When Cohomology Meets Linearity

AOPs in Therapy

Clémence Bouvier

Université de Lorraine, CNRS, Inria, LORIA

CARAMBA Team meeting, Nancy, France
June 19th, 2025

New symmetric primitives

What are AOPs?

New symmetric primitives

What are AOPs?

Appellations d'Origine Protégée ?

Munster

What are AOPs?

Appellations d'Origine Protégée ?

Munster

Arithmetization-Oriented Primitives!

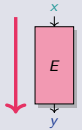
New symmetric primitives for

- ⋆ **MPC**: Multiparty Computation
- ⋆ **FHE**: Fully Homomorphic Encryption
- ⋆ **ZK**: Systems of Zero-Knowledge proofs

Comparison with the traditional case

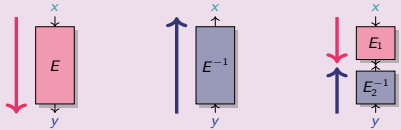
Traditional case

$y \leftarrow E(x)$



Arithmetization-oriented

$y \leftarrow E(x)$ and $y == E(x)$



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

Cryptanalysis

Decades of analysis

Arithmetization-oriented

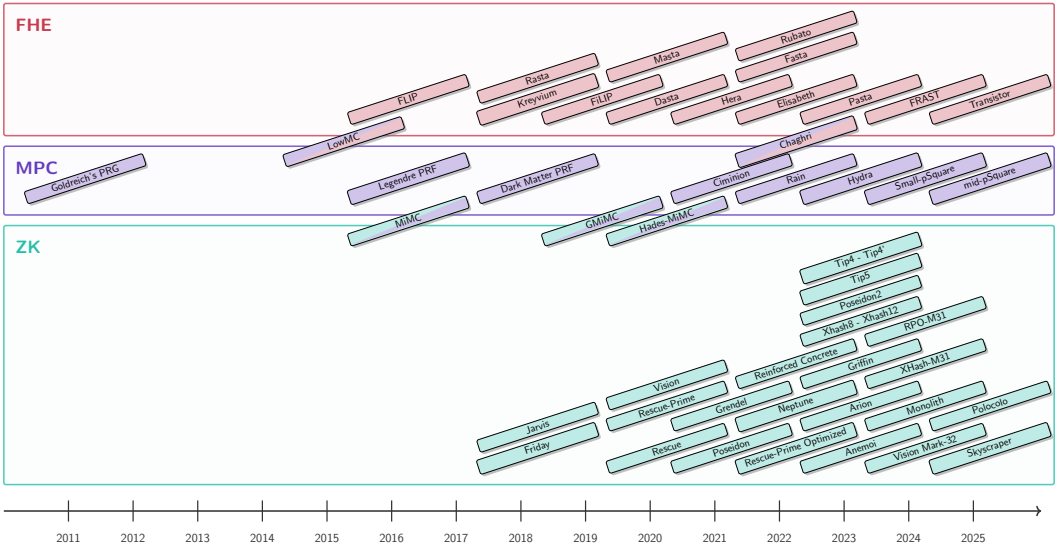
$$y \leftarrow E(x) \quad \text{and} \quad y == E(x)$$

- ⋆ 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

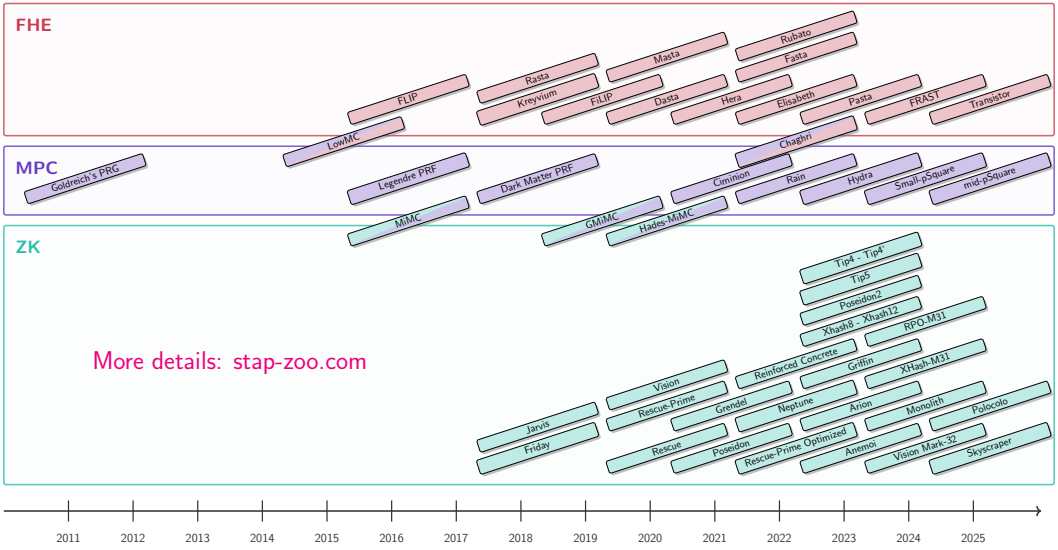
Cryptanalysis

≤ 8 years of analysis

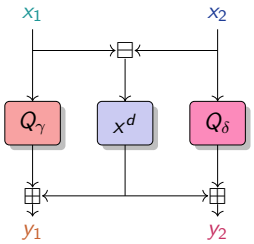
Many new symmetric primitives



Many new symmetric primitives



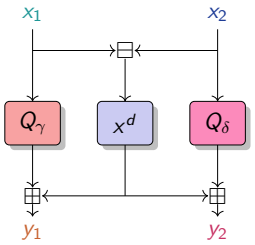
Past works



Closed Flystel: $F : \mathbb{F}_q^2 \to \mathbb{F}_q^2, (x_1, x_2) \mapsto (y_1, y_2)$

- ⋆ Introduced by [C. Bouvier, P. Briaud, P. Chaidos, L. Perrin, R. Salen, V. Velichkov and D. Willems, CRYPTO 2023]
- ⋆ Building block of Anemoi
- ⋆ Degenerated case of Butterfly

Past works



Closed Flystel: $F : \mathbb{F}_q^2 \to \mathbb{F}_q^2, (x_1, x_2) \mapsto (y_1, y_2)$

- ⋆ Introduced by [C. Bouvier, P. Briaud, P. Chaidos, L. Perrin, R. Salen, V. Velichkov and D. Willems, CRYPTO 2023]
- ⋆ Building block of Anemoi
- ⋆ Degenerated case of Butterfly

Solving an open problem since 2014 on APN permutations over $\mathbb{F}_p^2$

Existence of APN permutations

F is Almost Perfect Nonlinear iff

$$\delta_F = \max_{a \neq 0, b} |\{x \in \mathbb{F}_p^m, F(x+a) - F(x) = b\}| = 2 .$$

Flystel in $\mathbb{F}_p$ with x^d: $\delta_{Flystel} \leq d - 1$

Recent cryptanalysis progress

- ⋆ Direct applications of results for exponential sums [T. Beyne and C. Bouvier, 2024]
- ⋆ Solving a conjecture on the linearity of the Flystel construction

Linearity bound

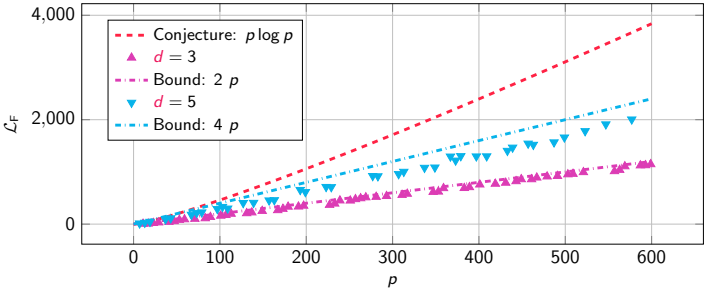
$$\mathcal{L}_{Flystel} = \max_{u \neq 0, v} \left| \sum_{x \in \mathbb{F}_p^2} e^{(2i\pi/p)(\langle v, F(x) \rangle - \langle u, x \rangle)} \right| \leq (d-1)p$$

Recent cryptanalysis progress

- ⋆ Direct applications of results for exponential sums [T. Beyne and C. Bouvier, 2024]
- ⋆ Solving a conjecture on the linearity of the Flystel construction

Linearity bound

$$\mathcal{L}_{Flystel} = \max_{u \neq 0, v} \left| \sum_{x \in \mathbb{F}_p^2} e^{(2i\pi/p)(\langle v, F(x)\rangle - \langle u, x\rangle)} \right| \leq (d-1)p$$



Work in progress

- ⋆ Can we provide detailed calculations of the cohomological spaces to refine bounds on the linearity of Butterfly-like constructions?
  (with C. Levrat)
- ⋆ Can we generalize to other constructions?
- ⋆ Is the Flystel an optimal construction? How to classify Butterfly-like constructions?
  [C. Bouvier, Fq 2025]

Work in progress

- ⋆ Can we provide detailed calculations of the cohomological spaces to refine bounds on the linearity of Butterfly-like constructions?
  (with C. Levrat)
- ⋆ Can we generalize to other constructions?
- ⋆ Is the Flystel an optimal construction? How to classify Butterfly-like constructions?
  [C. Bouvier, Fq 2025]

Thank you!