Arithmetization-Oriented Primitives

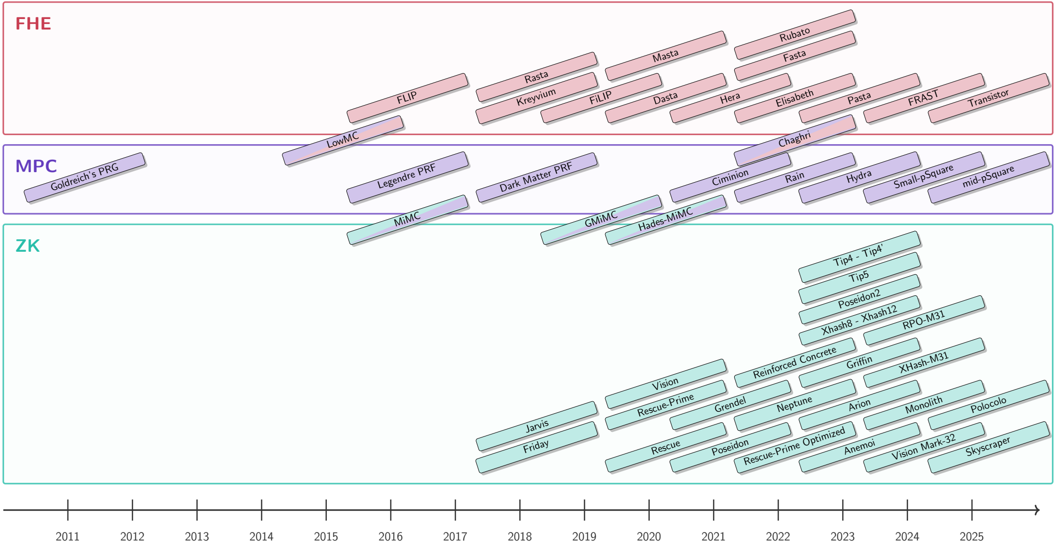
An overview of recent advances

Clémence Bouvier

Université de Lorraine, CNRS, Inria, LORIA

WRACH, Roscoff, France
April 24th, 2025

New symmetric primitives



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

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

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

Performance metric

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

"It depends"

Example

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

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

$t_0 = a \cdot x$

$t_1 = t_0 + b$

$t_2 = t_1 \times t_1$

$t_3 = t_2 \times t_1$

$t_4 = c \cdot x$

$t_5 = t_4 + d$

$t_6 = t_3 \times t_5$

$t_7 = e \cdot x$

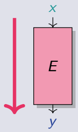
$t_8 = t_6 + t_7$

3 constraints

Comparison with the traditional case

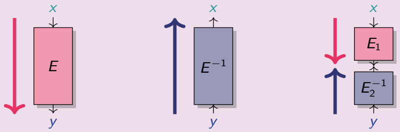
Traditional case

$$y \leftarrow E(x)$$



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:
  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

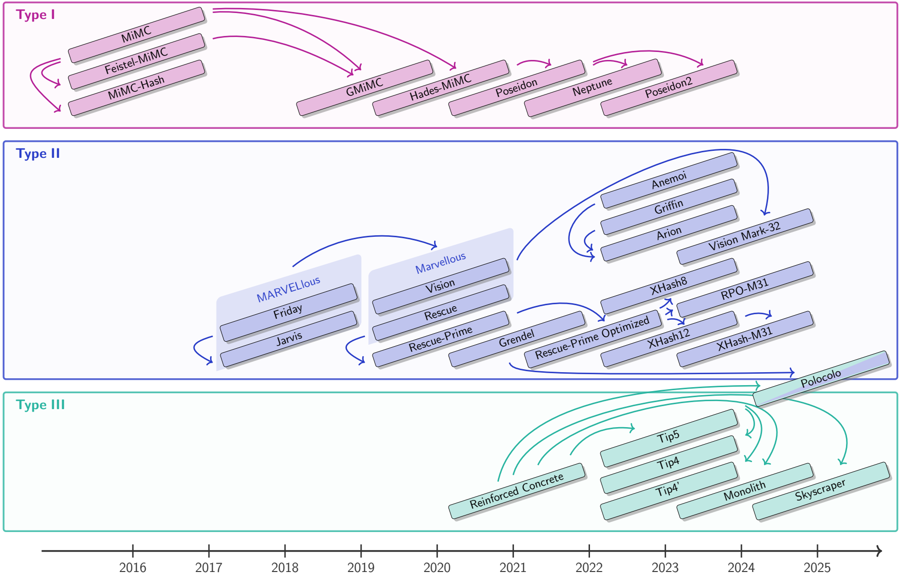
$$y \leftarrow E(x) \quad \text{and} \quad y == E(x)$$

- 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

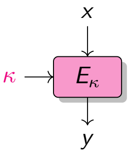
ZKP Primitives overview



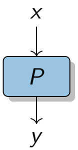
DESIGN

Iterated constructions

Block Ciphers $E_\kappa : \mathbb{F}_q^n \to \mathbb{F}_q^n$ (n fixed)



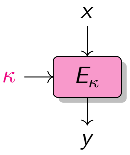
(a) *Block cipher*



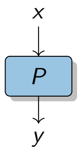
(b) *Random permutation*

Iterated constructions

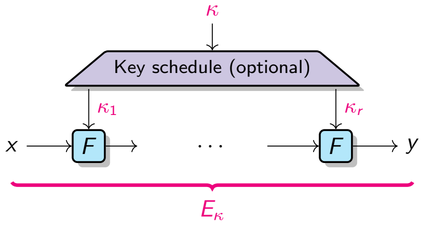
Block Ciphers $E_\kappa : \mathbb{F}_q^n \to \mathbb{F}_q^n$ (n fixed)



(a) *Block cipher*

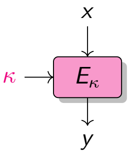


(b) *Random permutation*

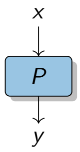


Iterated constructions

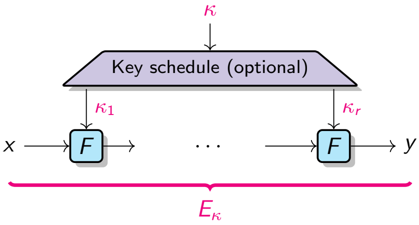
Block Ciphers $E_\kappa : \mathbb{F}_q^n \to \mathbb{F}_q^n$ (n fixed)



(a) *Block cipher*



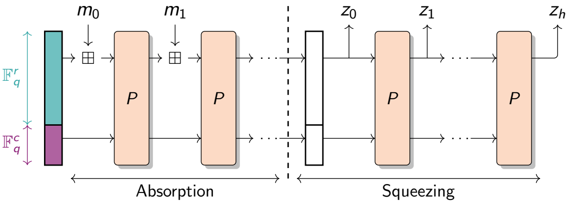
(b) *Random permutation*



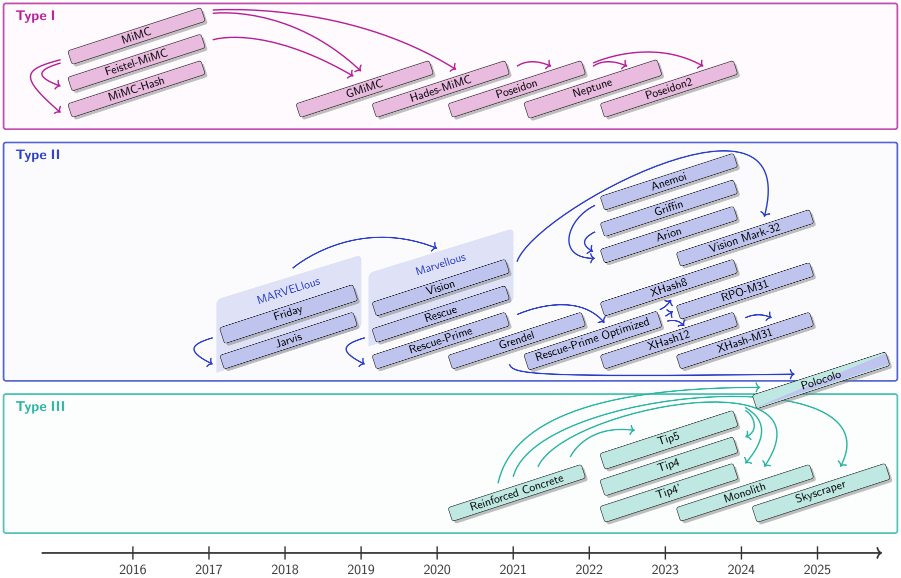
Hash functions $H : \mathbb{F}_q^\ell \to \mathbb{F}_q^h$ (ℓ arbitrary, h fixed)

Sponge construction

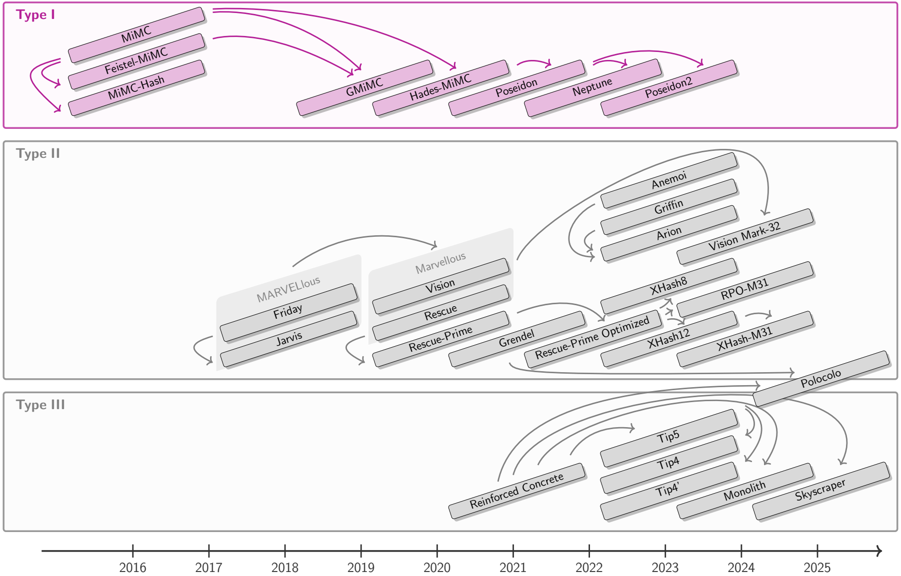
- ⋆ rate $r > 0$
- ⋆ capacity $c > 0$
- ⋆ permutation of $\mathbb{F}_q^n$ ($n = r + c$)



ZKP Primitives overview

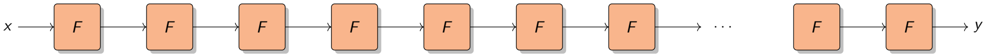


ZKP Primitives overview



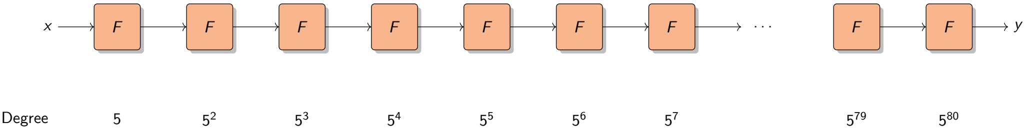
Type I

Low-Degree Primitives



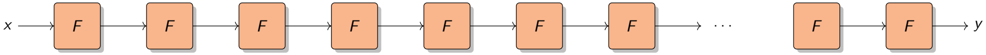
Type I

Low-Degree Primitives



Type I

Low-Degree Primitives

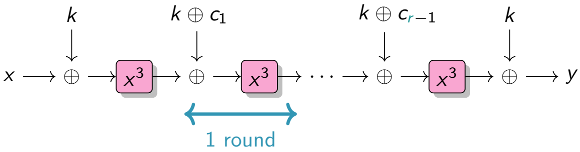


Degree	5	5^2	5^3	5^4	5^5	5^6	5^7	5^{79}	5^{80}
Constraints	3	3×2	3×3	3×4	3×5	3×6	3×7	3×79	3×80

MiMC / Feistel-MiMC

M. Albrecht, L. Grassi, C. Rechberger, A. Roy and T. Tiessen, 2016

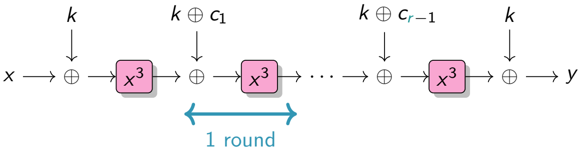
- ⋆ n-bit blocks (n odd ≈ 129): $x \in \mathbb{F}_{2^n}$
- ⋆ n-bit key: $k \in \mathbb{F}_{2^n}$
- ⋆ 82 rounds when $n = 129$

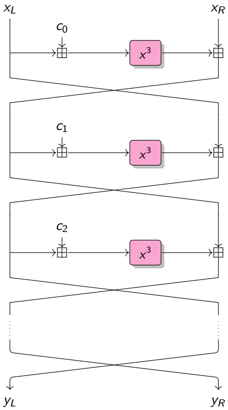


MiMC / Feistel-MiMC

M. Albrecht, L. Grassi, C. Rechberger, A. Roy and T. Tiessen, 2016

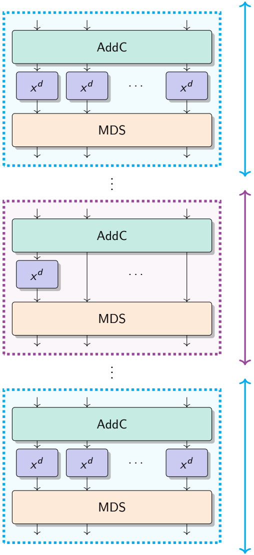
- ⋆ n-bit blocks (n odd ≈ 129): $x \in \mathbb{F}_{2^n}$
- ⋆ n-bit key: $k \in \mathbb{F}_{2^n}$
- ⋆ 82 rounds when $n = 129$





Feistel-MiMC

Poseidon



L. Grassi, D. Khovratovich, C. Rechberger, A. Roy and M. Schofnegger, 2021

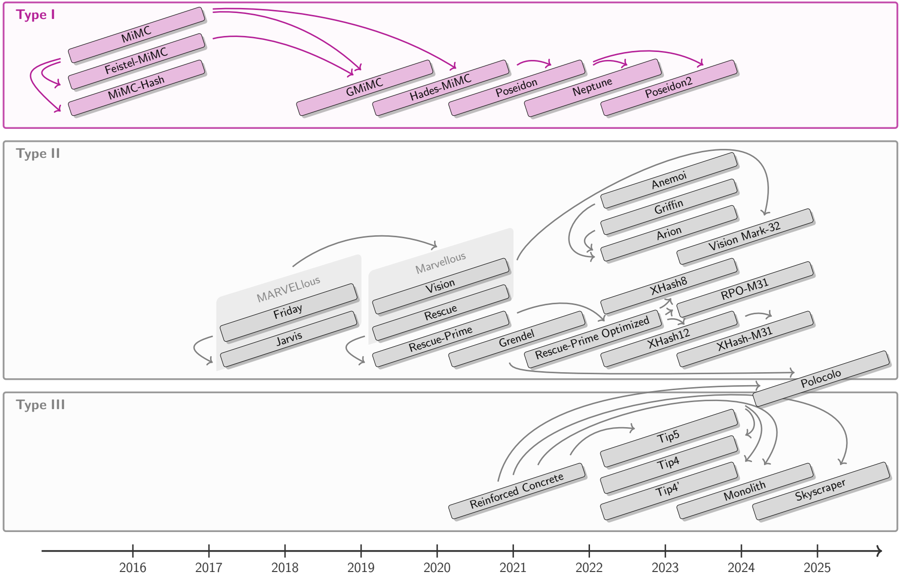
- ⋆ S-box:

$$x \mapsto x^3$$

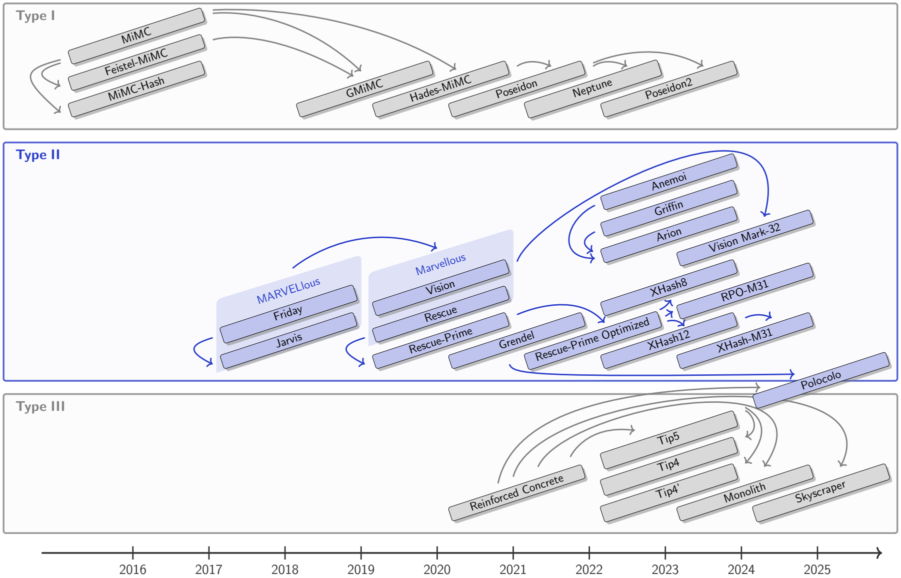
- ⋆ Nb rounds:

$$\begin{aligned} R &= 2 \times Rf + RP \\ &= 8 + (\text{from } 56 \text{ to } 84) \end{aligned}$$

ZKP Primitives overview

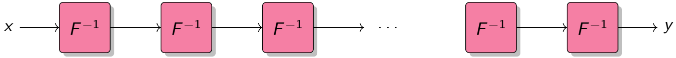


ZKP Primitives overview



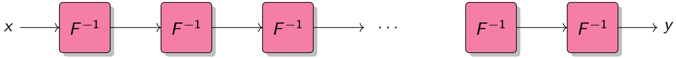
Type II

Primitives based on Equivalence



Type II

Primitives based on Equivalence



Degree 5^{-1} 5^{-2} 5^{-3} 5^{-19} 5^{-20}

Example

In $\mathbb{F}_p$ with

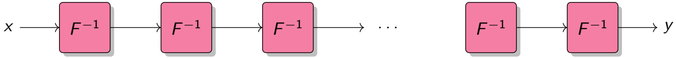
$$p = \texttt{0x73eda753299d7d483339d80809a1d80553bda402fffe5bfeffffffff00000001}$$

If $F(x) = x^5$ then $F^{-1}(x) = x^{5^{-1}}$ with

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

Type II

Primitives based on Equivalence



Degree	5^{-1}	5^{-2}	5^{-3}	5^{-19}	5^{-20}
Constraints	3×20	3×19	3×18	3×2	3

Example

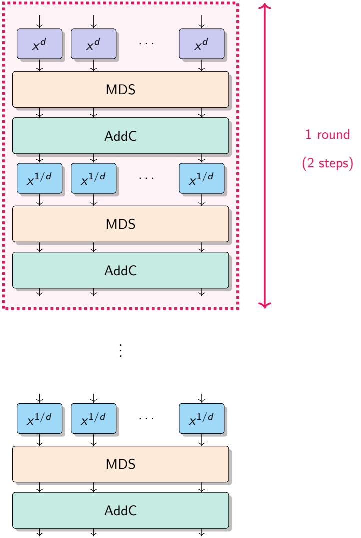
In $\mathbb{F}_p$ with

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

If $F(x) = x^5$ then $F^{-1}(x) = x^{5^{-1}}$ with

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

Rescue / Rescue-Prime



A. Aly, T. Ashur, E. Ben-Sasson, S. Dhooghe and A. Szepieniec, 2020

- S-box:

$$x \mapsto x^3 \quad \text{and} \quad x \mapsto x^{1/3}$$

- Nb rounds:

$$R = \text{from 8 to 26}$$

(2 S-boxes per round)

Anemoi

Need: verification using few multiplications.

⋆ **First approach:** evaluation using few multiplications, e.g. Poseidon [GKRRS21]

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

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

Anemoi

Need: verification using few multiplications.

⋆ **First approach:** evaluation using few multiplications, e.g. Poseidon [GKRRS21]

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

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

⋆ **First breakthrough:** using inversion, e.g. Rescue [AABDS20]

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

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

Anemoi

Need: verification using few multiplications.

- ⋆ **First approach:** evaluation using few multiplications, e.g. Poseidon [GKRRS21]

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

- ⋆ **First breakthrough:** using inversion, e.g. Rescue [AABDS20]

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

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

$y \leftarrow F(x)$ $\rightsquigarrow$ F: high degree $v == G(u)$ $\rightsquigarrow$ 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]

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

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

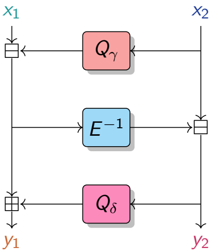
The FLYSTEL

C. Bouvier, P. Briaud, P. Chaidos, L. Perrin, R. Salen, V. Velichkov and D. Willems, 2023

Butterfly + Feistel ⇒ FLYSTEL

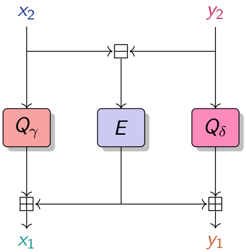
A 3-round Feistel-network with
$Q_\gamma : \mathbb{F}_q \to \mathbb{F}_q$ and $Q_\delta : \mathbb{F}_q \to \mathbb{F}_q$ two quadratic functions, and $E : \mathbb{F}_q \to \mathbb{F}_q$ a permutation

High-Degree permutation



Open FLYSTEL $\mathcal{H}$.

Low-Degree function



Closed FLYSTEL $\mathcal{V}$.

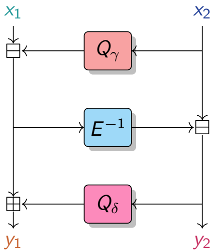
The FLYSTEL

C. Bouvier, P. Briaud, P. Chaidos, L. Perrin, R. Salen, V. Velichkov and D. Willems, 2023

Butterfly + Feistel ⇒ FLYSTEL

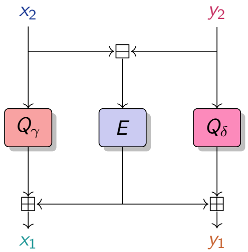
A 3-round Feistel-network with
$Q_\gamma : \mathbb{F}_q \to \mathbb{F}_q$ and $Q_\delta : \mathbb{F}_q \to \mathbb{F}_q$ two quadratic functions, and $E : \mathbb{F}_q \to \mathbb{F}_q$ a permutation

High-Degree permutation



Open FLYSTEL $\mathcal{H}$.

Low-Degree function



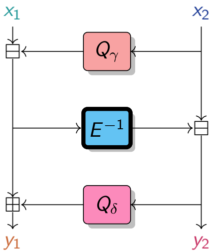
Closed FLYSTEL $\mathcal{V}$.

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

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

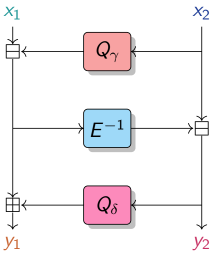
$$5^{-1} = \texttt{0x2e5f0fbadd72321ce14a56699d73f002}$$
$$\texttt{217f0e679998f19933333332cccccccd}$$

Advantage of CCZ-equivalence

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

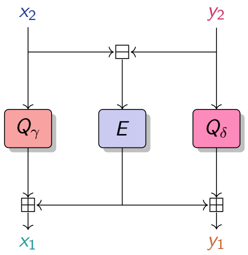
$$(y_1, y_2) == \mathcal{H}(x_1, x_2) \Leftrightarrow (x_1, y_1) == \mathcal{V}(x_2, y_2)$$

High-Degree permutation



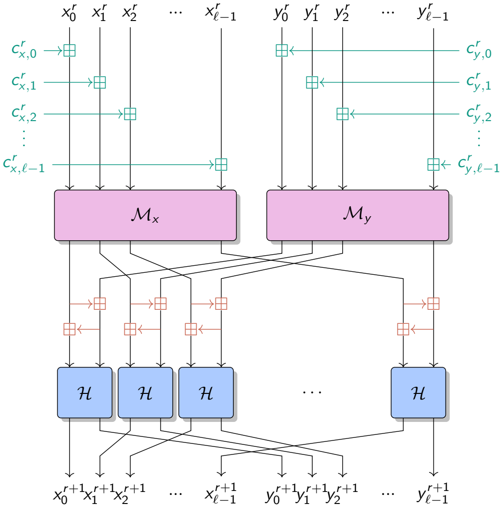
Open FLYSTEL $\mathcal{H}$.

Low-Degree function

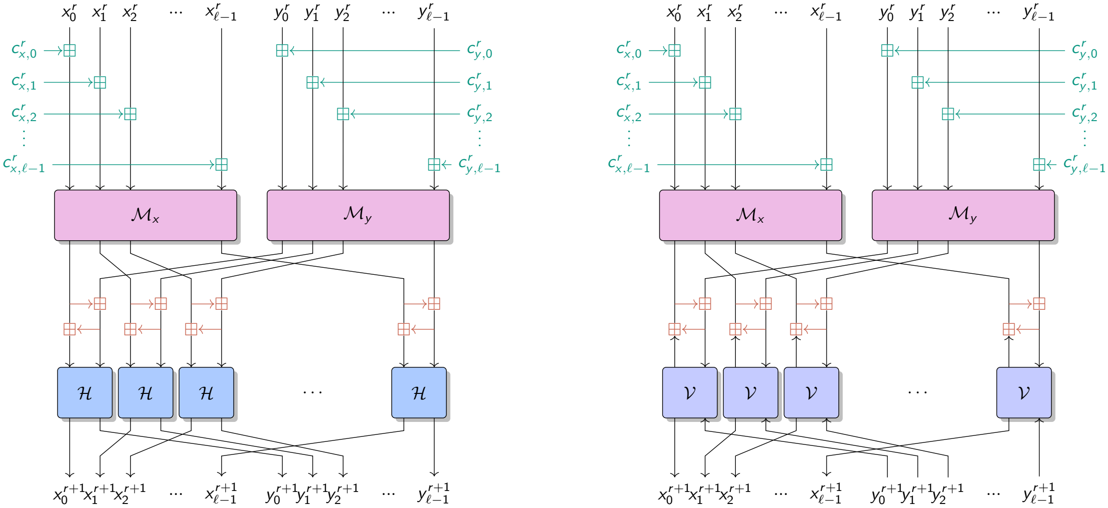


Closed FLYSTEL $\mathcal{V}$.

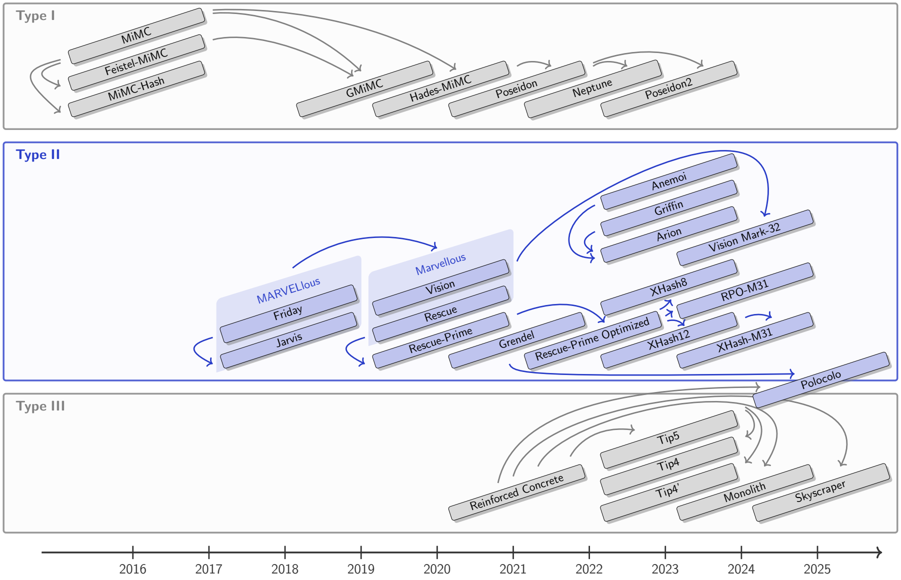
The SPN Structure



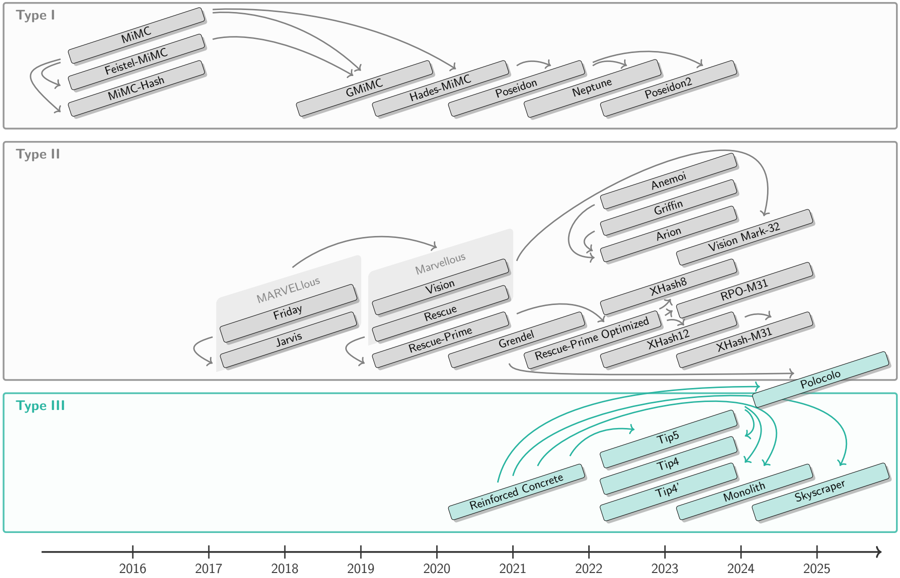
The SPN Structure



ZKP Primitives overview

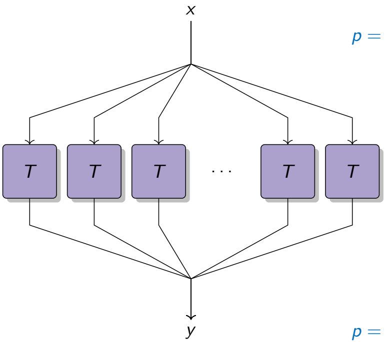


ZKP Primitives overview



Type III

Primitives using Look-up-Tables

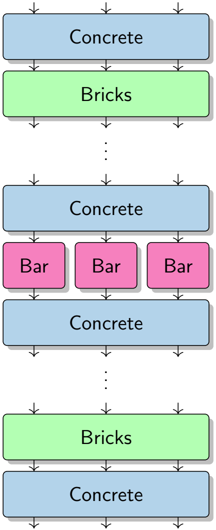


$\mathbb{F}_p$ with
$p =$ 0x73eda753299d7d483339d80809a1d80553bda402fffe5bfeffffffff00000001

$\mathbb{F}_2^8$
$(0,0,0,0,0,0,0,0)\ \ldots\ (1,1,1,1,1,1,1,1)$

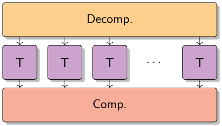
$\mathbb{F}_p$ with
$p =$ 0x73eda753299d7d483339d80809a1d80553bda402fffe5bfeffffffff00000001

Reinforced Concrete



L. Grassi, D. Khovratovich, R. Lüftenegger, C. Rechberger, M. Schofnegger and R. Walch, 2022

- S-box:

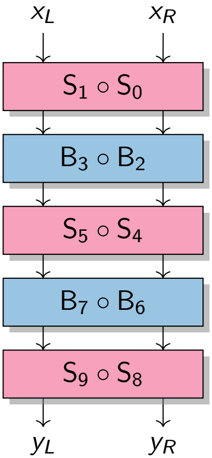


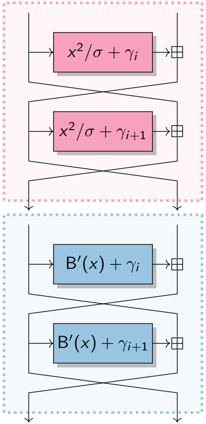
- Nb rounds:

$$R = 7$$

Skyscraper

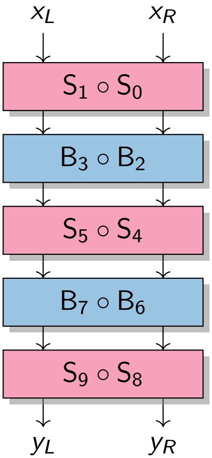
C. Bouvier, L. Grassi, D. Khovratovich, K. Koschatko, C. Rechberger, F. Schmid and M. Schofnegger, 2025

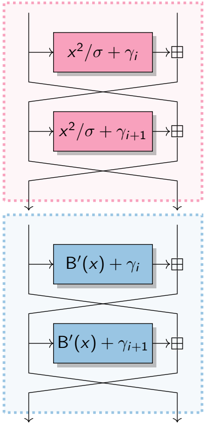


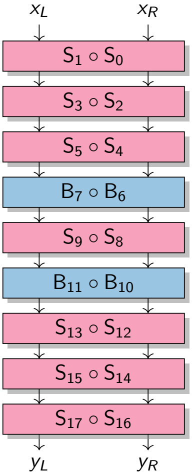


Skyscraper

C. Bouvier, L. Grassi, D. Khovratovich, K. Koschatko, C. Rechberger, F. Schmid and M. Schofnegger, 2025







Take-away

	Type I Low-degree primitives	**Type II** Equivalence relation	**Type III** Look-up tables
Alphabet	$\mathbb{F}_q^m$ for various q and m	$\mathbb{F}_q^m$ for various q and m	specific fields
Nb of rounds	many	few	fewer
Plain performance	fast	slow	faster
Nb of constraints	often more	fewer	it depends on the proof system
Examples	Feistel-MiMC Poseidon	Rescue Anemoi	Reinforced Concrete Skyscraper

CRYPTANALYSIS

Cryptanalysis overview

Some cryptanalysis techniques

- ⋆ Statistical attacks (differential and linear)
- ⋆ Algebraic attacks
- ⋆ Higher-Order differential attacks
- ⋆ ...

Cryptanalysis overview

Some cryptanalysis techniques

- ⋆ Statistical attacks (differential and linear)
- ⋆ Algebraic attacks
- ⋆ Higher-Order differential attacks
- ⋆ ...

Approaches so far:

- ⋆ **Type I**: HO attacks and algebraic attacks
- ⋆ **Type II**: algebraic attacks
- ⋆ **Type III**: combining statistical and algebraic attacks

Algebraic Attack

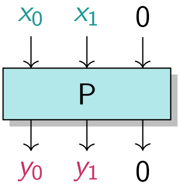
CICO: Constrained Input Constrained Output

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

Algebraic Attack

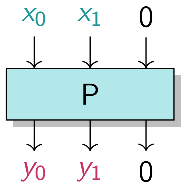
CICO: Constrained Input Constrained Output

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 $t = 3,\ u = 1.$

Need to solve a polynomial system

FreeLunch Attack

A. Bariant, A. Boeuf, A. Lemoine, I. Manterola Ayala, M. Øygarden, L. Perrin, and H. Raddum, 2024

Multivariate solving:

- Define the system
- Compute a grevlex order GB (**F5** algorithm)
- Convert it into lex order GB (**FGLM** algorithm)
- Find the roots in $\mathbb{F}_q^n$ of the GB polynomials using univariate system resolution.

FreeLunch Attack

A. Bariant, A. Boeuf, A. Lemoine, I. Manterola Ayala, M. Øygarden, L. Perrin, and H. Raddum, 2024

Multivariate solving:

- ⋆ Define the system
- ⋆ Compute a grevlex order GB (**F5** algorithm) $\rightsquigarrow$ **can be skipped**
- ⋆ Convert it into lex order GB (**FGLM** algorithm)
- ⋆ Find the roots in $\mathbb{F}_q^n$ of the GB polynomials using univariate system resolution.

Impact on the security of:

- ⋆ Griffin (practical attack for 7 out of 10 rounds)
- ⋆ Arion
- ⋆ Anemoi (need some tweak)

Resultant Attack

- **First approach** by HS. Yang, QX. Zheng, J. Yang, QF. Liu, D. Tang, 2024

  Impact on the security of:

  - Anemoi (practical attack for 8 out of 20 rounds)
  - Rescue (practical attack for 5 out of 18 rounds)
  - Jarvis (practical attack for 8 out of 10 rounds)

Resultant Attack

- **First approach** by HS. Yang, QX. Zheng, J. Yang, QF. Liu, D. Tang, 2024

  Impact on the security of:

  - Anemoi (practical attack for 8 out of 20 rounds)
  - Rescue (practical attack for 5 out of 18 rounds)
  - Jarvis (practical attack for 8 out of 10 rounds)

- **Improved** by A. Bariant, A. Boeuf, P. Briaud, M. Hostettler, M. Øygarden, H. Raddum, 2025

  Impact on the security of:

  - Griffin (practical attack for 8 out of 10 rounds)
  - Anemoi (practical attack for 11 out of 20 rounds)
  - Rescue (practical attack for 6 out of 18 rounds)
  - Arion

Linear attacks

Definition

Let $\mathsf{F} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ be a function and ω a primitive element.
The **Linearity** $\mathcal{L}_\mathsf{F}$ of $\mathsf{F} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ is the highest Walsh coefficient.

$$\mathcal{L}_\mathsf{F} = \max_{u,v \neq 0} \left| \sum_{x \in \mathbb{F}_q^n} \omega^{(\langle v, \mathsf{F}(x) \rangle - \langle u, x \rangle)} \right| .$$

Linear attacks

Definition

Let $\mathrm{F} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ be a function and ω a primitive element.
The **Linearity** $\mathcal{L}_\mathrm{F}$ of $\mathrm{F} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ is the highest Walsh coefficient.

$$\mathcal{L}_\mathrm{F} = \max_{u,v\neq 0} \left| \sum_{x\in\mathbb{F}_q^n} \omega^{(\langle v,\mathrm{F}(x)\rangle - \langle u,x\rangle)} \right| .$$

Examples:

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

$$\mathcal{L}_\mathrm{F} = \max_{u,v\neq 0} \left| \sum_{x\in\mathbb{F}_{2^n}^n} (-1)^{(\langle v,\mathrm{F}(x)\rangle - \langle u,x\rangle)} \right|$$

- If $\mathrm{F} : \mathbb{F}_p^n \to \mathbb{F}_p^m$, then

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

Weil bound

Proposition [Weil, 1948]

Let $f \in \mathbb{F}_p[x]$ be a univariate polynomial with $\deg(f) = d$. Then

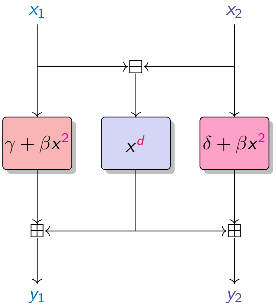
$$\mathcal{L}_f \leq (d-1)\sqrt{p}$$

Weil bound

Proposition [Weil, 1948]

Let $f \in \mathbb{F}_p[x]$ be a univariate polynomial with $\deg(f) = d$. Then

$$\mathcal{L}_f \leq (d-1)\sqrt{p}$$



Closed Flystel.

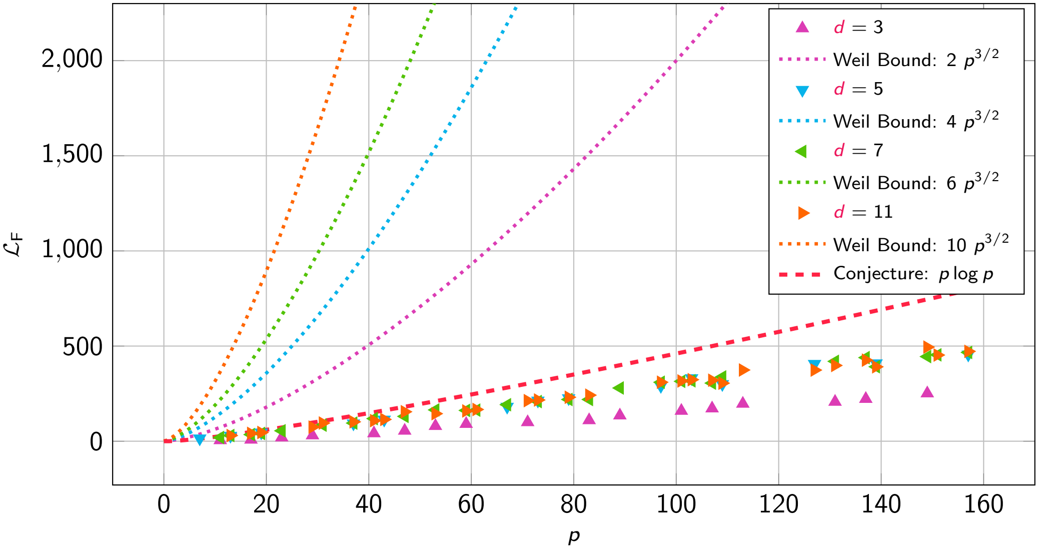
$$\mathcal{L}_F \leq (d-1)p\sqrt{p} \ ?$$

$$\begin{cases} \mathcal{L}_{\gamma+\beta x^2} & \leq \sqrt{p} \ , \\ \mathcal{L}_{x^d} & \leq (d-1)\sqrt{p} \ , \\ \mathcal{L}_{\delta+\beta x^2} & \leq \sqrt{p} \ . \end{cases}$$

Conjecture

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

Experimental results



Exponential sums

T. Beyne and C. Bouvier, 2024

- ⋆ Direct applications of results for exponential sums (generalization of Weil bound)

Exponential sums

T. Beyne and C. Bouvier, 2024

- ⋆ Direct applications of results for exponential sums (generalization of Weil bound)
- ⋆ 3 different results... for 3 important constructions
  - ⋆ Deligne, 1974 — Generalization of the Butterfly construction
  - ⋆ Denef and Loeser, 1991 — 3-round Feistel network
  - ⋆ Rojas-León, 2006 — Generalization of the Flystel construction

Functions with 2 variables

$$\mathsf{F} \in \mathbb{F}_q[x_1, x_2],\ \exists C \in \mathbb{F}_q,\ \mathcal{L}_{\mathsf{F}} \leq C \times q$$

Exponential sums

T. Beyne and C. Bouvier, 2024

- ⋆ Direct applications of results for exponential sums (generalization of Weil bound)
- ⋆ 3 different results... for 3 important constructions
  - ⋆ Deligne, 1974 — Generalization of the Butterfly construction
  - ⋆ Denef and Loeser, 1991 — 3-round Feistel network
  - ⋆ Rojas-León, 2006 — Generalization of the Flystel construction

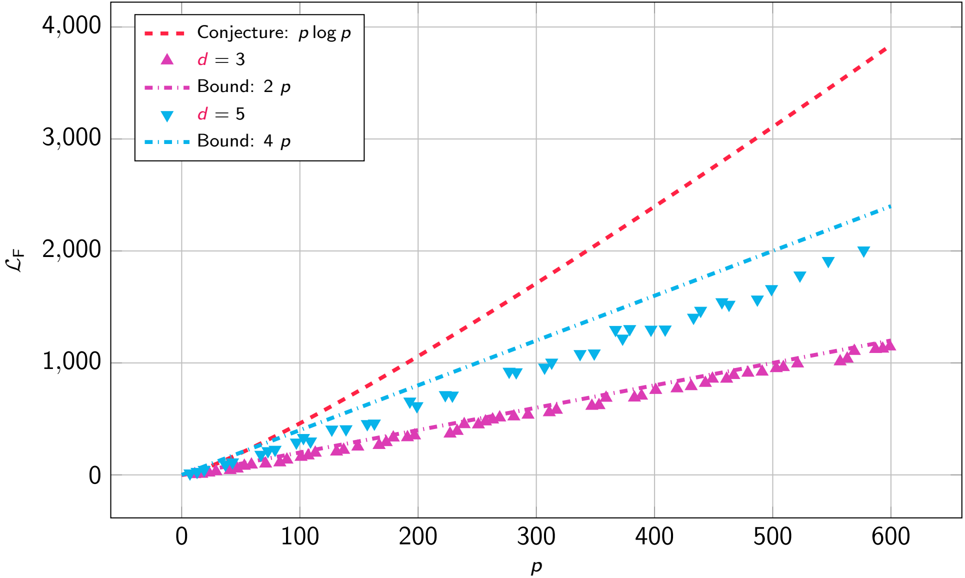
Functions with 2 variables

$$\mathrm{F} \in \mathbb{F}_q[x_1, x_2],\ \exists C \in \mathbb{F}_q,\ \mathcal{L}_\mathrm{F} \leq C \times q$$

- ⋆ Solving conjecture on the linearity of the Flystel construction (for $d \leq \log p$)

$$\mathcal{L}_\mathrm{F} \leq (d-1)p\ .$$

Solving conjecture



Website

`stap-zoo.com`

STAP Zoo   STAP primitive types   STAP use-cases   All STAP primitives

STAP

Symmetric Techniques for Advanced Protocols

The term *STAP* (Symmetric Techniques for Advanced Protocols) was first introduced in STAP'23, an affiliated workshop of **Eurocrypt'23**. It generally refers to algorithms in symmetric cryptography specifically designed to be efficient in new advanced cryptographic protocols. These contexts include zero-knowledge (ZK) proofs, secure multiparty computation (MPC) and (fully) homomorphic encryption (FHE) environments. It encompasses everything from arithmetization-oriented hash functions to homomorphic encryption-friendly stream ciphers.

Conclusions

⋆ Many new primitives have been proposed

Poseidon, Rescue, Anemoi, Skyscraper and many others...

Conclusions

- ⋆ Many new primitives have been proposed

  Poseidon, Rescue, Anemoi, Skyscraper and many others...

- ⋆ Some cryptanalysis progress have been done

  in particular for algebraic attacks,

  and very recently for statistical attacks using algebraic geometry.

Conclusions

- ⋆ Many new primitives have been proposed

  Poseidon, Rescue, Anemoi, Skyscraper and many others...

- ⋆ Some cryptanalysis progress have been done

  in particular for algebraic attacks,
  and very recently for statistical attacks using algebraic geometry.

Cryptanalysis and design of AOPs remain to be explored

Conclusions

- ⋆ Many new primitives have been proposed

  Poseidon, Rescue, Anemoi, Skyscraper and many others...

- ⋆ Some cryptanalysis progress have been done

  in particular for algebraic attacks,
  and very recently for statistical attacks using algebraic geometry.

Cryptanalysis and design of AOPs remain to be explored

Thank you