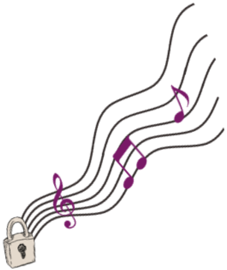
On the new generation of symmetric primitives: the AOP (Arithmetization-Oriented Primitives)



Clémence Bouvier

Seminar ECO, Montpellier
March 15th, 2024

RUHR UNIVERSITÄT BOCHUM RUB

Toy example of Zero-Knowledge Proof

	2		5		1		9	
8			2		3			6
	3			6			7	
		1				6		
5	4						1	9
		2				7		
	9			3			8	
2			8		4			7
	1		9		7		6	

Unsolved Sudoku

Toy example of Zero-Knowledge Proof

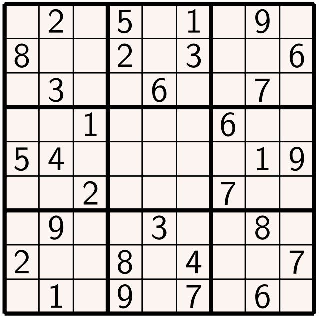
	2		5		1		9	
8			2		3			6
	3			6			7	
		1				6		
5	4						1	9
		2				7		
	9			3			8	
2			8		4			7
	1		9		7		6	

Unsolved Sudoku

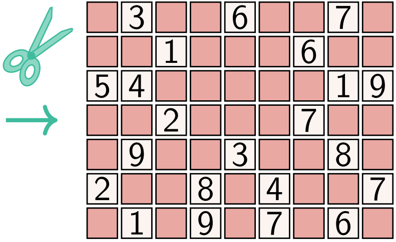
4	2	*6*	5	*7*	1	*3*	9	*8*
8	*5*	*7*	2	*9*	3	*1*	*4*	6
1	3	*9*	*4*	6	*8*	*2*	7	*5*
9	*7*	1	*3*	*8*	*5*	6	*2*	*4*
5	4	*3*	*7*	*2*	*6*	*8*	1	9
6	*8*	2	*1*	*4*	*9*	7	*5*	*3*
7	9	*4*	*6*	3	*2*	*5*	8	*1*
2	*6*	*5*	8	*1*	4	*9*	*3*	7
3	1	*8*	9	*5*	7	*4*	6	*2*

Solved Sudoku

Toy example of Zero-Knowledge Proof

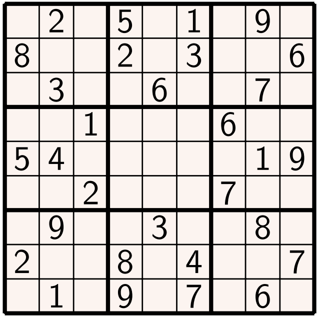


Unsolved Sudoku

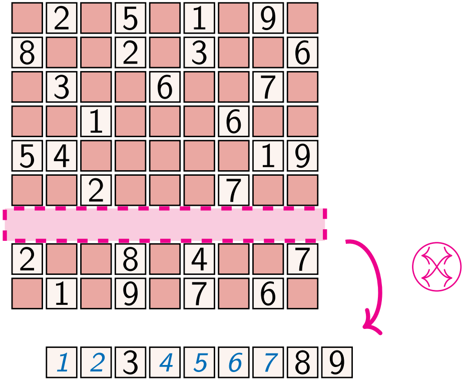


Grid cutting

Toy example of Zero-Knowledge Proof



Unsolved Sudoku

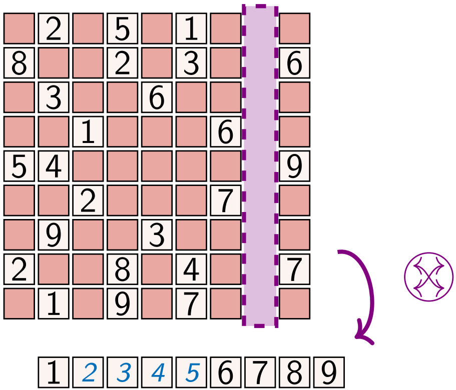


Rows checking

Toy example of Zero-Knowledge Proof

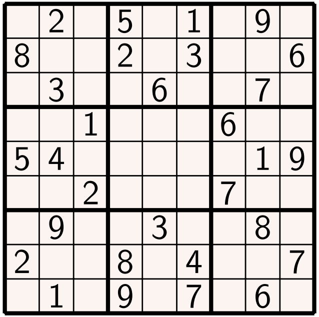
	2		5		1		9	
8			2		3			6
	3			6			7	
		1				6		
5	4						1	9
		2				7		
	9			3			8	
2			8		4			7
	1		9		7		6	

Unsolved Sudoku

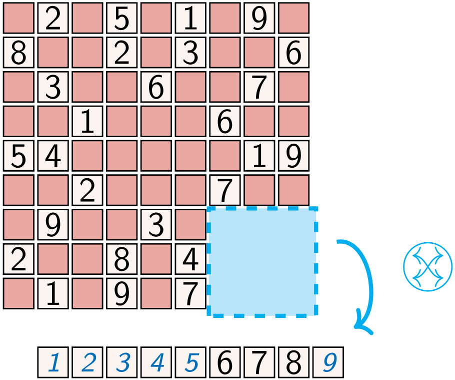


Columns checking

Toy example of Zero-Knowledge Proof



Unsolved Sudoku

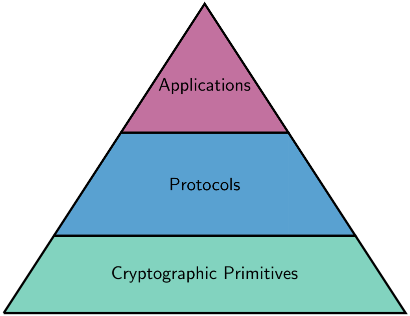


Squares checking

A need for new primitives

Protocols requiring new primitives:

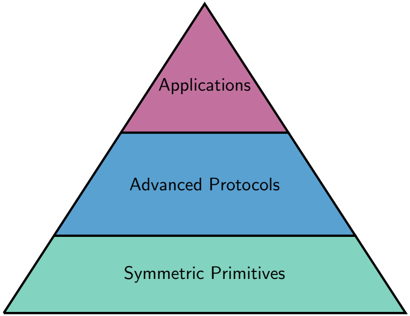
- ⋆ **MPC**: Multiparty Computation
- ⋆ **FHE**: Fully Homomorphic Encryption
- ⋆ **ZK**: Systems of Zero-Knowledge proofs
  Example: SNARKs, STARKs, Bulletproofs



A need for new primitives

Protocols requiring new primitives:

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



Problem: Designing new symmetric primitives

And analyse their security!

Block ciphers

- ⋆ input: n-bit block

$$x \in \mathbb{F}_2^n$$

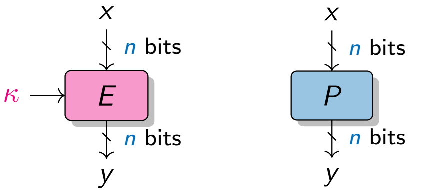
- ⋆ parameter: k-bit key

$$\kappa \in \mathbb{F}_2^k$$

- ⋆ output: n-bit block

$$y = E_\kappa(x) \in \mathbb{F}_2^n$$

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



(a) *Block cipher* **(b)** *Random permutation*

Block ciphers

- input: n-bit block

$$x \in \mathbb{F}_2^n$$

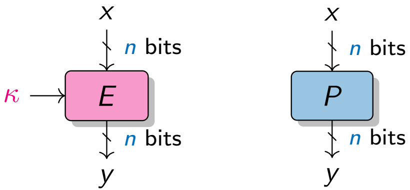
- parameter: k-bit key

$$\kappa \in \mathbb{F}_2^k$$

- output: n-bit block

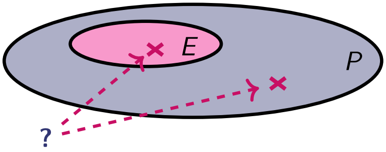
$$y = E_\kappa(x) \in \mathbb{F}_2^n$$

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



(a) *Block cipher* **(b)** *Random permutation*

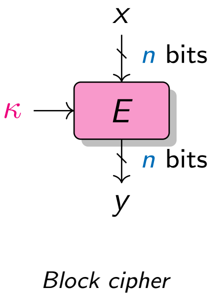
A block cipher is a family of 2^k permutations of $\mathbb{F}_2^n$.



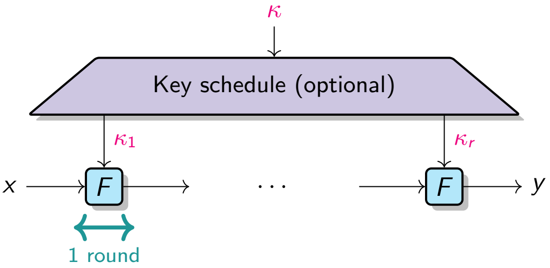
Iterated constructions

How to build an efficient block cipher?

By iterating a round function.



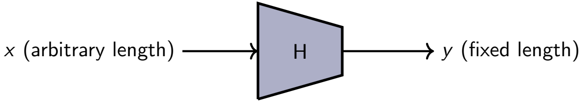
$\Rightarrow$



Hash functions

Definition

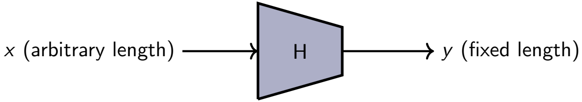
Hash function: $H : \mathbb{F}_q^\ell \to \mathbb{F}_q^h, x \mapsto y = H(x)$ where ℓ is arbitrary and h is fixed.



Hash functions

Definition

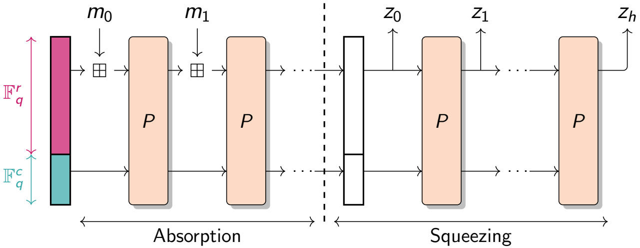
Hash function: $H : \mathbb{F}_q^{\ell} \to \mathbb{F}_q^{h}, x \mapsto y = H(x)$ where ℓ is arbitrary and h is fixed.



Sponge construction

Parameters:

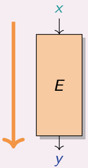
- ⋆ rate $r > 0$
- ⋆ capacity $c > 0$
- ⋆ permutation of $\mathbb{F}_q^r \times \mathbb{F}_q^c$



Comparison with the traditional case

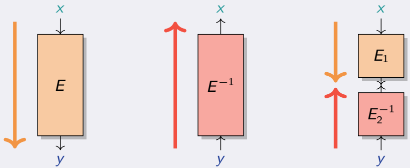
Traditional case

$$y \leftarrow E(x)$$



Arithmetization-oriented

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



Comparison with the traditional case

Traditional case

$$y \leftarrow E(x)$$

- ⋆ Optimized for:
  implementation in software/hardware

Arithmetization-oriented

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

- ⋆ Optimized for:
  integration within advanced protocols

Comparison with the traditional case

Traditional case

$$y \leftarrow E(x)$$

- Optimized for:
  implementation in software/hardware

- Alphabet size:
  $\mathbb{F}_2^n$, with $n \simeq 4, 8$

  Ex: Field of AES: $\mathbb{F}_{2^n}$ where $n = 8$

Arithmetization-oriented

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

- Optimized for:
  integration within advanced protocols

- Alphabet size:
  $\mathbb{F}_q$, with $q \in \{2^n, p\}, p \simeq 2^n$, $n \geq 64$

  Ex: Scalar Field of Curve `BLS12-381`: $\mathbb{F}_p$ where

  $p =$ `0x73eda753299d7d483339d80809a1d805`
  `53bda402fffe5bfeffffffff00000001`

Comparison with the traditional case

Traditional case

$$y \leftarrow E(x)$$

- ⋆ Optimized for:
  implementation in software/hardware
- ⋆ Alphabet size:
  $\mathbb{F}_2^n$, with $n \simeq 4, 8$
- ⋆ Operations:
  logical gates/CPU instructions

Arithmetization-oriented

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

- ⋆ Optimized for:
  integration within advanced protocols
- ⋆ Alphabet size:
  $\mathbb{F}_q$, with $q \in \{2^n, p\}, p \simeq 2^n$, $n \geq 64$
- ⋆ Operations:
  large finite-field arithmetic

Comparison with the traditional case

Traditional case

$$y \leftarrow E(x)$$

⋆ Optimized for: implem... /hardware

⋆ ...size: ..._2, with $n \simeq 4, 8$

⋆ Operations: logical gates/CPU instructions

Decades of Cryptanalysis

Arithmetization-oriented

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

⋆ Optimized for: integration ... protocols

⋆ ...: ...with $q \in \{2^n, p\}, p \simeq 2^n$, $n \geq 64$.

⋆ Operations: large finite-field arithmetic

$\leq$ 5 years of Cryptanalysis

Overview of the contributions

Theoretical cryptanalysis

- ⋆ *On the Algebraic Degree of Iterated Power Functions.*
  Bouvier, Canteaut, Perrin.
  DCC, 2023.

Practical cryptanalysis

- ⋆ *Algebraic Attacks Against some Arithmetization-Oriented Primitives.*
  Bariant, Bouvier, Leurent, Perrin.
  ToSC, 2022.

Design of a new AO primitive

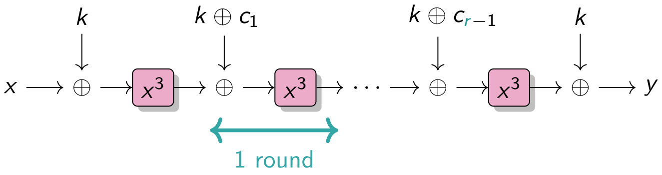
- ⋆ *New Design Techniques for Efficient Arithmetization-Oriented Hash Functions: Anemoi Permutations and Jive Compression Mode.*
  Bouvier, Briaud, Chaidos, Perrin, Salen, Velichkov, Willems.
  CRYPTO 2023.

Cryptanalysis of MIMC

- ⋆ Study of the corresponding sparse univariate polynomials
- ⋆ Bounding the algebraic degree
- ⋆ Tracing maximum-weight exponents reaching the upper bound
- ⋆ Study of higher-order differential attacks

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



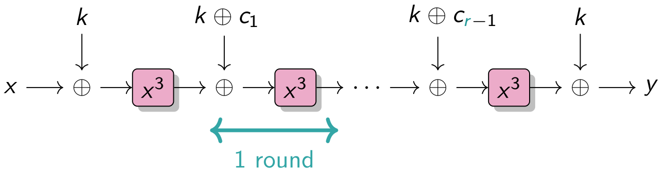
The block cipher MiMC

- Minimize the number of multiplications in $\mathbb{F}_{2^n}$.
- Construction of MiMC$_3$ [Albrecht et al., AC16]:
  - 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.



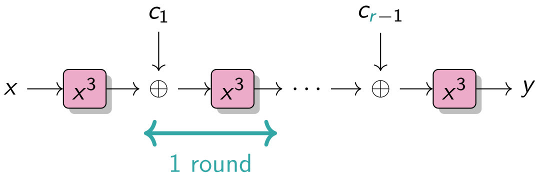
The block cipher MiMC

- Minimize the number of multiplications in $\mathbb{F}_{2^n}$.
- Construction of MiMC$_3$ [Albrecht et al., AC16]:
  - 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 $\mathbb{F}_2[x_1, \ldots x_n]/\left((x_i^2 + x_i)_{1 \le i \le n}\right)$:

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

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

Definition

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

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

Algebraic degree - 1st definition

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

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

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

Definition

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

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

If $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$, with $F(x) = (f_1(x), \ldots f_m(x))$, then

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

Algebraic degree - 1st definition

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

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

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

Example: ANF of $x \mapsto x^3$ in $\mathbb{F}_{2^{11}}$

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

Algebraic degree - 2nd definition

Let $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$. 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 $2^n - 1$:

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

Proposition

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

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

Algebraic 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 $2^n - 1$:

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

Proposition

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

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

Higher-Order differential attacks

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 $= n - 1$

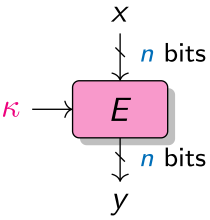
Higher-Order differential attacks

Exploiting a low algebraic degree

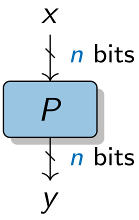
For any affine subspace $\mathcal{V} \subset \mathbb{F}_2^n$ with $\dim \mathcal{V} \geq \deg^a(F) + 1$, we have a 0-sum distinguisher:

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

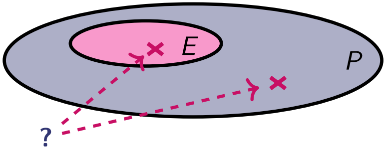
Random permutation: degree $= n - 1$



(a) *Block cipher*



(b) *Random permutation*



First Plateau

Polynomial representing r rounds of MIMC_3:

$$\mathcal{P}_{3,r}(x) = F_r \circ \ldots F_1(x) \ , \ \text{where } F_i = (x + c_{i-1})^3 \ .$$

Upper bound [Eichlseder et al., AC20]:

$$\lceil r \log_2 3 \rceil \ .$$

Aim: determine

$$B_3^r := \max_c \deg^a(\mathcal{P}_{3,r}) \ .$$

First Plateau

Polynomial representing r rounds of MIMC_3:

$$\mathcal{P}_{3,r}(x) = F_r \circ \ldots F_1(x) \ , \ \text{where } F_i = (x + c_{i-1})^3 \ .$$

Upper bound [Eichlseder et al., AC20]:

$$\lceil r \log_2 3 \rceil \ .$$

Aim: determine

$$B_3^r := \max_c \deg^a(\mathcal{P}_{3,r}) \ .$$

Example

⋆ Round 1: $B_3^1 = 2$

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

$$3 = [11]_2$$

First Plateau

Polynomial representing r rounds of MIMC$_3$:

$$\mathcal{P}_{3,r}(x) = F_r \circ \ldots F_1(x)\ , \text{ where } F_i = (x + c_{i-1})^3\ .$$

Upper bound [Eichlseder et al., AC20]:

$$\lceil r \log_2 3 \rceil\ .$$

Aim: determine

$$B_3^r := \max_c \deg^a(\mathcal{P}_{3,r})\ .$$

Example

⋆ Round 1: $B_3^1 = 2$

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

$$3 = [11]_2$$

⋆ Round 2: $B_3^2 = 2$

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

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

Observed degree

Definition

There is a **plateau** between rounds r and $r+1$ whenever:

$$B_3^{r+1} = B_3^r \ .$$

Proposition

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

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

Observed degree

Definition

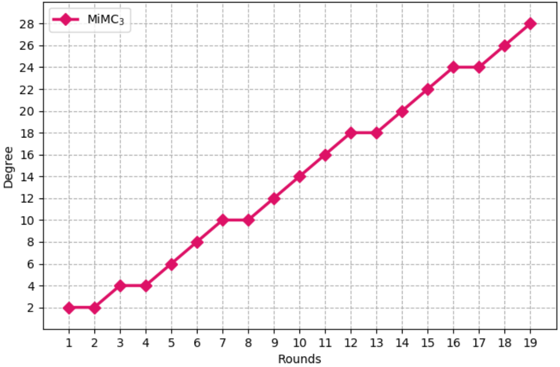
There is a **plateau** between rounds r and $r+1$ whenever:

$$B_3^{r+1} = B_3^r \ .$$

Proposition

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

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



Algebraic degree observed for $n = 31$.

Missing exponents

Proposition

Set of exponents that might appear in the polynomial:

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

Missing exponents

Proposition

Set of exponents that might appear in the polynomial:

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

Example

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

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

$$\mathcal{E}_{3,2} = \{0, 3, 6, 9\}\ , \quad \text{indeed} \quad \mathcal{P}_{3,2}(x) = x^9 + c_1 x^6 + c_1^2 x^3 + c_1^3\ .$$

Missing exponents

Proposition

Set of exponents that might appear in the polynomial:

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

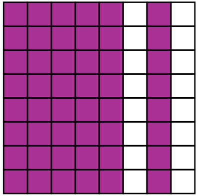
Missing exponents: no exponent $2^{2k} - 1$

Proposition

$$\forall i \in \mathcal{E}_{3,r}, i \not\equiv 5, 7 \bmod 8$$

0	1	2	3	4	5	6	7
8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23
24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47
48	49	50	51	52	53	54	55
56	57	58	59	60	61	62	63

Representation of exponents.



Missing exponents mod8.

Bounding the degree

Theorem

After r rounds of MIMC_3, 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_3, the algebraic degree is

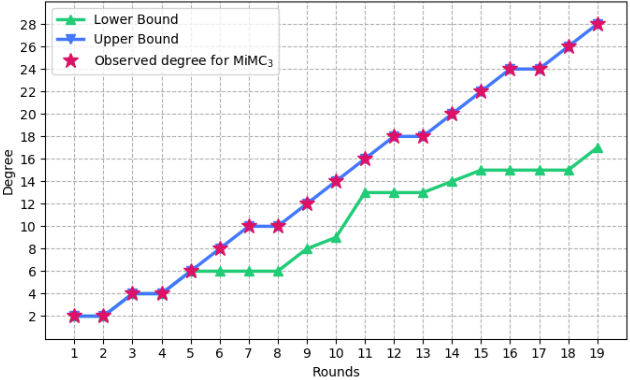
$$B_3^r \leq 2 \times \lceil \lfloor r \log_2 3 \rfloor / 2 - 1 \rceil$$

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

- A lower bound

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

- **Upper bound reached for almost 16265 rounds**

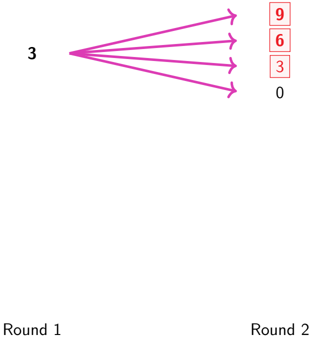


Tracing exponents

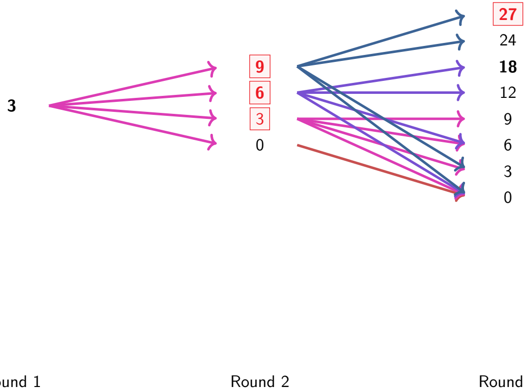
3

Round 1

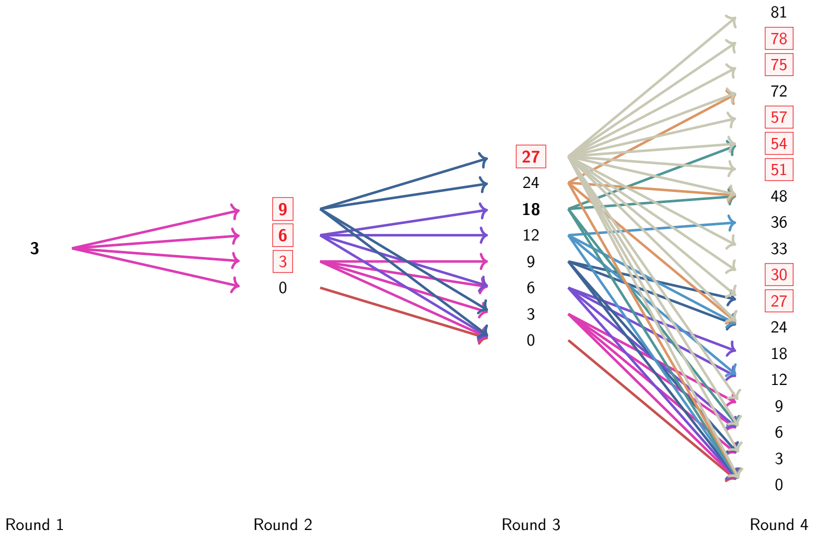
Tracing exponents



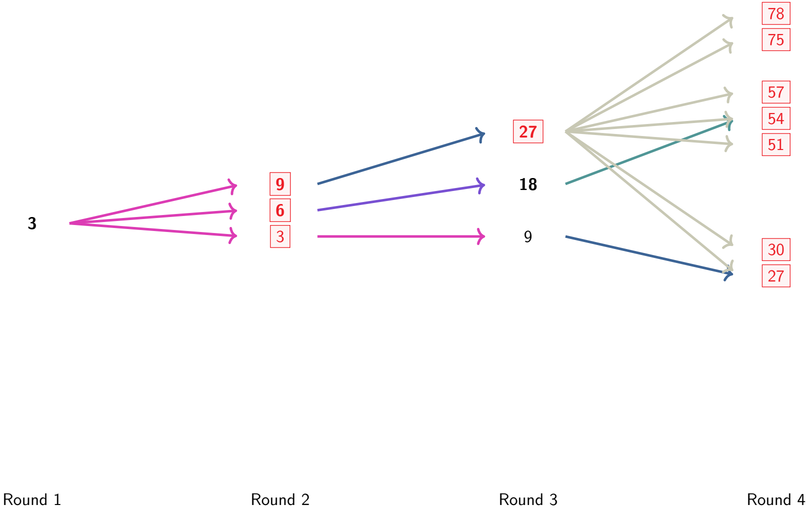
Tracing exponents



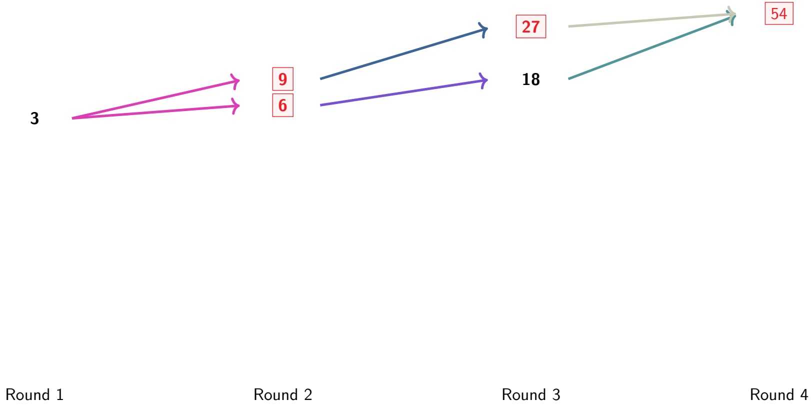
Tracing exponents



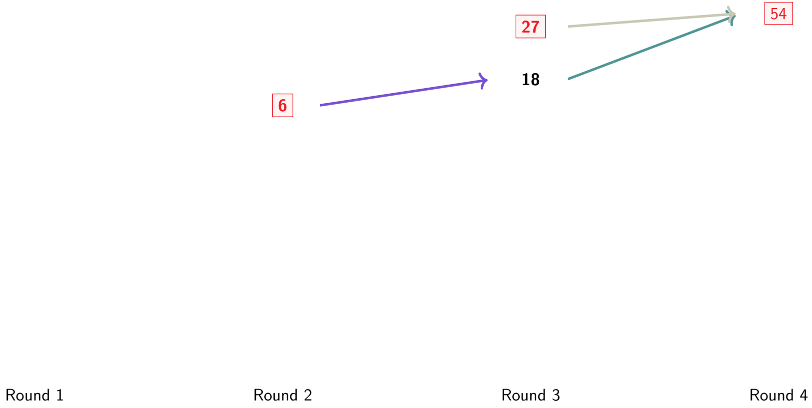
Tracing exponents



Tracing exponents



Tracing exponents

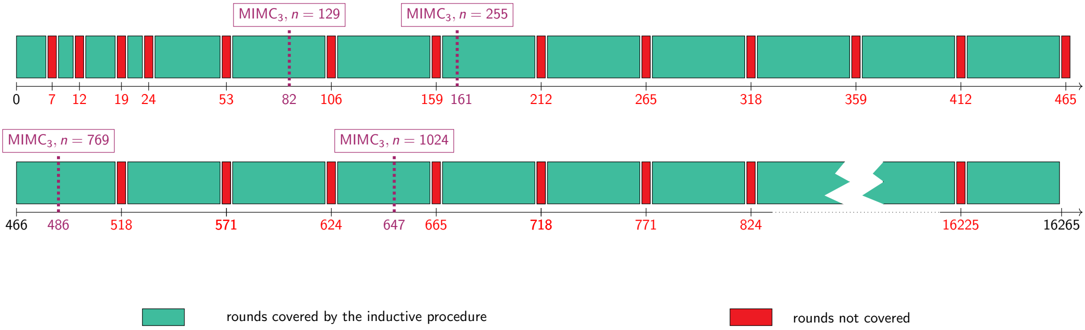


Covered rounds

Idea of the proof:

- inductive proof

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

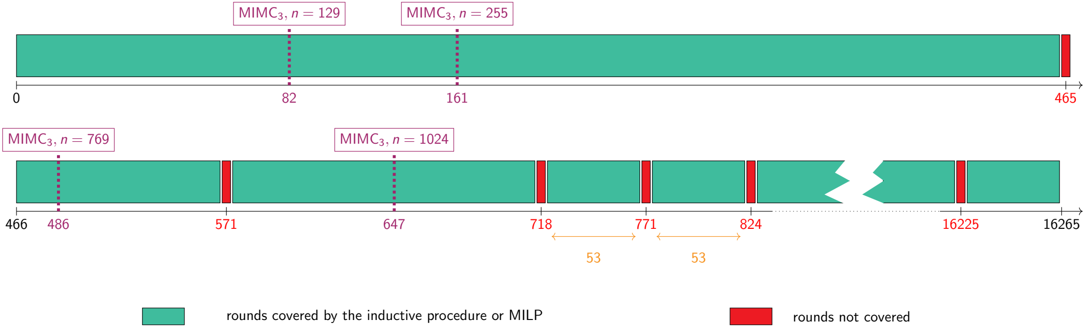


Covered rounds

Idea of the proof:

- ⋆ inductive proof
- ⋆ MILP solver (`PySCIPOpt`)

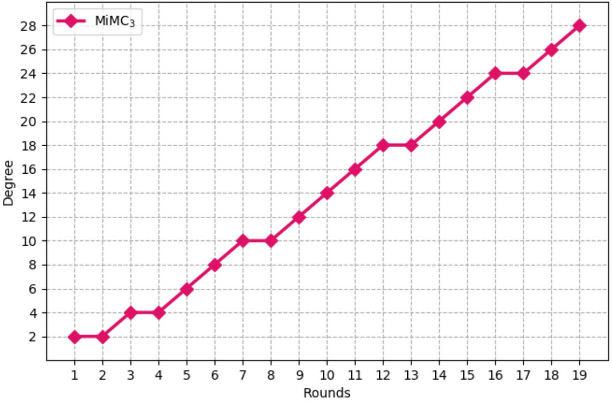
Rounds for which we are able to exhibit a maximum-weight exponent.



Plateau

Proposition

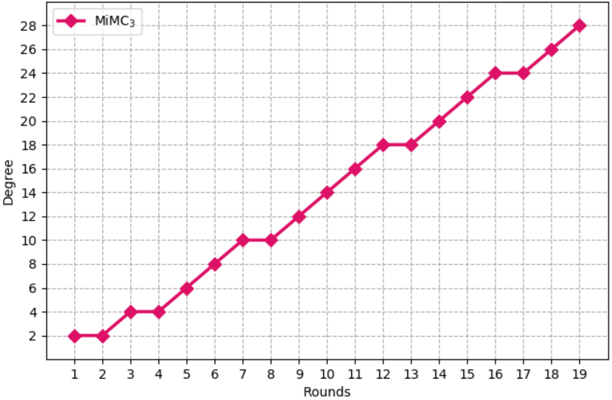
There is a plateau when $\lfloor r \log_2 3 \rfloor = 1 \bmod 2$ and $\lfloor (r+1) \log_2 3 \rfloor = 0 \bmod 2$



Plateau

Proposition

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



If we have a plateau

$$B_3^r = B_3^{r+1} ,$$

Then the next one is

$$B_3^{r+4} = B_3^{r+5}$$

or

$$B_3^{r+5} = B_3^{r+6} .$$

Music in MIMC$_3$

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

$$\log_2(3) \simeq 1.5849625$$

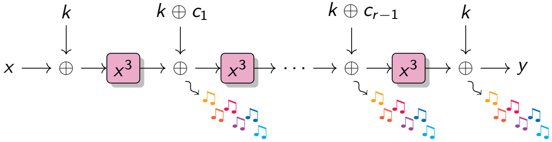
$$\mathfrak{D} = \{\boxed{1}, \boxed{2}, 3, 5, \boxed{7}, \boxed{12}, 17, 29, 41, \boxed{53}, 94, 147, 200, 253, 306, \boxed{359}, \ldots\},$$

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

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

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

$$\Leftrightarrow \quad \text{7 octaves} \sim \text{12 fifths}$$



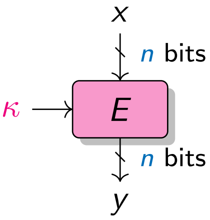
Higher-Order differential attacks

Exploiting a low algebraic degree

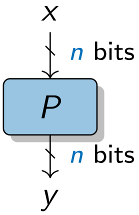
For any affine subspace $\mathcal{V} \subset \mathbb{F}_2^n$ with $\dim \mathcal{V} \geq \deg^a(F) + 1$, we have a 0-sum distinguisher:

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

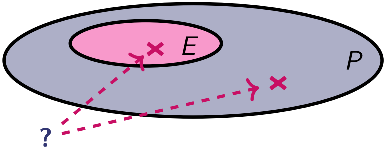
Random permutation: degree $= n - 1$



(a) *Block cipher*

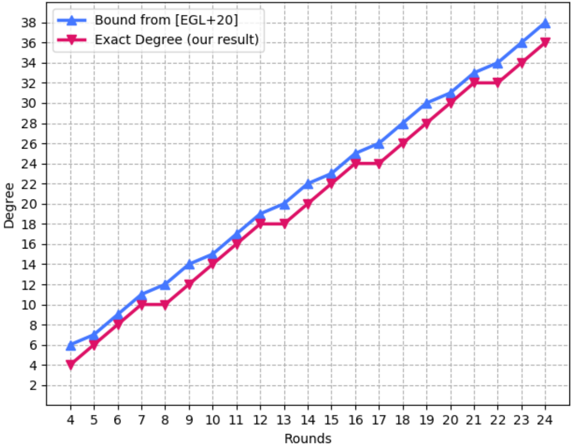


(b) *Random permutation*



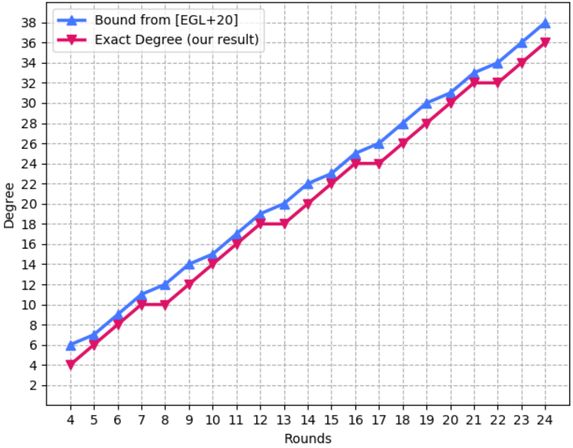
Comparison to previous work

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



Comparison to previous work

First Bound: $\lceil r \log_2 3 \rceil$ 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

A better understanding of the 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

Take-Away

A better understanding of the 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

Missing exponents in the univariate representation

Take-Away

A better understanding of the 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

Missing exponents in the univariate representation

$\downarrow$

Bounds on the algebraic degree

Take-Away

A better understanding of the 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

Missing exponents in the univariate representation

↓

Bounds on the algebraic degree → Higher-Order differential attacks

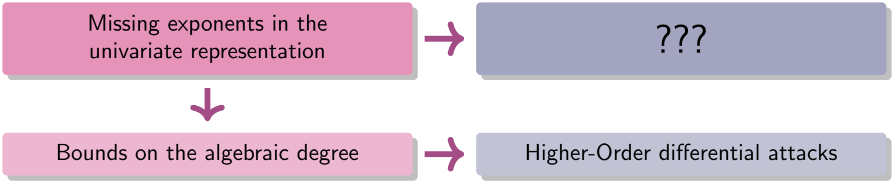
Take-Away

A better understanding of the 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



Algebraic Attacks against AOP

- ⋆ Solving the CICO problem
- ⋆ Trick to bypass rounds of SPN construction
- ⋆ Application to Poseidon and Rescue–Prime
- ⋆ Solving Ethereum Challenges

CICO Problem

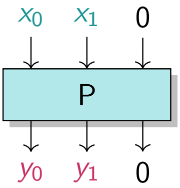
CICO: Constrained Input Constrained Output

Definition

Let $P : \mathbb{F}_q^t \rightarrow \mathbb{F}_q^t$ and $u < t$.

The **CICO** problem is:

$$\text{Finding } X, Y \in \mathbb{F}_q^{t-u} \text{ s.t. } P(X, 0^u) = (Y, 0^u).$$



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

CICO Problem

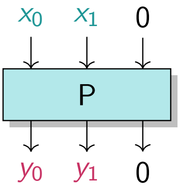
CICO: Constrained Input Constrained Output

Definition

Let $P : \mathbb{F}_q^t \to \mathbb{F}_q^t$ and $u < t$.

The **CICO** problem is:

Finding $X, Y \in \mathbb{F}_q^{t-u}$ s.t. $P(X, 0^u) = (Y, 0^u)$.



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

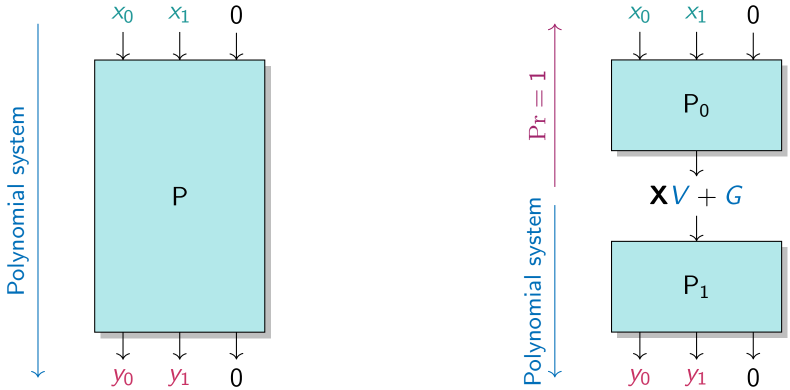
Ethereum Challenges: solving CICO problem for AO primitives with $q \sim 2^{64}$ prime

- ⋆ Feistel–MiMC [Albrecht et al., AC16]
- ⋆ Poseidon [Grassi et al., USENIX21]
- ⋆ Rescue–Prime [Aly et al., ToSC20]
- ⋆ Reinforced Concrete [Grassi et al., CCS22]

Trick for SPN

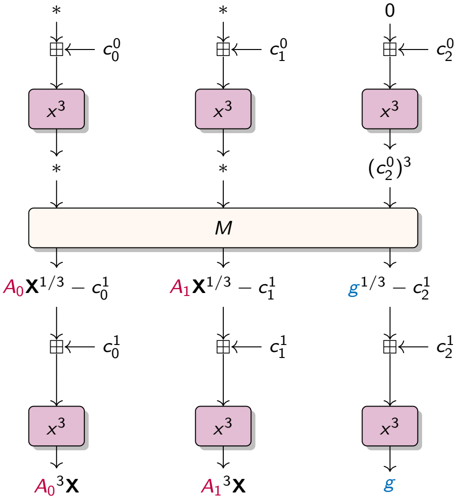
Let $P = P_0 \circ P_1$ be a permutation of $\mathbb{F}_p^3$ and suppose

$$\exists\ V, G \in \mathbb{F}_p^3, \quad \text{s.t. } \forall\ \mathbf{X} \in \mathbb{F}_p, \quad P_0^{-1}(\mathbf{X}V + G) = (*, *, 0)\ .$$

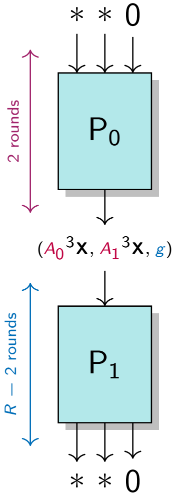


(a) *R-round system.* **(b)** $(R-2)$*-round system.*

Trick for POSEIDON

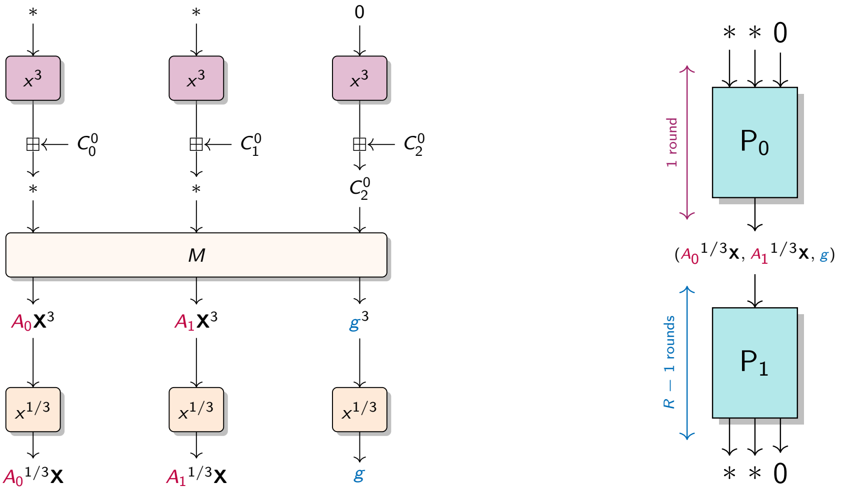


(a) *First two rounds.*



(b) *Overview.*

Trick for Rescue–Prime



(a) *First round.* **(b)** *Overview.*

Attack complexity

Univariate solving

RP	Authors claims	Ethereum claims	$\deg^u$	Our complexity
3	2^{17}	2^{45}	$3^9 \approx 2^{14.3}$	$\mathbf{2^{26}}$
8	2^{25}	2^{53}	$3^{14} \approx 2^{22.2}$	$\mathbf{2^{35}}$
13	2^{33}	2^{61}	$3^{19} \approx 2^{30.1}$	$\mathbf{2^{44}}$
19	2^{42}	2^{69}	$3^{25} \approx 2^{39.6}$	2^{54}
24	2^{50}	2^{77}	$3^{30} \approx 2^{47.5}$	2^{62}

(a) *For* POSEIDON.

Multivariate solving

R	m	Authors claims	Ethereum claims	$\deg^u$	Our complexity
4	3	2^{36}	$2^{37.5}$	$3^9 \approx 2^{14.3}$	$\mathbf{2^{43}}$
6	2	2^{40}	$2^{37.5}$	$3^{11} \approx 2^{17.4}$	2^{53}
7	2	2^{48}	$2^{43.5}$	$3^{13} \approx 2^{20.6}$	2^{62}
5	3	2^{48}	2^{45}	$3^{12} \approx 2^{19.0}$	2^{57}
8	2	2^{56}	$2^{49.5}$	$3^{15} \approx 2^{23.8}$	2^{72}

(b) *For Rescue–Prime.*

Cryptanalysis Challenge

Category	Parameters	Security level	Bounty
~~Easy~~	$\cancel{N = 4, m = 3}$	~~25~~	~~$2, 000~~
Easy	$N = 6, m = 2$	25	$4, 000
Medium	$N = 7, m = 2$	29	$6, 000
Hard	$N = 5, m = 3$	30	$12, 000
Hard	$N = 8, m = 2$	33	$26, 000

(a) *Rescue–Prime*

Category	Parameters	Security level	Bounty
~~Easy~~	$\cancel{r = 6}$	~~9~~	~~$2, 000~~
~~Easy~~	$\cancel{r = 10}$	~~15~~	~~$4, 000~~
~~Medium~~	$\cancel{r = 14}$	~~22~~	~~$6, 000~~
~~Hard~~	$\cancel{r = 18}$	~~28~~	$12, 000
~~Hard~~	$\cancel{r = 22}$	~~34~~	$26, 000

(b) *Feistel–MiMC*

Category	Parameters	Security level	Bounty
~~Easy~~	$\cancel{RP = 3}$	~~8~~	~~$2, 000~~
~~Easy~~	$\cancel{RP = 8}$	~~16~~	~~$4, 000~~
~~Medium~~	$\cancel{RP = 13}$	~~24~~	~~$6, 000~~
Hard	$RP = 19$	32	$12, 000
Hard	$RP = 24$	40	$26, 000

(c) POSEIDON

Category	Parameters	Security level	Bounty
Easy	$p = 281474976710597$	24	$4, 000
Medium	$p = 72057594037926839$	28	$6, 000
Hard	$p = 18446744073709551557$	32	$12, 000

(d) `Reinforced Concrete`

Take-Away

AOP cryptanalysis is a lucrative business!

Take-Away

AOP cryptanalysis is a lucrative business!

Recommendations for future designs

- ⋆ study possible tricks to bypass rounds
- ⋆ start (and end) with a linear layer
- ⋆ prefer univariate instead of multivariate systems
- ⋆ consider as many variants of modeling as possible

Take-Away

AOP cryptanalysis is a lucrative business!

Recommendations for future designs

- ⋆ study possible tricks to bypass rounds
- ⋆ start (and end) with a linear layer
- ⋆ prefer univariate instead of multivariate systems
- ⋆ consider as many variants of modeling as possible

Related works

- ⋆ FreeLunch attack against AOP [Bariant et al., 2024]

Design of Anemoi

- ⋆ Link between CCZ-equivalence and Arithmetization-Orientation
- ⋆ A new S-Box: the Flystel
- ⋆ A new family of ZK-friendly hash functions: Anemoi

Performance metric

What does "efficient" mean for Zero-Knowledge Proofs?

Performance metric

What does "efficient" mean for Zero-Knowledge Proofs?

"It depends"

Performance metric

What does "efficient" mean for Zero-Knowledge Proofs?

"It depends"

Example

R1CS (Rank-1 Constraint System): minimizing the number of multiplications

$$y = (ax + b)^3(cx + d) + ex$$

$$t_0 = a \cdot x \qquad t_3 = t_2 \times t_1 \qquad t_6 = t_3 \times t_5$$
$$t_1 = t_0 + b \qquad t_4 = c \cdot x \qquad t_7 = e \cdot x$$
$$t_2 = t_1 \times t_1 \qquad t_5 = t_4 + d \qquad t_8 = t_6 + t_7$$

Performance metric

What does "efficient" mean for Zero-Knowledge Proofs?

"It depends"

Example

R1CS (Rank-1 Constraint System): minimizing the number of multiplications

$$y = (ax + b)^3 (cx + d) + ex$$

$$\begin{array}{lll} t_0 = a \cdot x & t_3 = t_2 \times t_1 & t_6 = t_3 \times t_5 \\ t_1 = t_0 + b & t_4 = c \cdot x & t_7 = e \cdot x \\ t_2 = t_1 \times t_1 & t_5 = t_4 + d & t_8 = t_6 + t_7 \end{array}$$

3 constraints

Our approach

Need: verification using few multiplications.

Our approach

Need: verification using few multiplications.

⋆ **First approach:** evaluation using few multiplications, e.g. POSEIDON [Grassi et al., USENIX21]

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

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

Our approach

Need: verification using few multiplications.

⋆ **First approach:** evaluation using few multiplications, e.g. Poseidon [Grassi et al., USENIX21]

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

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

⋆ **First breakthrough:** using inversion, e.g. *Rescue* [Aly et al., ToSC20]

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

$\boxed{x == E^{-1}(y)}$ $\rightsquigarrow$ E^{-1}: low degree

Our approach

Need: verification using few multiplications.

⋆ **First approach:** evaluation using few multiplications, e.g. POSEIDON [Grassi et al., USENIX21]

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

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

⋆ **First breakthrough:** using inversion, e.g. *Rescue* [Aly et al., ToSC20]

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

$\boxed{x == E^{-1}(y)}$ $\rightsquigarrow$ E^{-1}: low degree

⋆ **Our approach:** using $(u, v) = \mathcal{L}(x, y)$, where $\mathcal{L}$ is linear

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

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

CCZ-equivalence

Inversion

$$\Gamma_F = \{(x, F(x)), x \in \mathbb{F}_q\} \quad \text{and} \quad \Gamma_{F^{-1}} = \left\{\left(y, F^{-1}(y)\right), y \in \mathbb{F}_q\right\}$$

Noting that

$$\Gamma_F = \left\{\left(F^{-1}(y), y\right), y \in \mathbb{F}_q\right\} ,$$

then, we have:

$$\Gamma_F = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \Gamma_{F^{-1}} .$$

CCZ-equivalence

Inversion

$$\Gamma_F = \{(x, F(x)), x \in \mathbb{F}_q\} \quad \text{and} \quad \Gamma_{F^{-1}} = \left\{\left(y, F^{-1}(y)\right), y \in \mathbb{F}_q\right\}$$

Noting that

$$\Gamma_F = \left\{\left(F^{-1}(y), y\right), y \in \mathbb{F}_q\right\} \ ,$$

then, we have:

$$\Gamma_F = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \Gamma_{F^{-1}} \ .$$

Definition [Carlet, Charpin and Zinoviev, DCC98]

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

$$\Gamma_F = \mathcal{L}(\Gamma_G) + c \ , \quad \text{where } \mathcal{L} \text{ is linear.}$$

Advantages of CCZ-equivalence

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

- ⋆ Differential properties are the same: $\delta_F = \delta_G$.

Differential uniformity

Maximum value of the DDT

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

Advantages of CCZ-equivalence

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

- ⋆ Differential properties are the same: $\delta_F = \delta_G$.

Differential uniformity

Maximum value of the DDT

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

- ⋆ Linear properties are the same: $\mathcal{W}_F = \mathcal{W}_G$.

Linearity

Maximum value of the LAT

$$\mathcal{W}_F = \max_{a, b \neq 0} \left| \sum_{x \in \mathbb{F}_{2^n}^m} (-1)^{a \cdot x + b \cdot F(x)} \right|$$

Advantages of CCZ-equivalence

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

- ⋆ Verification is the same: if $y \leftarrow F(x)$, $v \leftarrow G(u)$ and $(u, v) = \mathcal{L}(x, y)$

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

Advantages of CCZ-equivalence

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

- Verification is the same: if $y \leftarrow F(x)$, $v \leftarrow G(u)$ and $(u, v) = \mathcal{L}(x, y)$

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

- The degree is **not preserved**.

Example

in $\mathbb{F}_p$ where

$$p = \texttt{0x73eda753299d7d483339d80809a1d80553bda402fffe5bfeffffffff00000001}$$

if $F(x) = x^5$ then $F^{-1}(x) = x^{5^{-1}}$ where

$$5^{-1} = \texttt{0x2e5f0fbadd72321ce14a56699d73f002217f0e679998f19933333332cccccccd}$$

Advantages of CCZ-equivalence

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

- ⋆ Verification is the same: if $y \leftarrow F(x)$, $v \leftarrow G(u)$ and $(u, v) = \mathcal{L}(x, y)$

$$\boxed{y == F(x)? \quad \Longleftrightarrow \quad v == G(u)?}$$

- ⋆ The degree is **not preserved**.

Example

in $\mathbb{F}_p$ where

$$p = \mathtt{0x73eda753299d7d483339d80809a1d80553bda402fffe5bfeffffffff00000001}$$

if $F(x) = x^5$ then $F^{-1}(x) = x^{5^{-1}}$ where

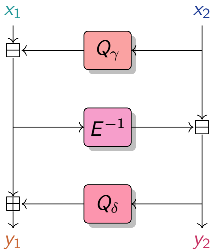
$$5^{-1} = \mathtt{0x2e5f0fbadd72321ce14a56699d73f002217f0e679998f19933333332cccccccd}$$

The Flystel

Butterfly + Feistel ⇒ Flystel

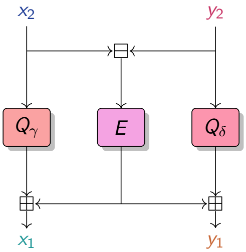
A 3-round Feistel-network with
$Q_\gamma : \mathbb{F}_q \to \mathbb{F}_q$ and $Q_\delta : \mathbb{F}_q \to \mathbb{F}_q$ two quadratic functions, and $E : \mathbb{F}_q \to \mathbb{F}_q$ a permutation

High-Degree permutation



Open Flystel $\mathcal{H}$.

Low-Degree function



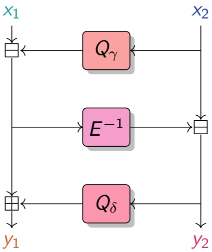
Closed Flystel $\mathcal{V}$.

The Flystel

$\boxed{\text{Butterfly} + \text{Feistel} \Rightarrow \texttt{Flystel}}$

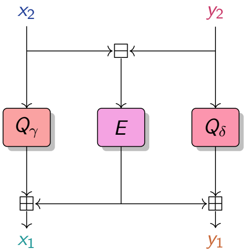
A 3-round Feistel-network with
$Q_\gamma : \mathbb{F}_q \to \mathbb{F}_q$ and $Q_\delta : \mathbb{F}_q \to \mathbb{F}_q$ two quadratic functions, and $E : \mathbb{F}_q \to \mathbb{F}_q$ a permutation

High-Degree
permutation



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

Low-Degree
function



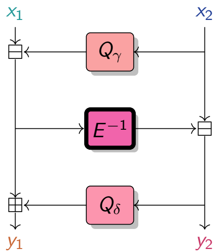
Closed `Flystel` $\mathcal{V}$.

$$\Gamma_{\mathcal{H}} = \mathcal{L}(\Gamma_{\mathcal{V}}) \quad \text{s.t.} \quad ((x_1, x_2), (y_1, y_2)) = \mathcal{L}\left(((y_2, x_2), (x_1, y_1)) \right)$$

Advantage of CCZ-equivalence

⋆ High-Degree Evaluation.

High-Degree
permutation



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

Example

if $E : x \mapsto x^5$ in $\mathbb{F}_p$ where

$$p = \texttt{0x73eda753299d7d483339d80809a1d805}$$
$$\texttt{53bda402fffe5bfeffffffff00000001}$$

then $E^{-1} : x \mapsto x^{5^{-1}}$ where

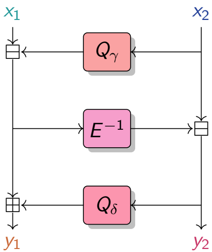
$$5^{-1} = \texttt{0x2e5f0fbadd72321ce14a56699d73f002}$$
$$\texttt{217f0e679998f19933333332cccccccd}$$

Advantage of CCZ-equivalence

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

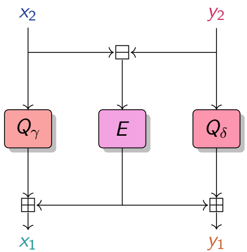
$$\boxed{(y_1, y_2) == \mathcal{H}(x_1, x_2) \Leftrightarrow (x_1, y_1) == \mathcal{V}(x_2, y_2)}$$

High-Degree
permutation



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

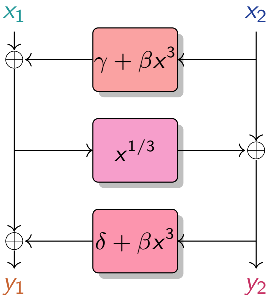
Low-Degree
function



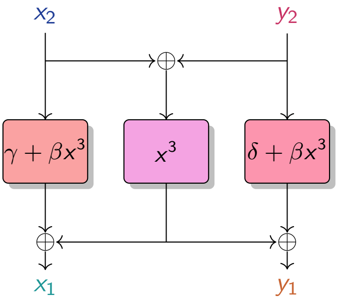
Closed `Flystel` $\mathcal{V}$.

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

$$Q_\gamma(x) = \gamma + \beta x^3 , \quad Q_\delta(x) = \delta + \beta x^3 , \quad \text{and} \quad E(x) = x^3$$

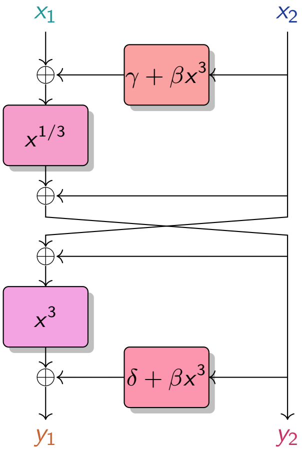


Open `Flystel`$_2$.



Closed `Flystel`$_2$.

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



Degenerated Butterfly.

Introduced by [Perrin et al. 2016].

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

- ⋆ Differential properties

$$\delta_{\mathcal{H}} = \delta_{\mathcal{V}} = 4$$

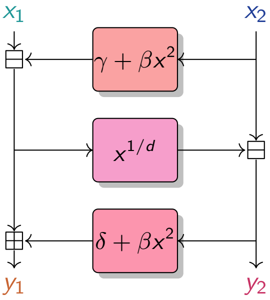
- ⋆ Linear properties

$$\mathcal{W}_{\mathcal{H}} = \mathcal{W}_{\mathcal{V}} = 2^{n+1}$$

- ⋆ Algebraic degree
  - ⋆ Open $\texttt{Flystel}_2$: $\deg_{\mathcal{H}} = n$
  - ⋆ Closed $\texttt{Flystel}_2$: $\deg_{\mathcal{V}} = 2$

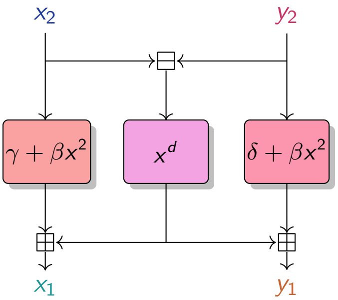
Flystel in $\mathbb{F}_p$

$$Q_\gamma(x) = \gamma + \beta x^2 \ , \quad Q_\delta(x) = \delta + \beta x^2 \ , \quad \text{and} \quad E(x) = x^d$$



Open `Flystel`$_p$.

usually
$d = 3$ or 5.



Closed `Flystel`$_p$.

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

⋆ Differential properties

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

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

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

⋆ Differential properties

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

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

Solving the open problem of finding an APN (Almost-Perfect Non-linear) permutation over $\mathbb{F}_p^2$

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

⋆ Differential properties

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

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

Solving the open problem of finding an APN (Almost-Perfect Non-linear) permutation over $\mathbb{F}_p^2$

⋆ Linear properties

Conjecture:

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

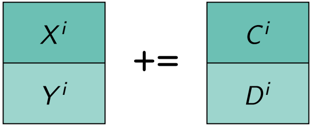
The SPN Structure

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

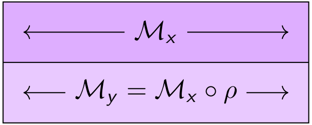
A Substitution-Permutation Network with:

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

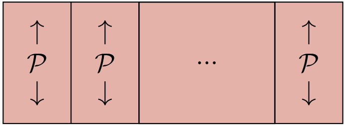
(a) *Internal state.*



(b) *The constant addition.*

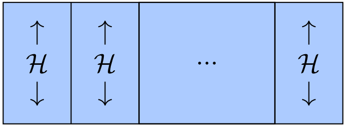


(c) *The diffusion layer.*



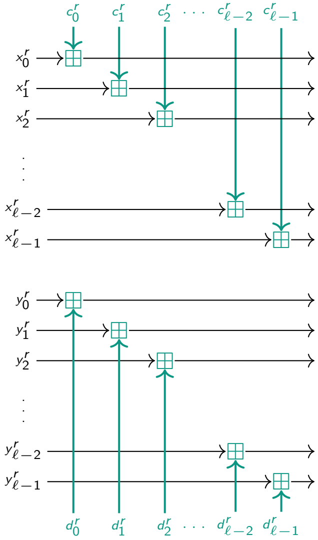
with $\mathcal{P} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$

(d) *The Pseudo-Hadamard Transform.*

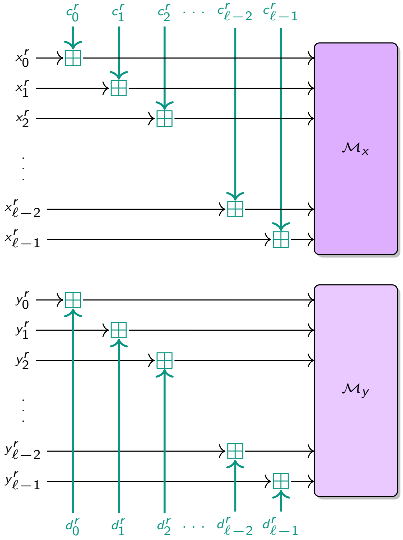


(e) *The S-box layer.*

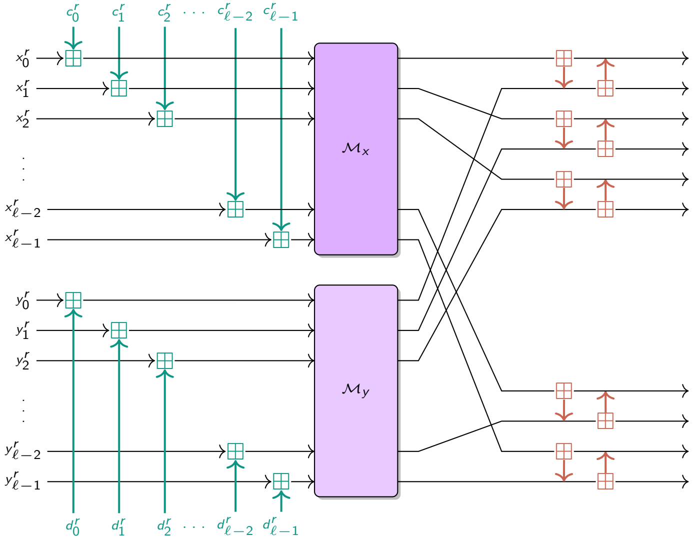
The SPN Structure



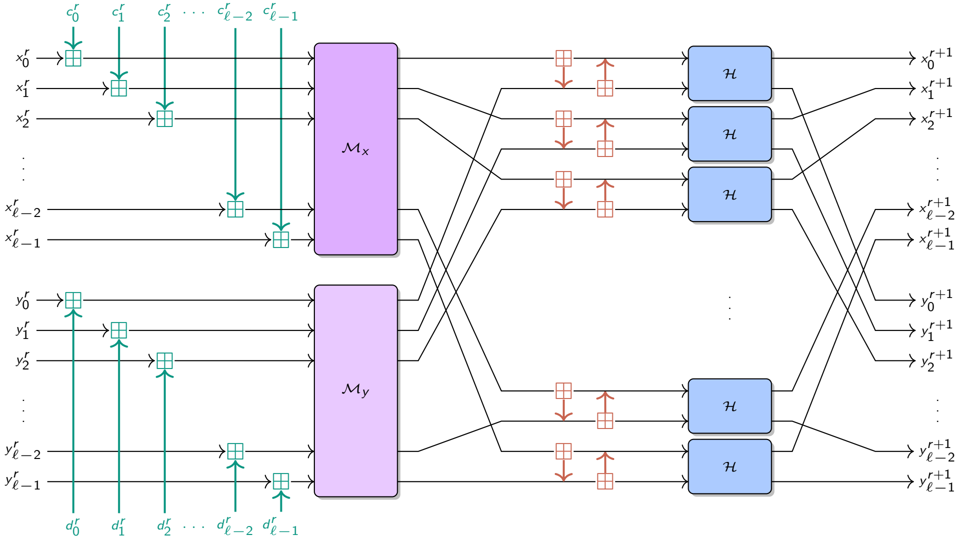
The SPN Structure



The SPN Structure



The SPN Structure



Performance metric

What does "efficient" mean for Zero-Knowledge Proofs?

"It depends"

Example

R1CS (Rank-1 Constraint System): minimizing the number of multiplications

$$y = (ax + b)^3 (cx + d) + ex$$

$t_0 = a \cdot x$ | $t_3 = t_2 \times t_1$ | $t_6 = t_3 \times t_5$

$t_1 = t_0 + b$ | $t_4 = c \cdot x$ | $t_7 = e \cdot x$

$t_2 = t_1 \times t_1$ | $t_5 = t_4 + d$ | $t_8 = t_6 + t_7$

3 constraints

Some Benchmarks

	m $(=2\ell)$	RP[1]	Poseidon[2]	Griffin[3]	Anemoi
R1CS	2	208	198	-	**76**
	4	224	232	112	**96**
	6	216	264	-	**120**
	8	256	296	176	**160**
Plonk	2	312	380	-	**191**
	4	560	832	**260**	316
	6	756	1344	-	**460**
	8	1152	1920	**574**	648
AIR	2	156	300	-	**126**
	4	**168**	348	**168**	**168**
	6	**162**	396	-	216
	8	**192**	456	264	288

(a) *when $d = 3$.*

	m $(=2\ell)$	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	-	**212**
	4	528	696	**222**	344
	6	768	1125	-	**496**
	8	1280	1609	**492**	696
AIR	2	**200**	360	-	210
	4	**220**	440	**220**	280
	6	**240**	540	-	360
	8	**320**	640	360	480

(b) *when $d = 5$.*

Constraint comparison for standard arithmetization, without optimization ($s = 128$).

[1] *Rescue* [Aly et al., ToSC20] [2] Poseidon [Grassi et al., USENIX21] [3] Griffin [Grassi et al., CRYPTO23]

Some Benchmarks

*** Numbers to be updated! ***

	m $(= 2\ell)$	*RP*[1]	Poseidon[2]	Griffin[3]	Anemoi
R1CS	2	208	198	-	**76**
	4	224	232	112	**96**
	6	216	264	-	**120**
	8	256	296	176	**160**
Plonk	2	312	380	-	**191**
	4	560	832	**260**	316
	6	756	1344	-	**460**
	8	1152	1920	**574**	648
AIR	2	156	300	-	**126**
	4	**168**	348	**168**	**168**
	6	**162**	396	-	216
	8	**192**	456	264	288

(a) *when* $d = 3$.

	m $(= 2\ell)$	*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	-	**212**
	4	528	696	**222**	344
	6	768	1125	-	**496**
	8	1280	1609	**492**	696
AIR	2	**200**	360	-	210
	4	**220**	440	**220**	280
	6	**240**	540	-	360
	8	**320**	640	360	480

(b) *when* $d = 5$.

Constraint comparison for standard arithmetization, without optimization $(s = 128)$.

[1] *Rescue* [Aly et al., ToSC20] [2] Poseidon [Grassi et al., USENIX21] [3] Griffin [Grassi et al., CRYPTO23]

Take-Away

Anemoi: A new family of ZK-friendly hash functions

- ⋆ Identify a link between AO and CCZ-equivalence
- ⋆ Contributions of fundamental interest:
  - ⋆ New S-box: Flystel
  - ⋆ New mode: Jive

Take-Away

Anemoi: A new family of ZK-friendly hash functions

- ⋆ Identify a link between AO and CCZ-equivalence
- ⋆ Contributions of fundamental interest:
  - ⋆ New S-box: Flystel
  - ⋆ New mode: Jive

Related works

- ⋆ $\texttt{AnemoiJive}_3$ with TurboPlonK [Liu et al., 2022]
- ⋆ Arion [Roy, Steiner and Trevisani, 2023]
- ⋆ APN permutations over prime fields [Budaghyan and Pal, 2023]

Conclusions

- Practical and theoretical cryptanalysis
  - a better insight into the behaviour of algebraic systems
  - a comprehensive understanding of the univariate representation of MiMC
  - guarantees on the algebraic degree of MiMC

Conclusions

- Practical and theoretical cryptanalysis
  - a better insight into the behaviour of algebraic systems
  - a comprehensive understanding of the univariate representation of MiMC
  - guarantees on the algebraic degree of MiMC
- New tools for designing primitives:
  - `Anemoi`: a new family of ZK-friendly hash functions
  - a link between CCZ-equivalence and AO
  - more general contributions: `Jive`, `Flystel`

Perspectives

- On the cryptanalysis
  - solve conjectures to trace maximum-weight exponents
  - generalization to other schemes
  - find a univariate distinguisher

Perspectives

- On the cryptanalysis
  - solve conjectures to trace maximum-weight exponents
  - generalization to other schemes
  - find a univariate distinguisher
- On the design
  - a `Flystel` with more branches
  - solve the conjecture for the linearity

Perspectives

- On the cryptanalysis
  - solve conjectures to trace maximum-weight exponents
  - generalization to other schemes
  - find a univariate distinguisher
- On the design
  - a `Flystel` with more branches
  - solve the conjecture for the linearity

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

Perspectives

- On the cryptanalysis
  - solve conjectures to trace maximum-weight exponents
  - generalization to other schemes
  - find a univariate distinguisher
- On the design
  - a `Flystel` with more branches
  - solve the conjecture for the linearity

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

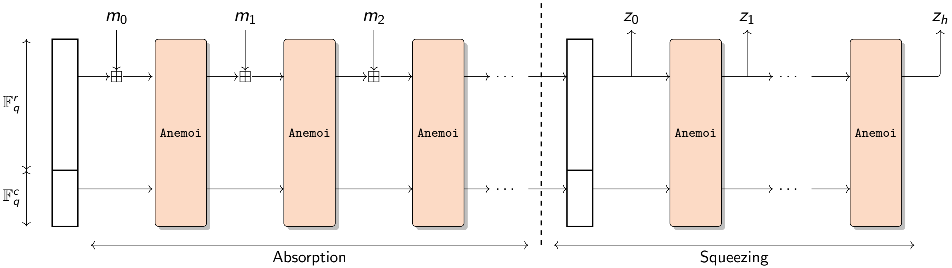
Thank you

Anemoi

More benchmarks and Cryptanalysis

Sponge construction

- Hash function (random oracle):
  - input: arbitrary length
  - ouput: fixed length

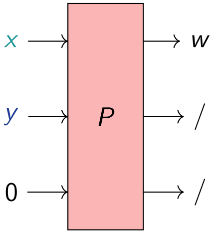


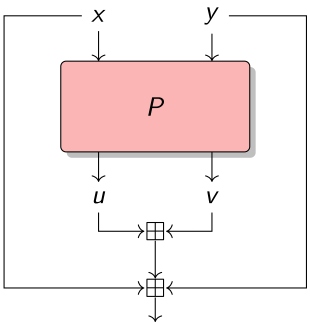
New Mode: Jive

- Compression function (Merkle-tree):
  - input: fixed length
  - output: (input length) /2

Dedicated mode: 2 words in 1

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



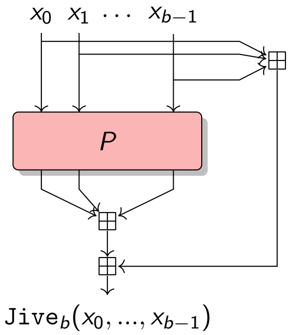


New Mode: Jive

- ⋆ Compression function (Merkle-tree):
  - ⋆ input: fixed length
  - ⋆ output: (input length) /b

Dedicated mode: b words in 1

$$\texttt{Jive}_b(P) : \begin{cases} (\mathbb{F}_q^m)^b & \to \mathbb{F}_q^m \\ (x_0, \dots, x_{b-1}) & \mapsto \displaystyle\sum_{i=0}^{b-1} (x_i + P_i(x_0, \dots, x_{b-1})) \end{cases} .$$



Comparison for Plonk (with optimizations)

	m	Constraints
Poseidon	3	110
	2	88
Reinforced Concrete	3	378
	2	236
Rescue–Prime	3	252
Griffin	3	125
AnemoiJive	2	**~~86~~ 56**

(a) *With 3 wires.*

	m	Constraints
Poseidon	3	98
	2	82
Reinforced Concrete	3	267
	2	174
Rescue–Prime	3	168
Griffin	3	111
AnemoiJive	2	**64**

(b) *With 4 wires.*

Constraints comparison with an additional custom gate for x^α. ($s = 128$).

with an additional quadratic custom gate: 56 constraints

Native performance

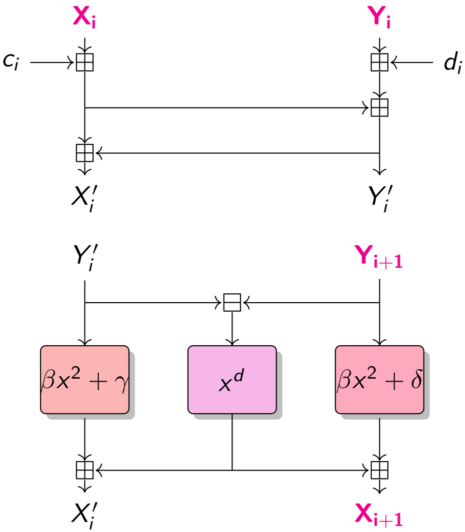
Rescue-12	*Rescue*-8	Poseidon-12	Poseidon-8	Griffin-12	Griffin-8	Anemoi-8
15.67 μs	9.13 μs	5.87 μs	2.69 μs	2.87 μs	**2.59 μs**	4.21 μs

2-to-1 compression functions for $\mathbb{F}_p$ with $p = 2^{64} - 2^{32} + 1$ ($s = 128$).

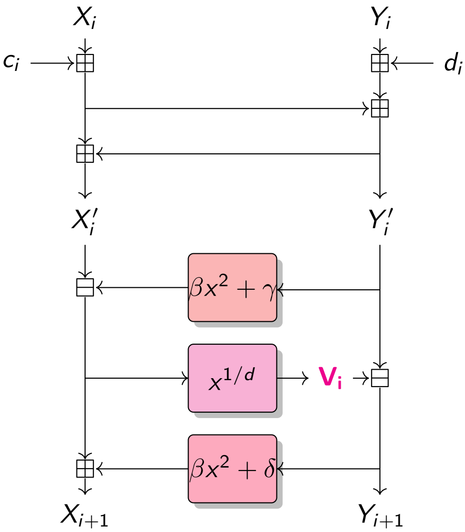
Rescue	Poseidon	Griffin	Anemoi
206 μs	**9.2 μs**	74.18 μs	128.29 μs

For BLS$12-381$, Rescue, Poseidon, Anemoi with state size of 2, Griffin of 3 ($s = 128$).

Algebraic attacks: 2 modelings



(a) *Model 1.*

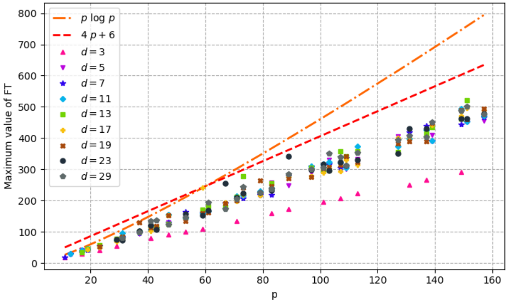


(b) *Model 2.*

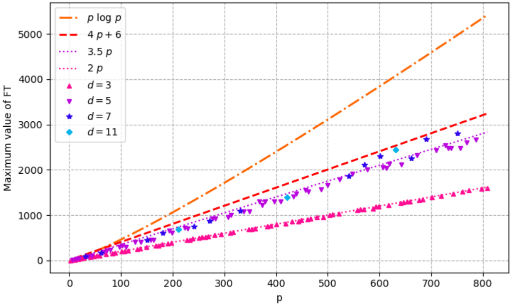
Properties of `Flystel` in $\mathbb{F}_p$

⋆ 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 d.*



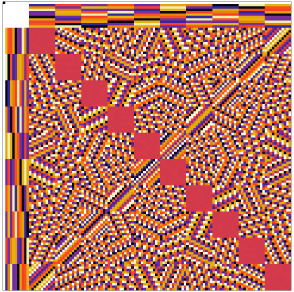
(b) *For the smallest d.*

Conjecture for the linearity.

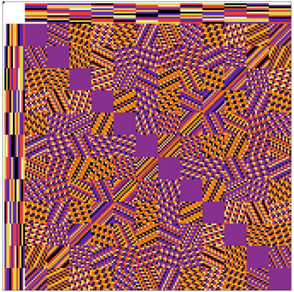
Properties of Flystel in $\mathbb{F}_p$

- ⋆ Linear properties

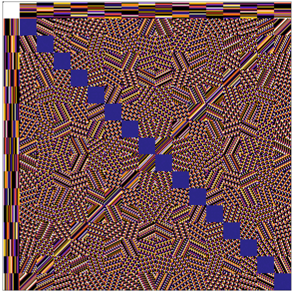
$$\mathcal{W}_{\mathcal{H}} = \max_{a,b \neq 0} \left| \sum_{x \in \mathbb{F}_p^2} exp\left(\frac{2\pi i(\langle a, x\rangle - \langle b, \mathcal{H}(x)\rangle)}{p} \right) \right| \leq p \log p \ ?$$



(a) *when* $p = 11$ *and* $d = 3$.



(b) *when* $p = 13$ *and* $d = 5$.



(c) *when* $p = 17$ *and* $d = 3$.

LAT of $\texttt{Flystel}_p$.

Open problems

on the Algebraic Degree

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

- For MIMC_3

$$i \bmod 8 \notin \{5, 7\} \ .$$

- For MIMC_7

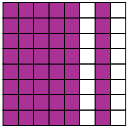
$$i \bmod 16 \notin \{9, 11, 13, 15\} \ .$$

- For MIMC_{15}

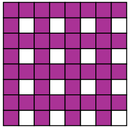
$$i \bmod 32 \notin \{17, 19, 21, 23, 25, 27, 29, 31\} \ .$$

- For MIMC_{31}

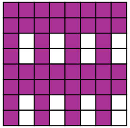
$$i \bmod 64 \notin \{33, 35, 37, 39, 41, 43, 45, 47, 49, 51, 53, 55, 57, 59, 61, 63\} \ .$$



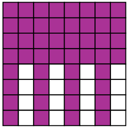
(a) *For* MIMC_3.



(b) *For* MIMC_7.



(c) *For* MIMC_{15}.



(d) *For* MIMC_{31}.

Proposition

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

$$\forall\, i \in \mathcal{E}_{d,r}, \ i \bmod 2^{j+1} \in \left\{0, 1, \dots 2^j\right\} \ \mathrm{U} \ \left\{2^j + 2\gamma, \gamma = 1, 2, \dots 2^{j-1} - 1\right\} \ .$$

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

- For MIMC_5

$$i \bmod 4 \in \{0, 1\} \ .$$

- For MIMC_9

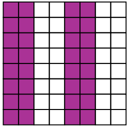
$$i \bmod 8 \in \{0, 1\} \ .$$

- For MIMC_{17}

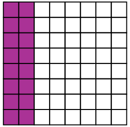
$$i \bmod 16 \in \{0, 1\} \ .$$

- For MIMC_{33}

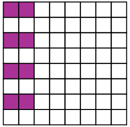
$$i \bmod 32 \in \{0, 1\} \ .$$



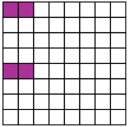
(a) *For* MIMC_5.



(b) *For* MIMC_9.



(c) *For* MIMC_{17}.



(d) *For* MIMC_{33}.

Proposition

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

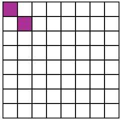
$$\forall\, i \in \mathcal{E}_{d,r},\ i \bmod 2^j \in \{0, 1\} \ .$$

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

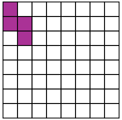
Corollary

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

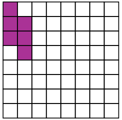
$$\begin{cases} i \bmod 2^{2j} \in \{\{\gamma 2^j, (\gamma+1)2^j + 1\},\ \gamma = 0, \ldots r-1\} & \text{if } r \leq 2^j\ , \\ i \bmod 2^j \in \{0, 1\} & \text{if } r \geq 2^j\ . \end{cases}$$



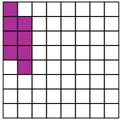
(a) *Round 1*



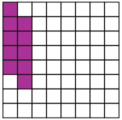
(b) *Round 2*



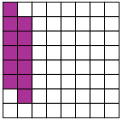
(c) *Round 3*



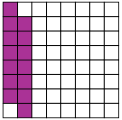
(d) *Round 4*



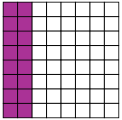
(a) *Round 5*



(b) *Round 6*



(c) *Round 7*



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

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

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

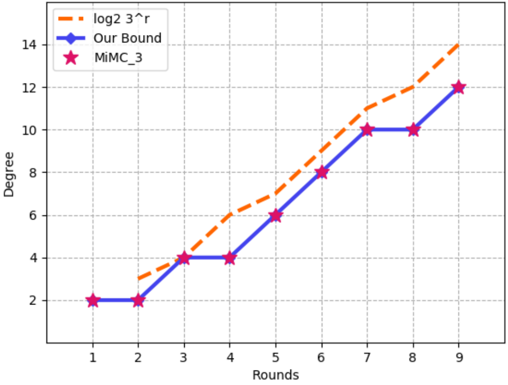
Corollary

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

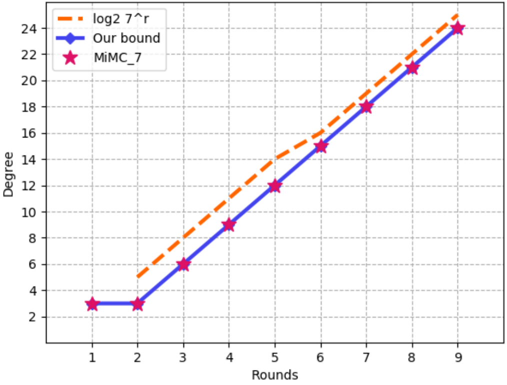
$$B_d^r \leq \begin{cases} \lfloor r \log_2 d \rfloor - j & \text{if } \lfloor r \log_2 d \rfloor \bmod j = 0 \ , \\ \lfloor r \log_2 d \rfloor - (\lfloor r \log_2 d \rfloor \bmod j) & \text{else} \ . \end{cases}$$

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

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

Proposition

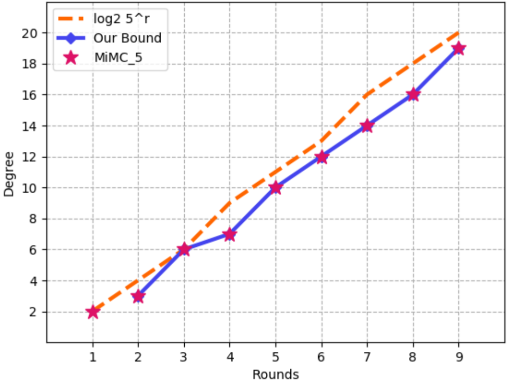
Let $d = 2^j + 1$ s.t. $j > 1$. Then if $r > 1$:

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

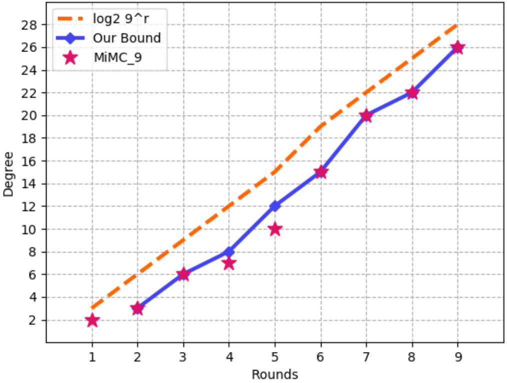
The bound can be refined on the first rounds!

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

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 $k_r = 1 \bmod 2$,

$$\omega_r = 2^{k_r} - 5 \in \mathcal{E}_{3,r},$$

⋆ if $k_r = 0 \bmod 2$,

$$\omega_r = 2^{k_r} - 7 \in \mathcal{E}_{3,r}.$$

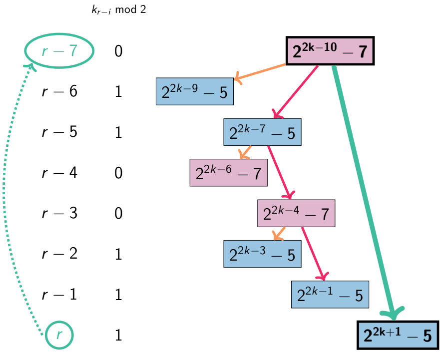
Exact degree

Maximum-weight exponents:

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

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

- $\star$ if $k_r = 1 \bmod 2$,
$$\omega_r = 2^{k_r} - 5 \in \mathcal{E}_{3,r},$$
- $\star$ if $k_r = 0 \bmod 2$,
$$\omega_r = 2^{k_r} - 7 \in \mathcal{E}_{3,r}.$$



Constructing exponents.

Exact degree

Maximum-weight exponents:

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

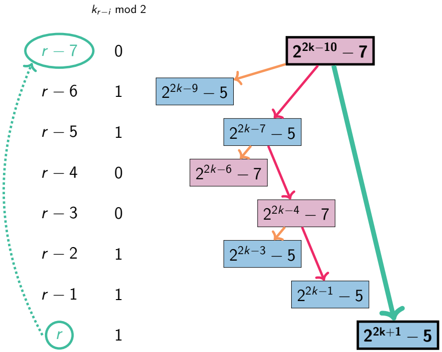
$\forall r \in \{4, \ldots, 16265\} \backslash \mathcal{F}$ with $\mathcal{F} = \{465, 571, \ldots\}$:

- $\star$ if $k_r = 1 \bmod 2$,

$$\omega_r = 2^{k_r} - 5 \in \mathcal{E}_{3,r},$$

- $\star$ if $k_r = 0 \bmod 2$,

$$\omega_r = 2^{k_r} - 7 \in \mathcal{E}_{3,r}.$$



Constructing exponents.

$$\boxed{\text{In most cases,} \quad \exists \ell \text{ s.t.} \quad \omega_{r-\ell} \in \mathcal{E}_{3,r-\ell} \Rightarrow \omega_r \in \mathcal{E}_{3,r}}$$

Sporadic Cases

Observation

Let $k_{3,r} = \lfloor r \log_2 3 \rfloor$. If $4 \leq r \leq 16265$, then

$$3^r > 2^{k_{3,r}} + 2^r \,.$$

Observation

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

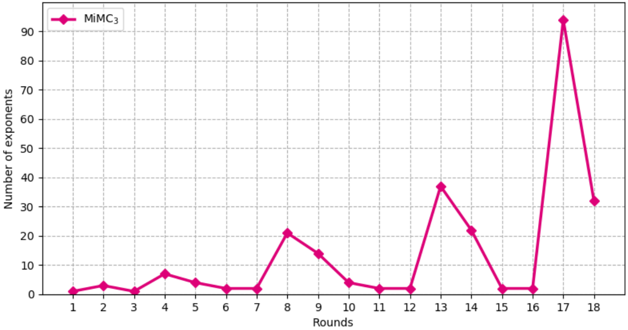
$$\forall x \in \mathbb{Z}/3^t\mathbb{Z},\ \exists \varepsilon_2, \ldots, \varepsilon_{2t+2} \in \{0,1\},\ \text{s.t. } x = \sum_{j=2}^{2t+2} \varepsilon_j 4^j \bmod 3^t \,.$$

Is it true for any t?

Should we consider more ε_j for larger t?

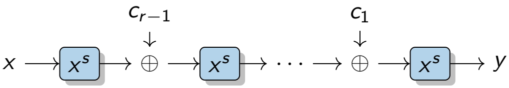
More maximum-weight exponents

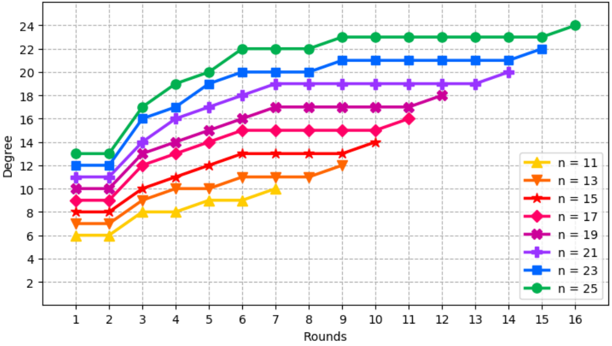
r	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$k_{3,r}$	1	3	4	6	7	9	11	12	14	15	17	19	20	22	23	25	26	28
$b_{3,r}$	1	1	0	0	1	1	1	0	0	1	1	1	0	0	1	1	0	0



Study of MiMC_3^{-1}

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





First plateau

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

- Round 1:

$$B_s^1 = \mathrm{wt}(s) = (n+1)/2$$

- Round 2:

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

Proposition

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

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

Next Rounds

Proposition [Boura and Canteaut, IEEE13]

$\forall i \in [1, n-1]$, if the algebraic degree of encryption is $\deg^a(F) < (n-1)/i$, then the algebraic degree of decryption is $\deg^a(F^{-1}) < n - i$

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

In particular:

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