Mathematical tools to design and analyze the security of Arithmetization-Oriented symmetric primitives

Clémence Bouvier [1,2]

including joint works with Pierre Briaud, Anne Canteaut, Pyrros Chaidos, Léo Perrin, Robin Salen, Vesselin Velichkov and Danny Willems

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

June 7th, 2023

Content

Mathematical tools to design and analyze the security of Arithmetization-Oriented symmetric primitives.

1. Preliminaries
   - Symmetric cryptography
   - Emerging uses
2. Algebraic Degree of MiMC
   - Missing exponents
   - Bound on the degree
   - Higher-Order differential attacks
3. Anemoi
   - CCZ-equivalence
   - New S-box: Flystel
   - SPN construction

Symmetric cryptography

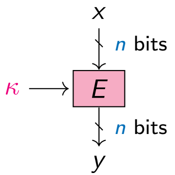
We assume that a key is already shared.

- ⋆ Stream cipher
- ⋆ Block cipher

Symmetric cryptography

We assume that a key is already shared.

- ⋆ Stream cipher
- ⋆ Block cipher



Block cipher

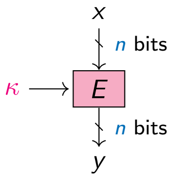
- ⋆ input: $x \in \mathbb{F}_{2^n}$
- ⋆ parameter: key $\kappa \in \mathbb{F}_{2^k}$
- ⋆ output: $y \in \mathbb{F}_{2^n}$ s.t. $y = E_\kappa(x)$
- ⋆ symmetry: E and E^{-1} use the same κ

$$\begin{aligned} E_\kappa : \mathbb{F}_{2^n} &\to \mathbb{F}_{2^n} \\ x &\mapsto y = E_\kappa(x) \end{aligned}$$

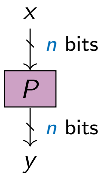
Symmetric cryptography

We assume that a key is already shared.

- ⋆ Stream cipher
- ⋆ Block cipher



Block cipher



Random permutation

- ⋆ input: $x \in \mathbb{F}_{2^n}$
- ⋆ parameter: key $\kappa \in \mathbb{F}_{2^k}$
- ⋆ output: $y \in \mathbb{F}_{2^n}$ s.t. $y = E_\kappa(x)$
- ⋆ symmetry: E and E^{-1} use the same κ

$$\begin{aligned} E_\kappa : \mathbb{F}_{2^n} &\to \mathbb{F}_{2^n} \\ x &\mapsto y = E_\kappa(x) \end{aligned}$$

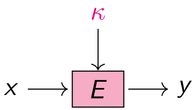
$$\begin{aligned} P : \mathbb{F}_{2^n} &\to \mathbb{F}_{2^n} \\ x &\mapsto y = P(x) \end{aligned}$$

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

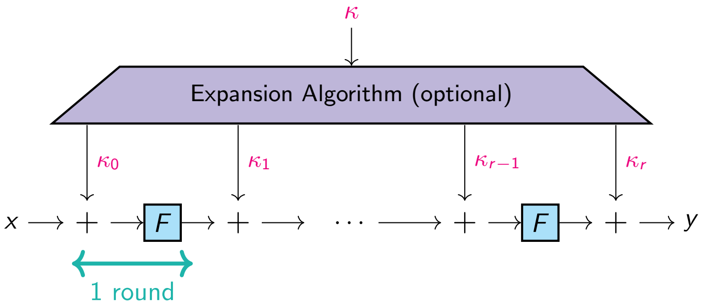
Iterated constructions

⇒ How to build a block cipher?

By iterating a round function.



⇒

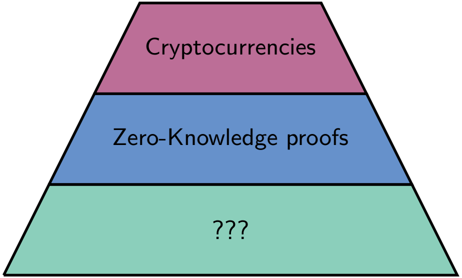


Performance constraints! The primitive must be fast.

A need of new primitives

Protocols requiring new primitives:

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



Problem: Designing new symmetric primitives

And analyse their security!

Toy example: the sudoku

	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: the sudoku

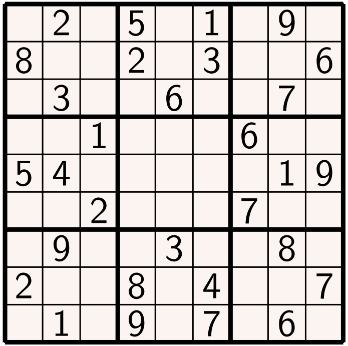
	2		5		1		9	
8			2		3			6
	3			6			7	
		1				6		
5	4						1	9
		2				7		
	9			3			8	
2			8		4			7
	1		9		7		6	

Unsolved Sudoku

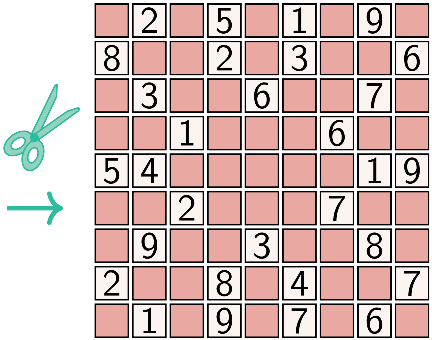
4	2	*6*	5	*7*	1	*3*	9	*8*
8	*5*	*7*	2	*9*	3	*1*	*4*	6
1	3	*9*	*4*	6	*8*	*2*	7	*5*
9	*7*	1	*3*	*8*	*5*	6	*2*	*4*
5	4	*3*	*7*	*2*	*6*	*8*	1	9
6	*8*	2	*1*	*4*	*9*	7	*5*	*3*
7	9	*4*	*6*	3	*2*	*5*	8	*1*
2	*6*	*5*	8	*1*	4	*9*	*3*	7
3	1	*8*	9	*5*	7	*4*	6	*2*

Solved Sudoku

Toy example: the sudoku



Unsolved Sudoku

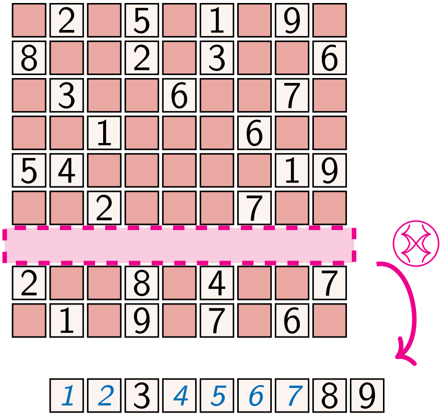


Grid cutting

Toy example: the sudoku

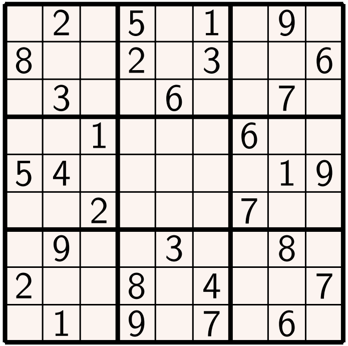
	2		5		1		9	
8			2		3			6
	3			6			7	
		1				6		
5	4						1	9
		2				7		
	9			3			8	
2			8		4			7
	1		9		7		6	

Unsolved Sudoku

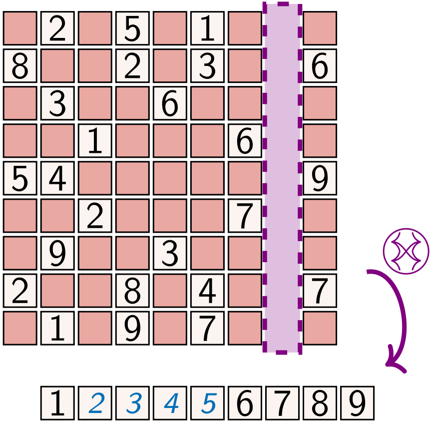


Rows checking

Toy example: the sudoku



Unsolved Sudoku

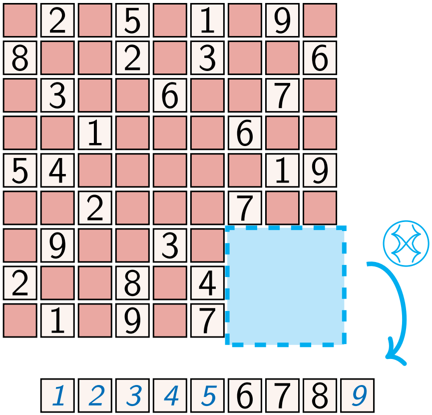


Columns checking

Toy example: the sudoku

	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



Squares checking

Performance metric

Need to **verify efficiently** that $y == E(x)$.

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

Performance metric

Need to **verify efficiently** that $y == E(x)$.

What does “efficient” mean for Zero-Knowledge Proofs?

“It depends”

For R1CS: Minimize the number of multiplications

Examples:

- *? R1CS contraints* for
$$y = (ax + b)^3(cx + d) + ex$$
- *? R1CS contraints* for
$$y = x^7$$

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 $\log_2 p = 255$

  $p = 52435875175126190479447740508185965837690552500527637822603658699938581184513$

- ⋆ Curve BLS12-377 $\log_2 p = 253$

  $p = 8444461749428370424248824938781546531375899335154063827935233455917409239041$

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

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

Arithmetization-friendly

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

Decades of Cryptanalysis

$\leq$ 5 years of Cryptanalysis

N...

"Usual" case

$$y \leftarrow E(x)$$

- $\star$ Optimized for: implementation in software/hardware

Arithmetization-friendly

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

- $\star$ Optimized for: integration within advanced protocols

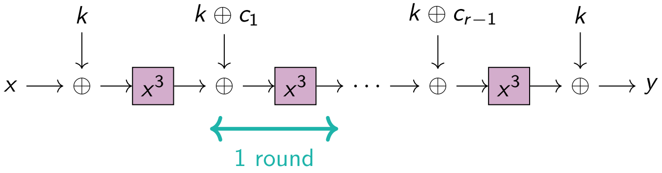
1 Preliminaries
- Symmetric cryptography
- Emerging uses

2 Algebraic Degree of MiMC
- Missing exponents
- Bound on the degree
- Higher-Order differential attacks

3 Anemoi
- CCZ-equivalence
- New S-box: Flystel
- SPN construction

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



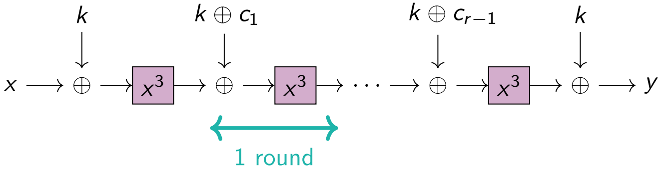
The block cipher MiMC

- 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.



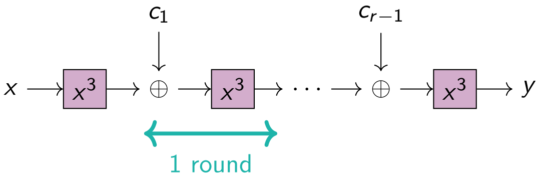
The block cipher MiMC

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

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

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

Definition

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

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

Algebraic degree - 1st definition

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

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

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

Definition

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

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

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

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

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

Algebraic degree - 1st definition

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

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

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

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

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

Definition

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

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

Algebraic degree - 2nd definition

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

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

Definition

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

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

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 $= n - 1$

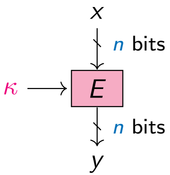
Higher-Order differential attacks

Exploiting a low algebraic degree

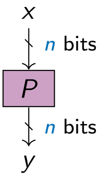
For any affine subspace $\mathcal{V} \subset \mathbb{F}_2^n$ with $\dim \mathcal{V} \geq \deg^a(F) + 1$, we have a 0-sum distinguisher:

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

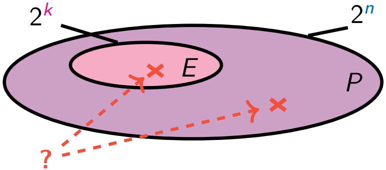
Random permutation: degree $= n - 1$



Block cipher



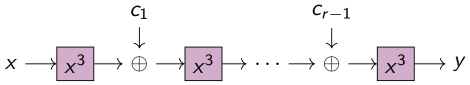
Random permutation



First Plateau

Round i of MiMC_3

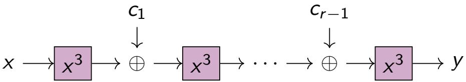
$$x \mapsto (x + c_{i-1})^3$$



First Plateau

Round i of MiMC_3

$$x \mapsto (x + c_{i-1})^3$$



For r rounds:

- ⋆ Upper bound [Eichlseder et al., AC20]:

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

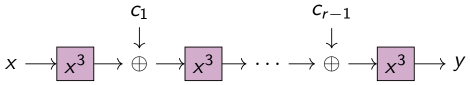
- ⋆ Aim: determine

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

First Plateau

Round i of MiMC_3

$$x \mapsto (x + c_{i-1})^3$$



For r rounds:

- ⋆ Upper bound [Eichlseder et al., AC20]:

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

- ⋆ Aim: determine

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

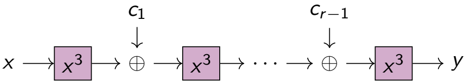
Definition

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

First Plateau

Round i of MiMC$_3$

$$x \mapsto (x + c_{i-1})^3$$



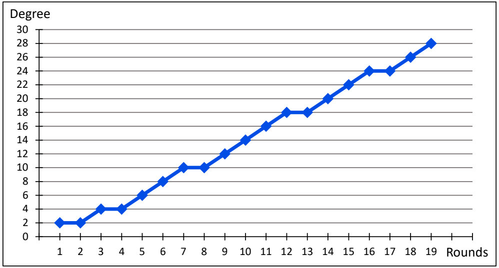
For r rounds:

- ⋆ Upper bound [Eichlseder et al., AC20]:

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

- ⋆ Aim: determine

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



Algebraic degree observed for $n = 31$.

Definition

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

Missing exponents

Proposition

Set of exponents that might appear in the polynomial:

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

Missing exponents

Proposition

Set of exponents that might appear in the polynomial:

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

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

Proposition

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

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

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

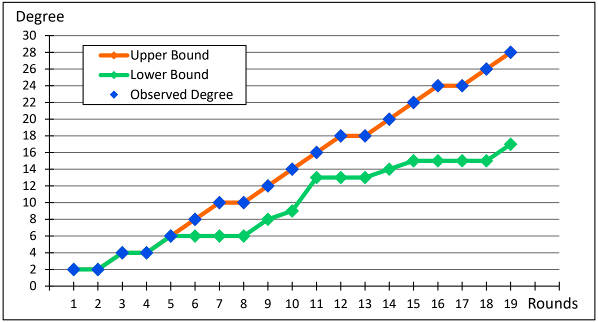
After r rounds of MiMC, the algebraic degree is

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

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

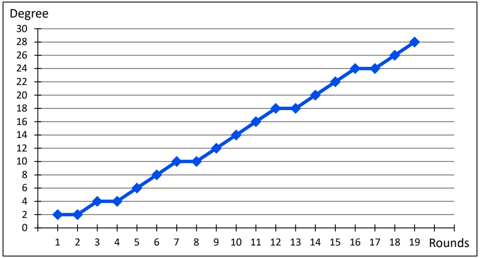
$$B_3^r \geq \max\{wt(3^i), i \leq r\}$$

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

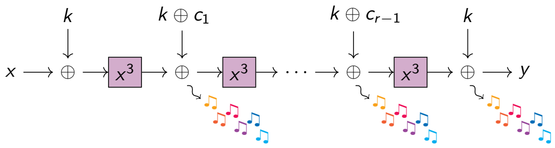
$$\Rightarrow \text{denominators of semiconvergents of } \log_2(3) \simeq 1.5849625$$

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

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

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

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



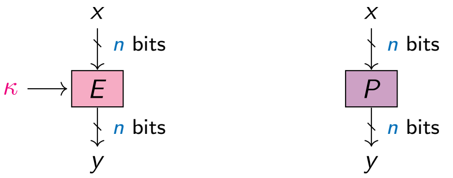
Higher-Order differential attacks

Exploiting a low algebraic degree

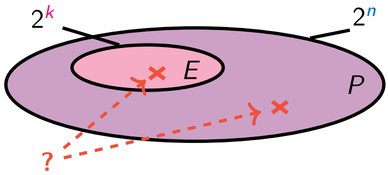
For any affine subspace $\mathcal{V} \subset \mathbb{F}_2^n$ with $\dim \mathcal{V} \geq \deg^a(F) + 1$, we have a 0-sum distinguisher:

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

Random permutation: degree $= n - 1$

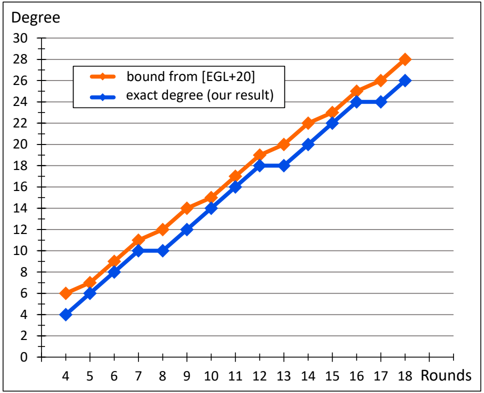


Block cipher *Random permutation*



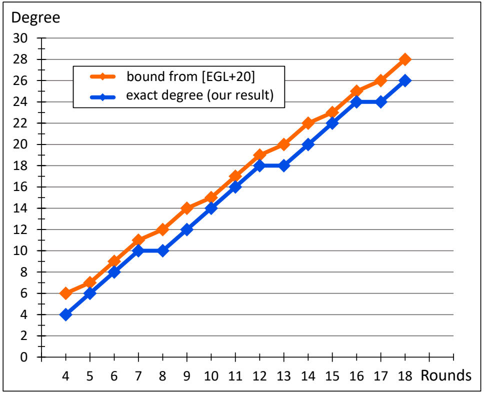
Comparison to previous work

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



Comparison to previous work

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



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

Futur work

Some open problems

- ⋆ Conjecture for maximum-weight exponents
- ⋆ Form of coefficients
- ⋆ Sparse univariate polynomials
- ⋆ Inverse transformation
- ⋆ SPN construction
- ⋆ . . .

Sporadic Cases

Observation

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

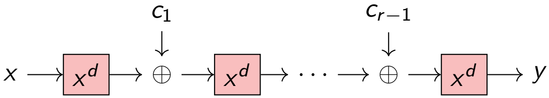
$$\forall x \in \mathbb{Z}/3^t\mathbb{Z},\ \exists \varepsilon_2, \ldots, \varepsilon_{2t+2} \in \{0,1\},\ \text{s.t. } x = \sum_{j=2}^{2t+2} \varepsilon_j 4^j \bmod 3^t\ .$$

Is it true for any t?

Should we consider more ε_j for larger t?

Sparse Univariate Polynomials

Gold Functions: $x^3, x^5, x^9, \ldots$



Proposition

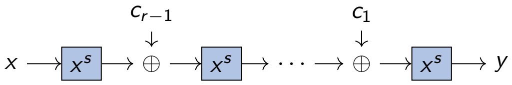
Let $\mathcal{E}_{d,r}$ be the set of exponents in the univariate form of $\mathrm{MIMC}_d[r]$, where $d = 2^j + 1$ and $d > 3$. Then:

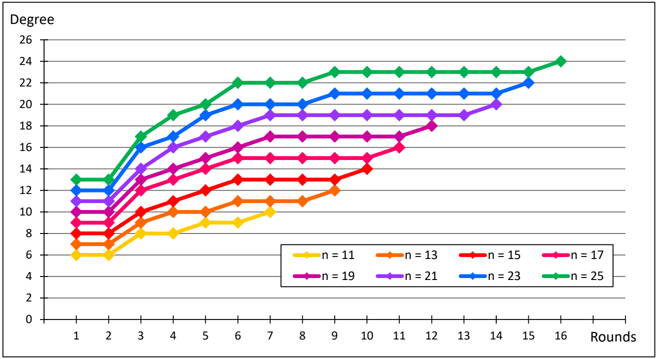
$$\forall\, i \in \mathcal{E}_{d,r},\ i \bmod 2^j \in \{0, 1\}\ .$$

- ⋆ for MIMC_5 : $i \equiv 0, 1 \mod 4$
- ⋆ for MIMC_9 : $i \equiv 0, 1 \mod 8$
- ⋆ for MIMC_{17} : $i \equiv 0, 1 \mod 16$

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:

$$B_s^1 = wt(s) = (n+1)/2$$

- Round 2:

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

Proposition

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

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

Next Rounds

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

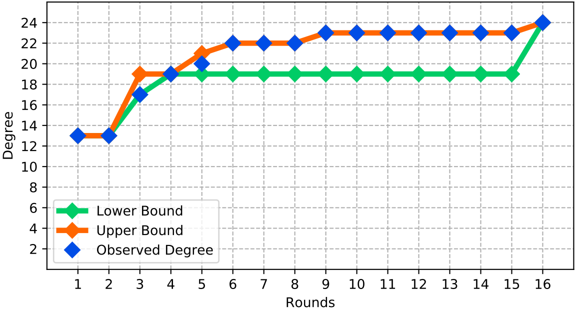
Proposition [BC13]

$\forall i \in [1, n-1]$, 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:

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



1. Preliminaries
   - Symmetric cryptography
   - Emerging uses
2. Algebraic Degree of MiMC
   - Missing exponents
   - Bound on the degree
   - Higher-Order differential attacks
3. Anemoi
   - CCZ-equivalence
   - New S-box: Flystel
   - SPN construction

Why Anemoi?

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

Why Anemoi?

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

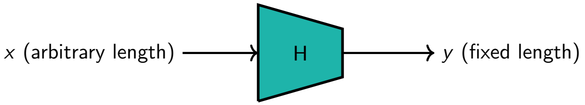
  ⇓

- ⋆ **Anemoi**
  Greek gods of winds

Hash Functions

Definition

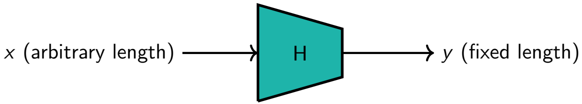
Hash function: $H : \mathbb{F}_q^\ell \to \mathbb{F}_q^h, x \mapsto y = H(x)$ where ℓ is arbitrary and h is fixed.



Hash Functions

Definition

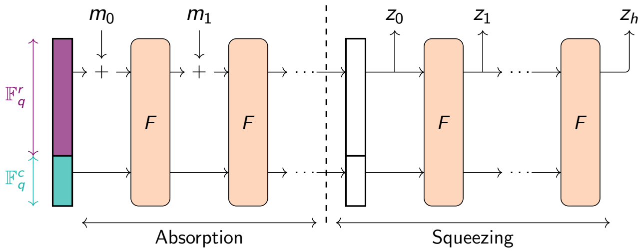
Hash function: $H : \mathbb{F}_q^\ell \to \mathbb{F}_q^h, x \mapsto y = H(x)$ where ℓ is arbitrary and h is fixed.



Sponge construction

Parameters:

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



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.

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

$y == E(x)$ $\rightsquigarrow$ 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

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

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

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

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

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

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, $\mathcal{A}(x) = \mathcal{L}(x) + c$.

Differential and Linear properties

Let $F : \mathbb{F}_q^m \rightarrow \mathbb{F}_q^m$

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

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

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

$$\mathcal{W}_F = \max_{a, b \neq 0} \left| \sum_{x \in \mathbb{F}_2^m} (-1)^{a \cdot x + b \cdot F(x)} \right|$$

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

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

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

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

CCZ-equivalence

Definition [Carlet, Charpin, Zinoviev, DCC98]

$F : \mathbb{F}_q \to \mathbb{F}_q$ 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: $\delta_F = \delta_G$.

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: $\mathcal{W}_F = \mathcal{W}_G$.

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]

$F : \mathbb{F}_q \rightarrow \mathbb{F}_q$ 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, $\mathcal{A}(x) = \mathcal{L}(x) + c$.

- ⋆ 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]

$F : \mathbb{F}_q \to \mathbb{F}_q$ 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: $\mathcal{W}_F = \mathcal{W}_G$.
- ⋆ 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.

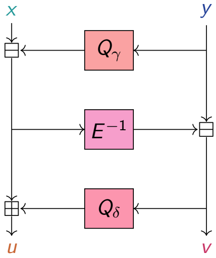
The Flystel

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

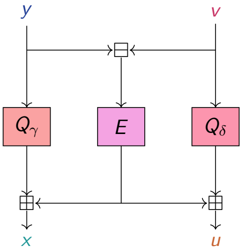
Open Flystel $\mathcal{H}$.

High-degree permutation



Closed Flystel $\mathcal{V}$.

Low-degree function



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

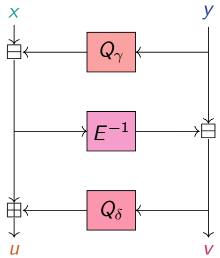
$$\begin{cases} x &= Q_\gamma(y) + E(y - v) \\ u &= Q_\delta(v) + E(y - v) \end{cases}$$

The Flystel

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

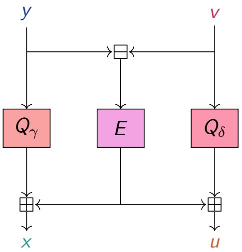
Open Flystel $\mathcal{H}$.

High-degree permutation



Closed Flystel $\mathcal{V}$.

Low-degree function



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

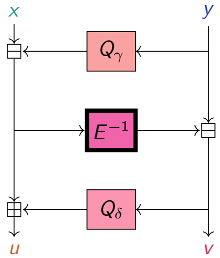
$$\begin{cases} x &= Q_\gamma(y) + E(y - v) \\ u &= Q_\delta(v) + E(y - v) \end{cases}$$

Advantage of CCZ-equivalence

- High Degree Evaluation.

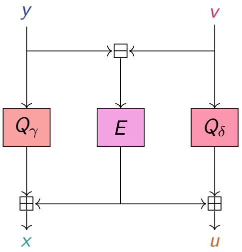
Open Flystel $\mathcal{H}$.

High-degree permutation



Closed Flystel $\mathcal{V}$.

Low-degree function



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

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

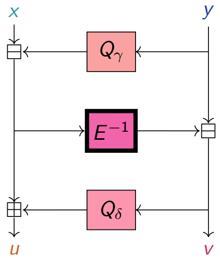
Advantage of CCZ-equivalence

⋆ High Degree Evaluation.

$$\begin{cases} p &= 4002409555221667393417789825735904156556882819939007885332 \\ & \quad 058136124031650490837864442687629129015664037894272559787 \\ \alpha &= 5 \\ \alpha^{-1} &= 3201927644177333914734231860588723325245506255951206308265 \\ & \quad 6465088992253203926702915541501033032125312303154180478 29 \end{cases}$$

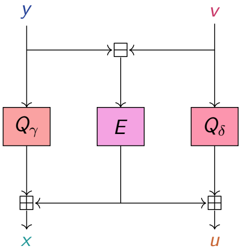
Open Flystel $\mathcal{H}$.

High-degree permutation



Closed Flystel $\mathcal{V}$.

Low-degree function



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

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

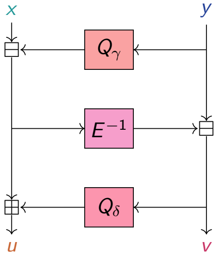
Advantage of CCZ-equivalence

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

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

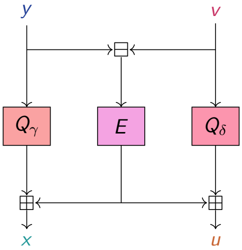
Open `Flystel` $\mathcal{H}$.

High-degree permutation



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

Low-degree function



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

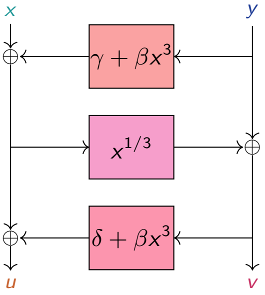
$$\begin{cases} x &= Q_\gamma(y) + E(y - v) \\ u &= Q_\delta(v) + E(y - v) \end{cases}$$

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

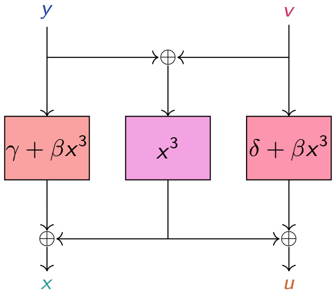
$$Q_\gamma(x) = \gamma + \beta x^3 , \quad Q_\delta(x) = \delta + \beta x^3 , \quad E(x) = x^3$$

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

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

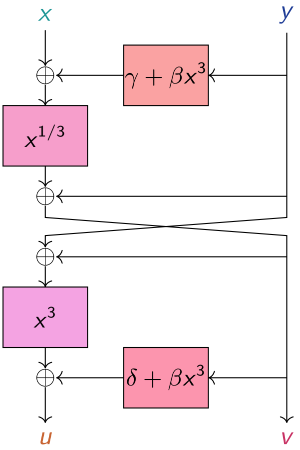


Open Flystel$_2$.



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 $\beta \neq 0$:

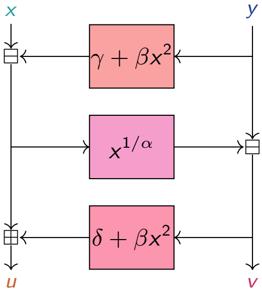
- Differential properties
  - $\texttt{Flystel}_2$: $\delta_{\mathcal{H}} = \delta_{\mathcal{V}} = 4$
- Linear properties
  - $\texttt{Flystel}_2$: $\mathcal{W}_{\mathcal{H}} = \mathcal{W}_{\mathcal{V}} = 2^{n+1}$
- Algebraic degree
  - Open $\texttt{Flystel}_2$: $\deg_{\mathcal{H}} = n$
  - Closed $\texttt{Flystel}_2$: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

Flystel in $\mathbb{F}_p$

$$Q_\gamma(x) = \gamma + \beta x^2 \ , \quad Q_\delta(x) = \delta + \beta x^2 \ , \quad E(x) = x^\alpha$$

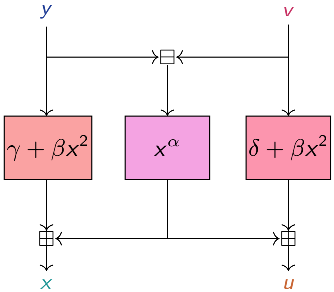
$$\mathcal{H} : \begin{cases} \mathbb{F}_p \times \mathbb{F}_p & \to \mathbb{F}_p \times \mathbb{F}_p \\ (x, y) & \mapsto \Big(x - \beta y^2 - \gamma + \beta \left(y - (x - \beta y^2 - \gamma)^{1/\alpha} \right)^2 + \delta \ , \\ & \qquad y - (x - \beta y^2 - \gamma)^{1/\alpha} \Big) \ . \end{cases}$$

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



Open Flystel$_p$.

usually
$\alpha = 3$ or 5.

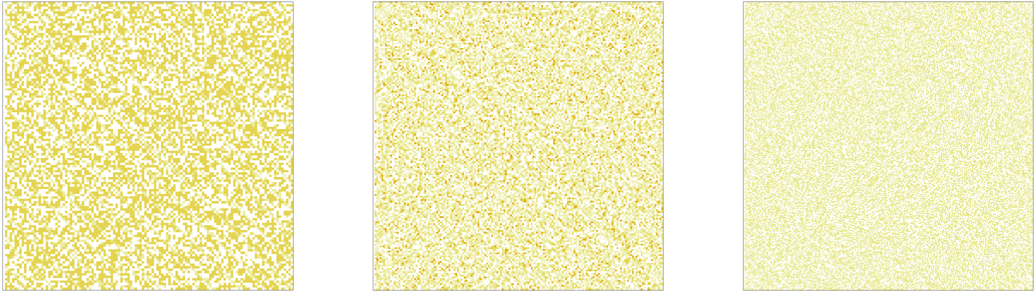


Closed Flystel$_p$.

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

⋆ Differential properties
$\texttt{Flystel}_\texttt{p}$ has a differential uniformity equals to $\alpha - 1$.

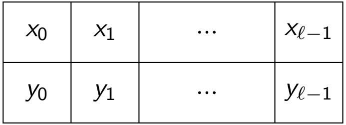
$$\delta_{\mathcal{H}} = \max_{a \neq 0, b} \left| \{ x \in \mathbb{F}_p^2, \mathcal{H}(x+a) - \mathcal{H}(x) = b \} \right| = \alpha - 1$$



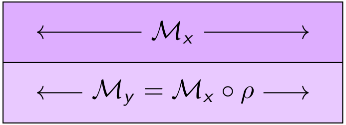
(a) *when $p = 11$ and $\alpha = 3$.* **(b)** *when $p = 13$ and $\alpha = 5$.* **(c)** *when $p = 17$ and $\alpha = 3$.*

The SPN (Substitution-Permutation Network) Structure

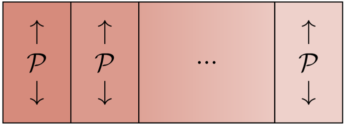
The internal state of Anemoi and its basic operations.



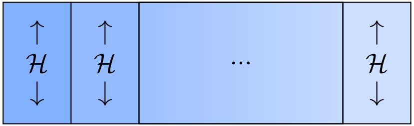
(a) *Internal state*



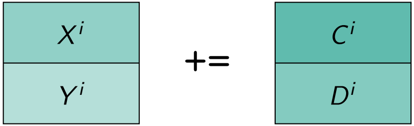
(b) *The diffusion layer $\mathcal{M}$.*



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



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



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

SPN - mathematical point of view

Let

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

Internal state of Anemoi:

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

Addition of constants and the linear layer:

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

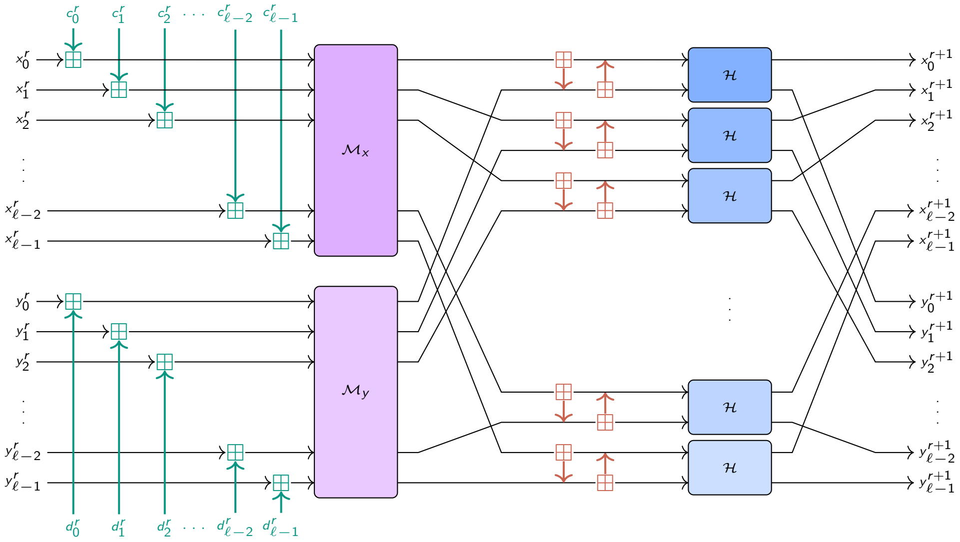
The Pseudo Hadamard Transform:

$$\begin{pmatrix} X \\ Y \end{pmatrix} \mapsto \begin{pmatrix} {}^t\mathcal{P}(x_0, y_0) & \dots & {}^t\mathcal{P}(x_{\ell-1}, y_{\ell-1}) \end{pmatrix} \quad \text{where} \quad \mathcal{P} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} .$$

And the S-Box layer:

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

The SPN Structure



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

Futur work

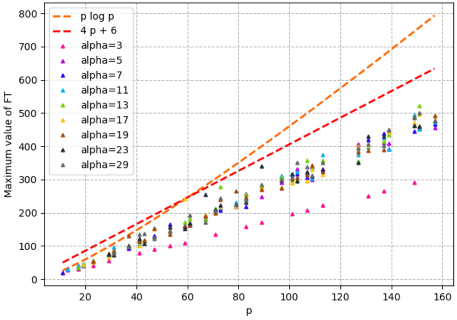
Some open problems

- Conjecture for the linearity
- Flystel with more branches
- ...

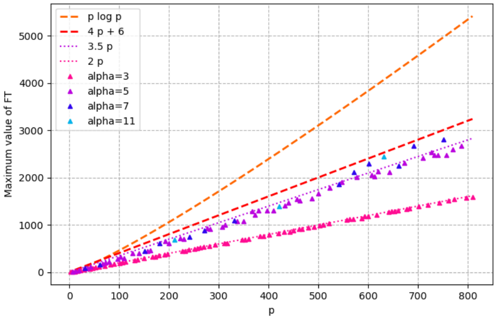
Properties of Flystel in $\mathbb{F}_p$

- Linear properties

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



(a) *For different α.*



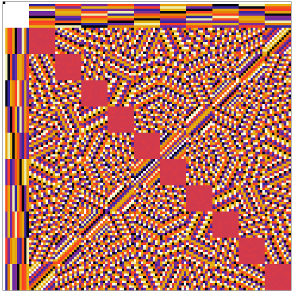
(b) *For the smallest α.*

Conjecture for the linearity.

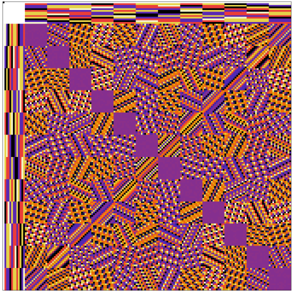
Properties of Flystel in $\mathbb{F}_p$

⋆ Linear properties

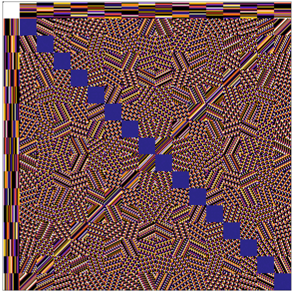
$$\mathcal{W} = \max_{a,b \neq 0} \left| \sum_{x \in \mathbb{F}_p^2} exp\left(\frac{2\pi i(\langle a, x\rangle - \langle b, F(x)\rangle)}{p} \right) \right| \leq p \log p \ ?$$



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



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



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

LAT of $\texttt{Flystel}_p$*.*

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!