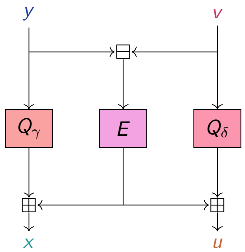
Open `Flystel` $\mathcal{H}$.

High-degree permutation



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

Low-degree function



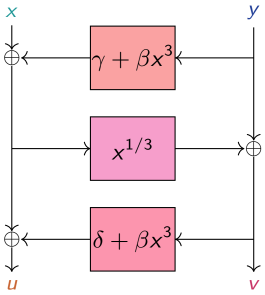
$$\begin{cases} u &= x - Q_\gamma(y) + Q_\delta(E^{-1}(x - Q_\gamma(y)) - y) \\ y &= E^{-1}(x - Q_\gamma(y)) - y \end{cases}$$

$$\begin{cases} x &= Q_\gamma(y) + E(y - v) \\ u &= Q_\delta(v) + E(y - v) \end{cases}$$

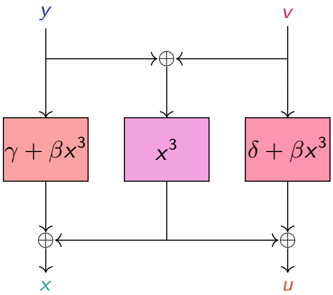
Flystel in $\mathbb{F}_{2^n}$

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

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

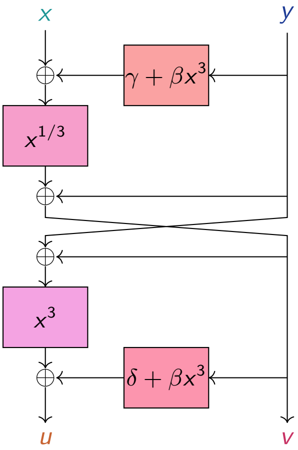


Open `Flystel`$_2$.



Closed `Flystel`$_2$.

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



Degenerated Butterfly.

First introduced by [Perrin et al. 2016].

Well-studied butterfly.

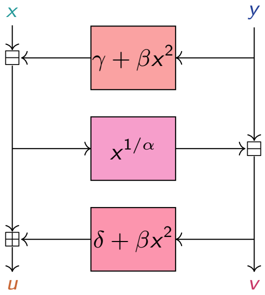
Theorems in [Li et al. 2018] state that if $\beta \neq 0$:

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

Flystel in $\mathbb{F}_p$

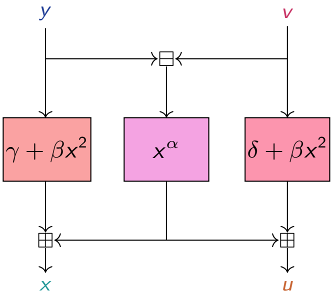
$$\mathcal{H}: \begin{cases} \mathbb{F}_p \times \mathbb{F}_p & \to \mathbb{F}_p \times \mathbb{F}_p \\ (x,y) & \mapsto \left(x - \beta y^2 - \gamma + \beta\left(y - (x - \beta y^2 - \gamma)^{1/\alpha}\right)^2 + \delta\right., \\ & \qquad \left. y - (x - \beta y^2 - \gamma)^{1/\alpha}\right) . \end{cases}$$

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



Open $\texttt{Flystel}_p$.

usually
$\alpha = 3$ or 5.



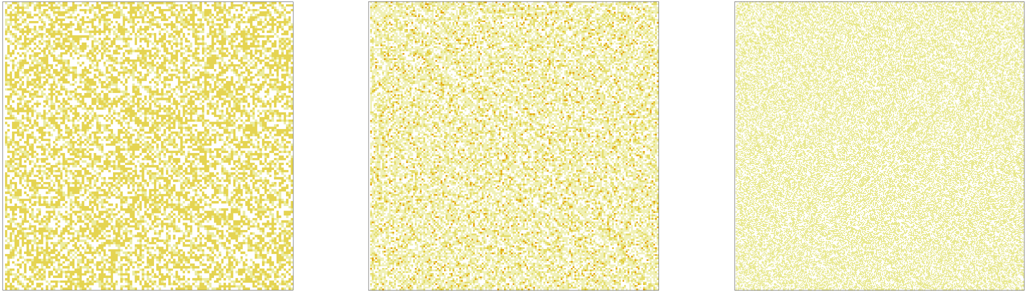
Closed $\texttt{Flystel}_p$.

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

- Differential properties

  $\texttt{Flystel}_\texttt{p}$ has a differential uniformity:

$$\delta_{\mathcal{H}} = \max_{a \neq 0, b} \left| \{ x \in \mathbb{F}_p^2, \mathcal{H}(x+a) - \mathcal{H}(x) = b \} \right| = \alpha - 1$$



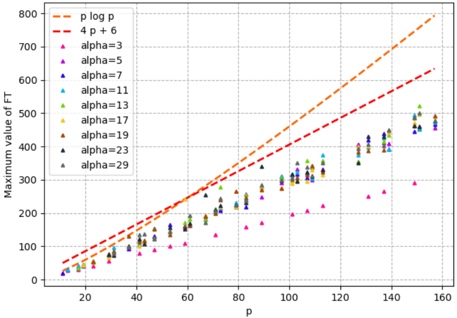
(a) *when $p = 11$ and $\alpha = 3$.* **(b)** *when $p = 13$ and $\alpha = 5$.* **(c)** *when $p = 17$ and $\alpha = 3$.*

DDT of $\texttt{Flystel}_\texttt{p}$.

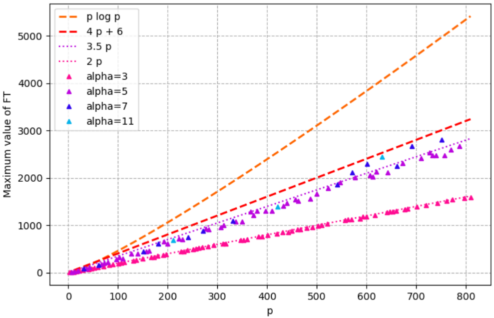
Properties of Flystel in $\mathbb{F}_p$

- Linear properties

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



(a) *For different α.*



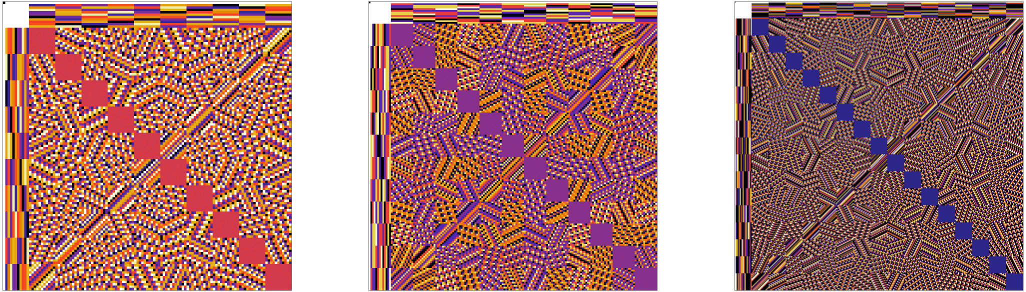
(b) *For the smallest α.*

Conjecture for the linearity.

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

- Linear properties

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



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

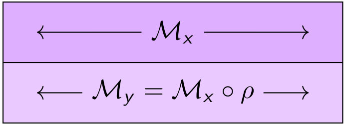
LAT of $\texttt{Flystel}_p$.

The SPN Structure

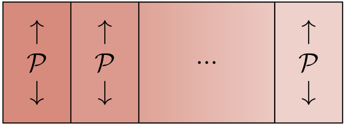
The internal state of Anemoi and its basic operations.

x_0	x_1	$\cdots$	$x_{\ell-1}$
y_0	y_1	$\cdots$	$y_{\ell-1}$

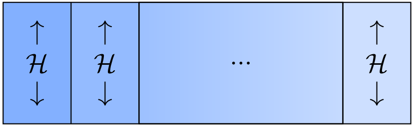
(a) *Internal state*



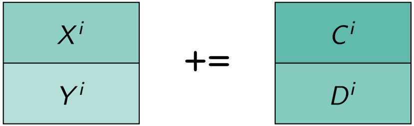
(b) *The diffusion layer $\mathcal{M}$.*



(c) *The PHT $\mathcal{P}$.*

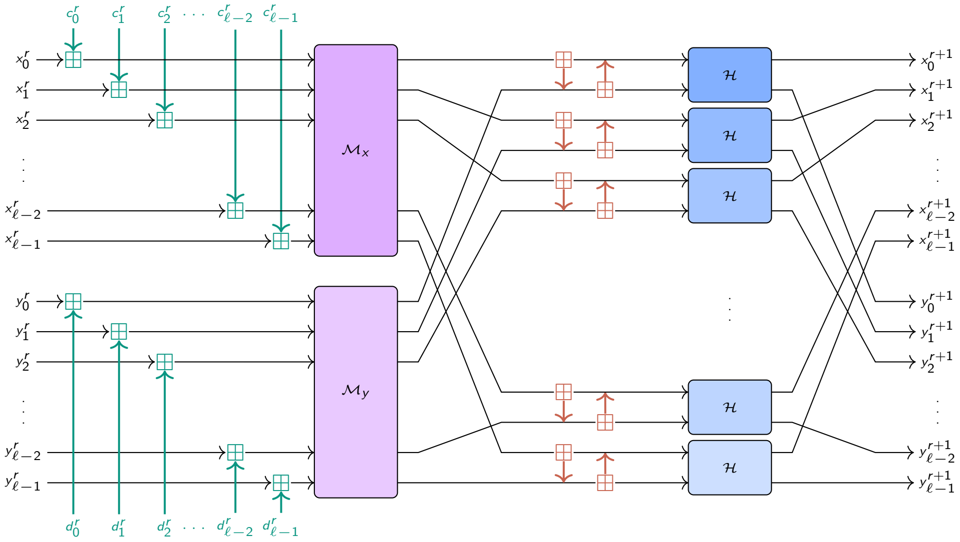


(d) *The S-box layer $\mathcal{S}$.*



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

The SPN Structure



Number of rounds

$$\texttt{Anemoi}_{q,\alpha,\ell} = \mathcal{M} \circ \mathrm{R}_{n_r-1} \circ \ldots \circ \mathrm{R}_0$$

⇒ Choosing the number of rounds:

$$n_r \geq \max\left\{ 8 \ , \ \underbrace{\min(5, 1+\ell)}_{\text{security margin}} + \underbrace{2 + \min\left\{ r \in \mathbb{N} \ \middle| \ \binom{4\ell r + \kappa_\alpha}{2\ell r}^2 \geq 2^s \right\}}_{\text{to prevent algebraic attacks}} \right\} .$$

α (κ_α)	3 (1)	5 (2)	7 (4)	11 (9)
$\ell = 1$	21	21	20	19
$\ell = 2$	14	14	13	13
$\ell = 3$	12	12	12	11
$\ell = 4$	12	12	11	11

Number of Rounds of Anemoi ($s = 128$).

Some Benchmarks

	m	RP	Poseidon	Griffin	Anemoi
R1CS	2	208	198	-	**76**
	4	224	232	112	**96**
	6	216	264	-	**120**
	8	256	296	176	**160**
Plonk	2	312	380	-	**189**
	4	560	1336	**260**	308
	6	756	3024	-	**444**
	8	1152	5448	**574**	624
AIR	2	156	300	-	**126**
	4	**168**	348	**168**	**168**
	6	**162**	396	-	216
	8	**192**	480	264	288

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

	m	RP	Poseidon	Griffin	Anemoi
R1CS	2	240	216	-	**95**
	4	264	264	**110**	120
	6	288	315	-	**150**
	8	384	363	**162**	200
Plonk	2	320	344	-	**210**
	4	528	1032	**222**	336
	6	768	2265	-	**480**
	8	1280	4003	**492**	672
AIR	2	**200**	360	-	210
	4	**220**	440	**220**	280
	6	**240**	540	-	360
	8	**320**	640	360	480

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

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

for standard arithmetization, without optimization.

Take-Away

Anemoi

- A new family of ZK-friendly hash functions
- Contributions of fundamental interest:
  - New S-box: Flystel
- Identify a link between AO and CCZ-equivalence

Joint work with Pierre Briaud, Pyrros Chaidos, Léo Perrin, Robin Salen, Vesselin Velichkov and Danny Willems

To appear in CRYPTO 2023

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

Conclusions

- A better understanding of the algebraic degree of MIMC_3
  - More details on eprint.iacr.org/2022/366
- Anemoi: a new family of ZK-friendly hash functions
  - More details on eprint.iacr.org/2022/840

Conclusions

- ⋆ A better understanding of the algebraic degree of MIMC_3
  - ☞ More details on eprint.iacr.org/2022/366
- ⋆ Anemoi: a new family of ZK-friendly hash functions
  - ☞ More details on eprint.iacr.org/2022/840

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

Thanks for your attention!

Exact degree

Maximum-weight exponents:

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

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

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

Example:

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

Exact degree

Maximum-weight exponents:

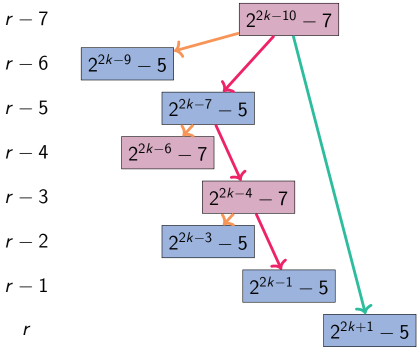
Let $k_r = \lfloor \log_2 3^r \rfloor$.

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

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

Example:

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



Constructing exponents.

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

Exact degree

Maximum-weight exponents:

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

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

- if $k_r = 1 \mod 2$,

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

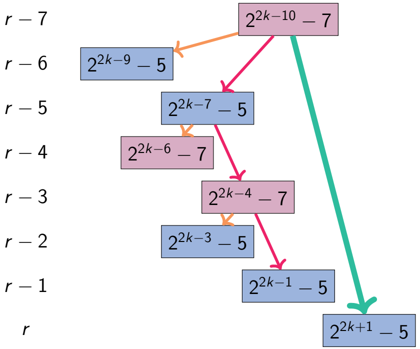
- if $k_r = 0 \mod 2$,

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

Example:

$$123 = 2^7 - 5 = 2^{k_5} - 5 \quad \in \mathcal{E}_5,$$

$$4089 = 2^{12} - 7 = 2^{k_8} - 7 \quad \in \mathcal{E}_8.$$



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:

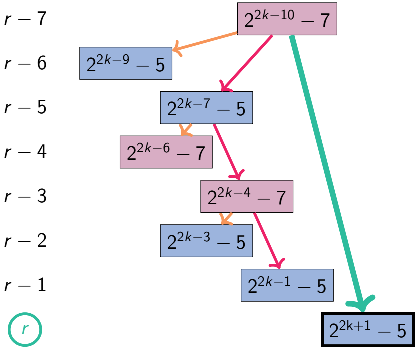
Let $k_r = \lfloor \log_2 3^r \rfloor$.

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

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

Example:

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



Constructing exponents.

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

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 $k_r = 1 \bmod 2$,

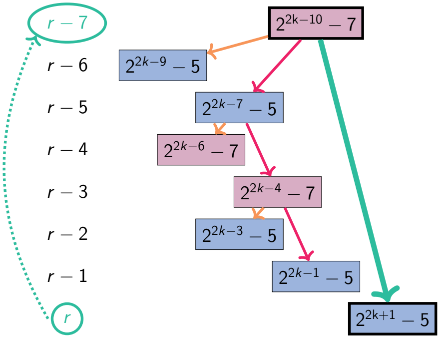
$$\omega_r = 2^{k_r} - 5 \in \mathcal{E}_r,$$

- if $k_r = 0 \bmod 2$,

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

Example:

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



Constructing exponents.

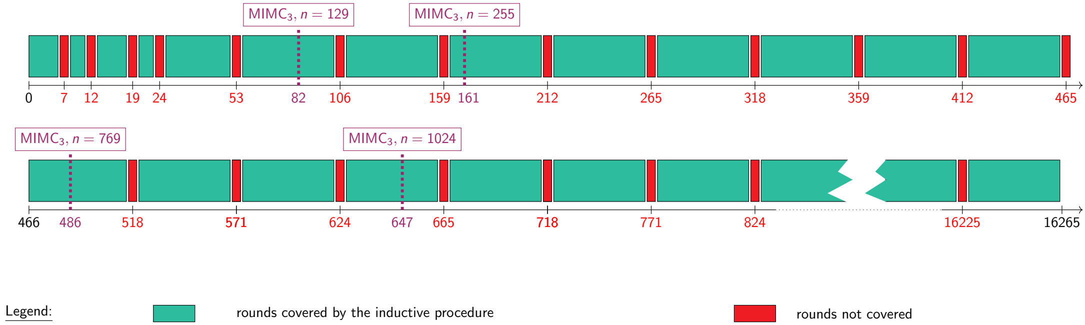
$$\exists \ell \text{ s.t. } \quad \omega_{r-\ell} \in \mathcal{E}_{r-\ell} \Rightarrow \omega_r \in \mathcal{E}_r$$

Covered rounds

Idea of the proof:

- ⋆ inductive proof: existence of “good” ℓ

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

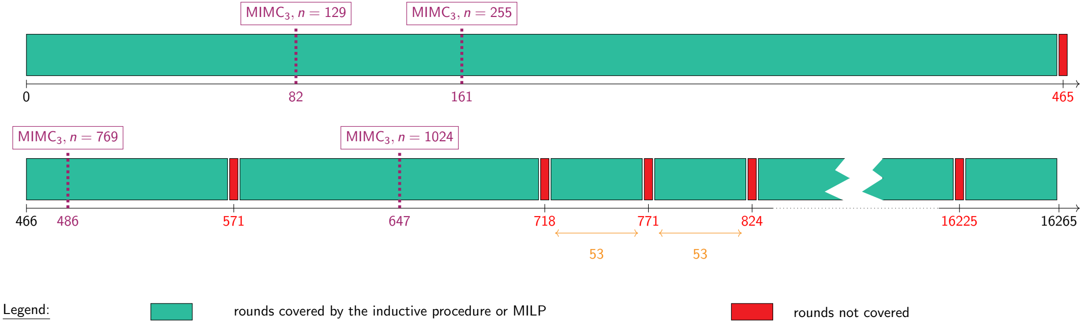


Covered rounds

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.



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 $\omega_r \in \mathcal{E}_r$.

MILP Solver

Let

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

and

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

So that:

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

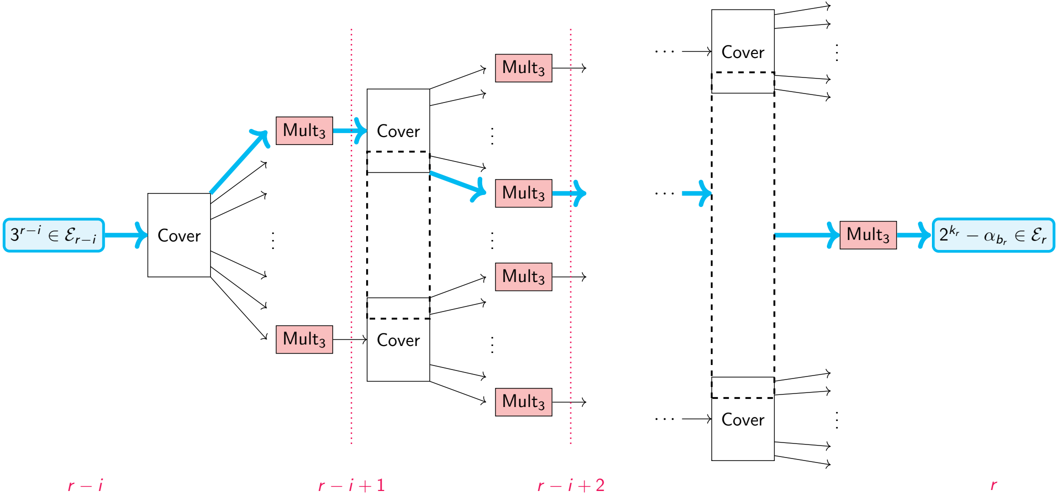
$\Rightarrow$ MILP problem solved using PySCIPOpt

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

With $\ell = 1$:

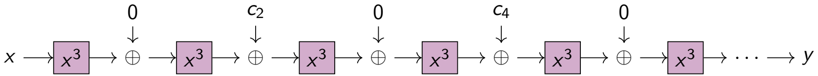
$$3^{r-1} \in \mathcal{E}_{r-1} \longrightarrow \boxed{\mathsf{Cover}} \longrightarrow \boxed{\mathsf{Mult}_3} \longrightarrow 2^{k_r} - \alpha_{b_r} \in \mathcal{E}_r$$

MILP Solver (i rounds)

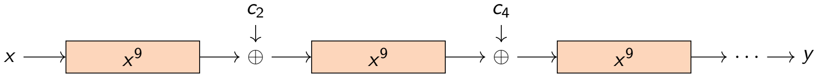


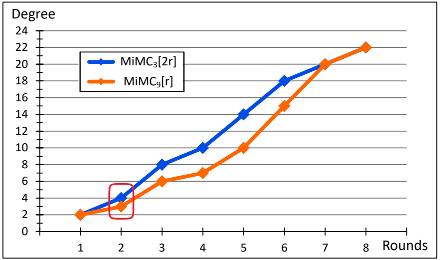
MiMC_9 and form of coefficients

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



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





Example: coefficients of maximum weight exponent monomials at round 4

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

$30 : c_1^{17}$

$51 : c_1^{10}$

$54 : c_1^9 + c_3$

$57 : c_1^8$

$75 : c_1^2$

$78 : c_1$

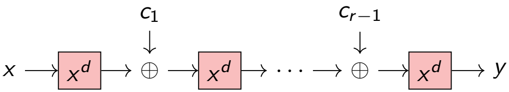
Other Quadratic functions

Proposition

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

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

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



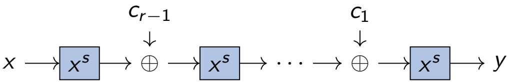
Proposition

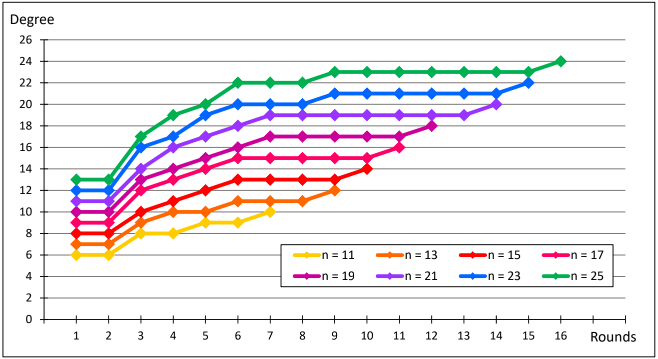
Let $\mathcal{E}_r$ be the set of exponents in the univariate form of $\mathrm{MIMC}_d[r]$, where $d = 2^j + 1$. Then:

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

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 $wt(i) \geq 2$:

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

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

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

Affine-equivalence

Definition

$F : \mathbb{F}_q \rightarrow \mathbb{F}_q$ and $G : \mathbb{F}_q \rightarrow \mathbb{F}_q$ are **affine equivalent** if

$$F(x) = (B \circ G \circ A)(x) \ ,$$

where A, B are affine permutations.

Definition

$F : \mathbb{F}_q \rightarrow \mathbb{F}_q$ and $G : \mathbb{F}_q \rightarrow \mathbb{F}_q$ are **extended affine equivalent** if

$$F(x) = (B \circ G \circ A)(x) + C(x) \ ,$$

where A, B, C are affine functions with A, B permutations s.t.

$$\Gamma_F = \{ (x, F(x)) \mid x \in \mathbb{F}_q \} = \begin{pmatrix} A^{-1} & 0 \\ CA^{-1} & B \end{pmatrix} \{ (x, G(x)) \mid x \in \mathbb{F}_q \} \ ,$$

CCZ-equivalence

Definition

$F : \mathbb{F}_q \rightarrow \mathbb{F}_q$ and $G : \mathbb{F}_q \rightarrow \mathbb{F}_q$ are **extended affine equivalent** if

$$\Gamma_F = \left\{ (x, F(x)) \mid x \in \mathbb{F}_q \right\} = \begin{pmatrix} A^{-1} & 0 \\ CA^{-1} & B \end{pmatrix} \left\{ (x, G(x)) \mid x \in \mathbb{F}_q \right\},$$

CCZ-equivalence

Definition

$F : \mathbb{F}_q \to \mathbb{F}_q$ and $G : \mathbb{F}_q \to \mathbb{F}_q$ are **extended affine equivalent** if

$$\Gamma_F = \left\{ (x, F(x)) \mid x \in \mathbb{F}_q \right\} = \begin{pmatrix} A^{-1} & 0 \\ CA^{-1} & B \end{pmatrix} \left\{ (x, G(x)) \mid x \in \mathbb{F}_q \right\} ,$$

Definition [Carlet, Charpin, Zinoviev, DCC98]

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

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

where $\mathcal{A}$ is an affine permutation, $\mathcal{A}(x) = \mathcal{L}(x) + c$.

CCZ-equivalence

Definition

$F : \mathbb{F}_q \rightarrow \mathbb{F}_q$ and $G : \mathbb{F}_q \rightarrow \mathbb{F}_q$ are **extended affine equivalent** if

$$\Gamma_F = \{ (x, F(x)) \mid x \in \mathbb{F}_q \} = \begin{pmatrix} A^{-1} & 0 \\ CA^{-1} & B \end{pmatrix} \{ (x, G(x)) \mid x \in \mathbb{F}_q \} ,$$

Definition [Carlet, Charpin, Zinoviev, DCC98]

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

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

where $\mathcal{A}$ is an affine permutation, $\mathcal{A}(x) = \mathcal{L}(x) + c$.

- ⋆ EA-equivalence and CCZ-equivalence preserve differential and linear properties,

$$\delta_G(a, b) = \delta_F(\mathcal{L}^{-1}(a, b)) \quad \text{and} \quad \mathcal{W}_G(\alpha, \beta) = (-1)^{c \cdot (\alpha, \beta)} \mathcal{W}_F(\mathcal{L}^T(\alpha, \beta))$$

- ⋆ EA-equivalence preserves the degree BUT CCZ-equivalence does not!

CCZ-equivalence

Definition

$F : \mathbb{F}_q \to \mathbb{F}_q$ and $G : \mathbb{F}_q \to \mathbb{F}_q$ are **extended affine equivalent** if

$$\Gamma_F = \{ (x, F(x)) \mid x \in \mathbb{F}_q \} = \begin{pmatrix} A^{-1} & 0 \\ CA^{-1} & B \end{pmatrix} \{ (x, G(x)) \mid x \in \mathbb{F}_q \} ,$$

Definition [Carlet, Charpin, Zinoviev, DCC98]

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

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

where $\mathcal{A}$ is an affine permutation, $\mathcal{A}(x) = \mathcal{L}(x) + c$.

- ⋆ EA-equivalence and CCZ-equivalence preserve differential and linear properties,

$$\delta_G(a, b) = \delta_F(\mathcal{L}^{-1}(a, b)) \quad \text{and} \quad \mathcal{W}_G(\alpha, \beta) = (-1)^{c \cdot (\alpha, \beta)} \mathcal{W}_F(\mathcal{L}^T(\alpha, \beta))$$

- ⋆ EA-equivalence preserves the degree BUT CCZ-equivalence does not!

$\Rightarrow$ **Can we get CCZ-equivalence from EA-equivalence?**

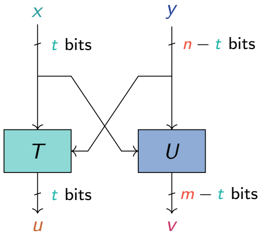
Twist

Using isomorphisms $\mathbb{F}_2^n \simeq \mathbb{F}_2^t \times \mathbb{F}_2^{n-t}$ and $\mathbb{F}_2^m \simeq \mathbb{F}_2^t \times \mathbb{F}_2^{m-t}$:

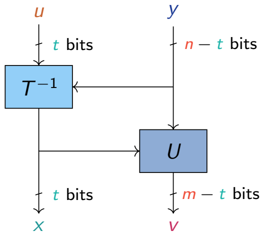
Definition

$F : \mathbb{F}_2^t \times \mathbb{F}_2^{n-t} \rightarrow \mathbb{F}_2^t \times \mathbb{F}_2^{m-t}$ and $G : \mathbb{F}_2^t \times \mathbb{F}_2^{n-t} \rightarrow \mathbb{F}_2^t \times \mathbb{F}_2^{m-t}$ are t-**twist-equivalent** if T_y is a permutation for all y and

$$G(u, y) = (T_y^{-1}(u), U_{T_y^{-1}(u)}(y)) .$$



t-twist
$\Longleftrightarrow$



$\Gamma_F = \{(x, F(x)) \mid x \in \mathbb{F}_2^n\}$

swap matrix M_t
$\Longleftrightarrow$

$\Gamma_G = \{(x, G(x)) \mid x \in \mathbb{F}_2^n\}$

CCZ = EA + twist

Theorem [Canteaut, Perrin, FFA19]

Let $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ and $G : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ be two CCZ-equivalent functions. We can obtain G from F or F from G by composing:

$$\text{EA transformation} + t\text{-twist} + \text{EA transformation} .$$

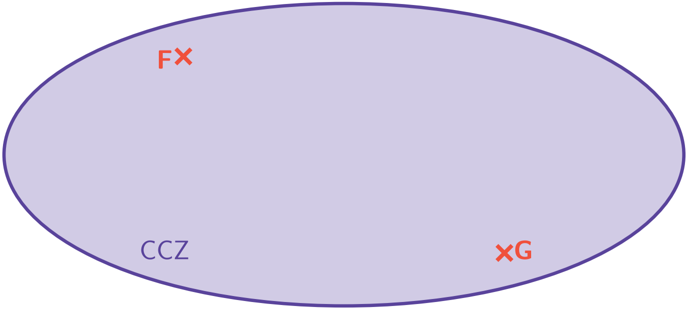
$$\Gamma_F = \mathcal{A}(\Gamma_G) ,$$

with $\mathcal{A}$ affine permutation.

$$\Downarrow$$

$$\Gamma_F = (A \cdot M_t \cdot B)(\Gamma_G) ,$$

with M_t swap matrix and A, B EA-mappings.



CCZ = EA + twist

Theorem [Canteaut, Perrin, FFA19]

Let $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ and $G : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ be two CCZ-equivalent functions. We can obtain G from F or F from G by composing:

$$\text{EA transformation} + t\text{-twist} + \text{EA transformation} .$$

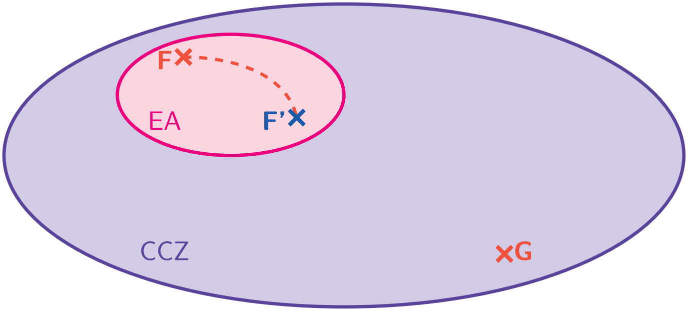
$$\Gamma_F = \mathcal{A}(\Gamma_G) ,$$

with $\mathcal{A}$ affine permutation.

$$\Downarrow$$

$$\Gamma_F = (A \cdot M_t \cdot B)(\Gamma_G) ,$$

with M_t swap matrix and A, B EA-mappings.



CCZ = EA + twist

Theorem [Canteaut, Perrin, FFA19]

Let $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ and $G : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ be two CCZ-equivalent functions. We can obtain G from F or F from G by composing:

$$\text{EA transformation} + t\text{-twist} + \text{EA transformation} .$$

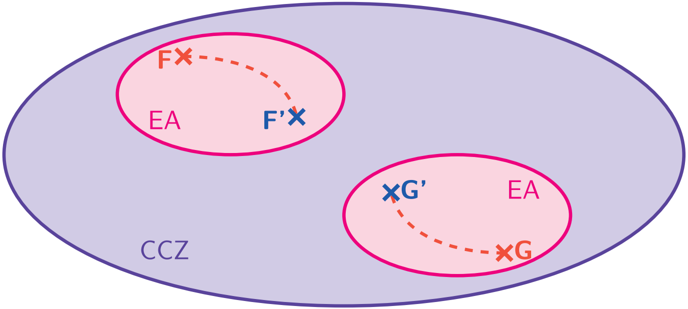
$$\Gamma_F = \mathcal{A}(\Gamma_G) ,$$

with $\mathcal{A}$ affine permutation.

$$\Downarrow$$

$$\Gamma_F = (A \cdot M_t \cdot B)(\Gamma_G) ,$$

with M_t swap matrix and A, B EA-mappings.



CCZ = EA + twist

Theorem [Canteaut, Perrin, FFA19]

Let $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ and $G : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ be two CCZ-equivalent functions. We can obtain G from F or F from G by composing:

$$\text{EA transformation} + t\text{-twist} + \text{EA transformation} .$$

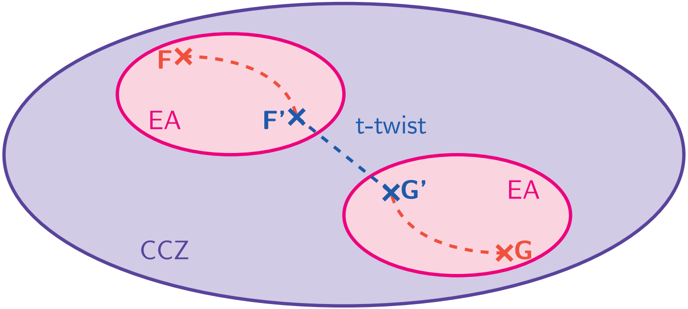
$$\Gamma_F = \mathcal{A}(\Gamma_G) ,$$

with $\mathcal{A}$ affine permutation.

$$\Downarrow$$

$$\Gamma_F = (A \cdot M_t \cdot B)(\Gamma_G) ,$$

with M_t swap matrix and A, B EA-mappings.

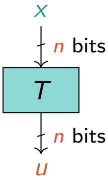


Example: Inverse

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

$$\Gamma_F = \{ (x, F(x)) \mid x \in \mathbb{F}_{2^n} \} \quad \text{and} \quad \Gamma_{F^{-1}} = \{ (y, F^{-1}(y)) \mid y \in \mathbb{F}_{2^n} \} = \{ (F(x), x) \mid x \in \mathbb{F}_{2^n} \} .$$

$$\begin{pmatrix} x \\ F(x) \end{pmatrix} = \begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix} \begin{pmatrix} F(x) \\ x \end{pmatrix} \quad \Rightarrow \quad \text{swap matrix } M_n = \begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix} .$$

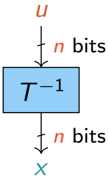


F

n-twist

$\Longleftrightarrow$

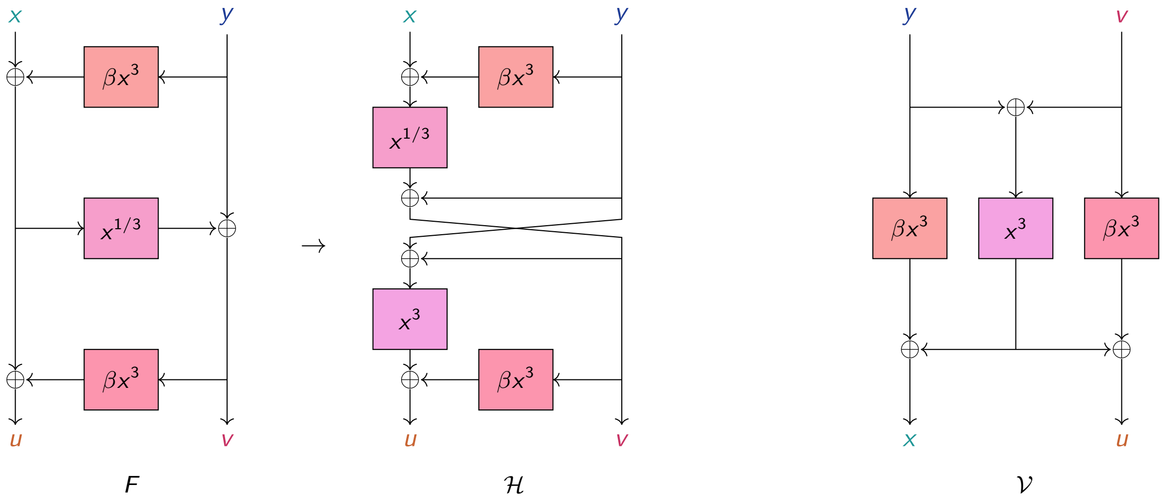
$(n = t)$



F^{-1}

$\Rightarrow$ F and F^{-1} are CCZ-equivalent and the degree is indeed not preserved.

Example: Butterfly [PUB16]



Example: Butterfly [PUB16]