New Design Techniques for Efficient Arithmetization-Oriented Hash Functions: Anemoi Permutations and Jive Compression Mode

Clémence Bouvier [1,2]

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

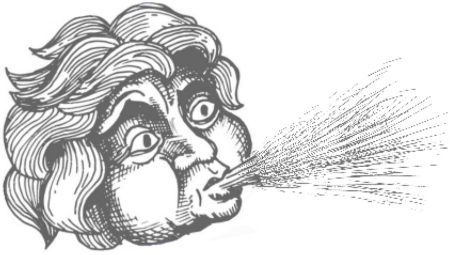
[1]Sorbonne Université, [2]Inria Paris,

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

CRYPTO, August 22nd, 2023

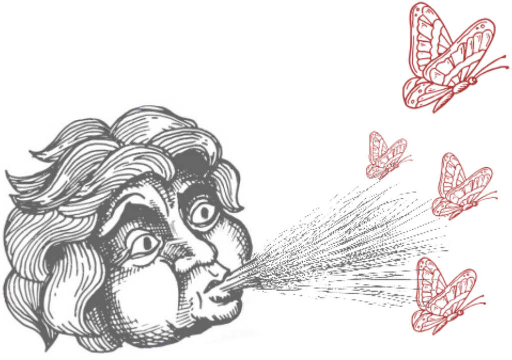
Why Anemoi?

⋆ Anemoi: Greek gods of winds



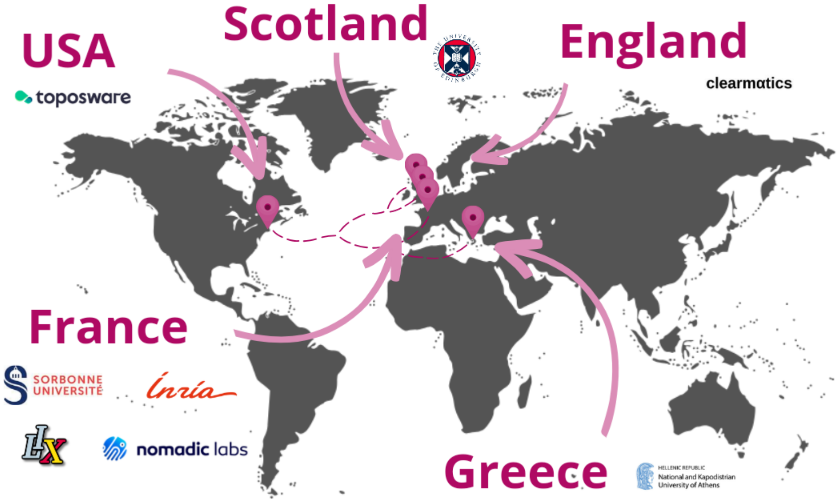
Why Anemoi?

- **Anemoi:** Greek gods of winds



Why Anemoi?

- Anemoi: Greek gods of winds



Why Anemoi?

- Anemoi: Family of ZK-friendly Hash functions

Content

New Design Techniques for Efficient Arithmetization-Oriented Hash Functions:
Anemoi Permutations and Jive Compression Mode

Comparison with "usual" case

A new environment

"Usual" case

- Field size:
  $\mathbb{F}_{2^n}$, with $n \simeq 4, 8$
- 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 $n \simeq 4, 8$
- 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

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

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

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

Comparison with "usual" case

A new environment

"Usual" case

- Field size:
  $\mathbb{F}_{2^n}$, with $n \simeq 4, 8$
- 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

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

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

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

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

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: Minimize the number of multiplications (R1CS)

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

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

Performance metric

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

“It depends”

Example: Minimize the number of multiplications (R1CS)

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

$t_0 = a \cdot x$
$t_1 = t_0 + b$
$t_2 = t_1 \times t_1$

$t_3 = t_2 \times t_1$
$t_4 = c \cdot x$
$t_5 = t_4 + d$

$t_6 = t_3 \times t_5$
$t_7 = e \cdot x$
$t_8 = t_6 + t_7$

3 constraints

Our approach

Need: verification using few multiplications.

Our approach

Need: verification using few multiplications.

⋆ **First approach:** evaluation also using few multiplications (Poseidon)

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

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

Our approach

Need: verification using few multiplications.

- **First approach:** evaluation also using few multiplications (POSEIDON)

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

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

- **Rescue approach:** using inversion

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

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

Our approach

Need: verification using few multiplications.

- **First approach:** evaluation also using few multiplications (Poseidon)

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

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

- **Rescue approach:** using inversion

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

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

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

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

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

Design of Anemoi

Construction of Anemoi permutations:

- ⋆ Substitution-Permutation Network (SPN)
- ⋆ relying on the CCZ-equivalence

Using a new non-linear layer: the Flystel

CCZ-equivalence

Example: the inverse

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

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

Example: the inverse

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

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, Zinoviev, DCC98]

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

$$\Gamma_F = \mathcal{L}(\Gamma_G) + c .$$

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

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

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

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

- 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 $(u, v) = \mathcal{L}(x, y)$

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

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 $(u, v) = \mathcal{L}(x, y)$

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

- ⋆ 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 $F : \mathbb{F}_q \rightarrow \mathbb{F}_q$ 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 $(u, v) = \mathcal{L}(x, y)$

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

- 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

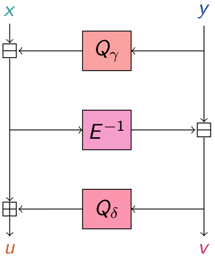
$$5^{-1} = \texttt{0x2e5f0fbadd72321ce14a56699d73f002217f0e679998f19933333332cccccccd}$$

The Flystel

Butterfly + Feistel ⇒ Flystel

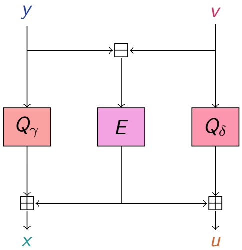
A 3-round Feistel-network with
$Q_\gamma : \mathbb{F}_q \to \mathbb{F}_q$ and $Q_\delta : \mathbb{F}_q \to \mathbb{F}_q$ two quadratic functions, and $E : \mathbb{F}_q \to \mathbb{F}_q$ a permutation

High-degree permutation



Open Flystel $\mathcal{H}$.

Low-degree function



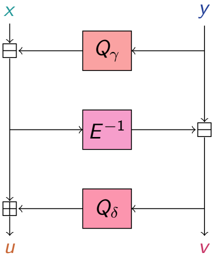
Closed Flystel $\mathcal{V}$.

The Flystel

Butterfly + Feistel ⇒ Flystel

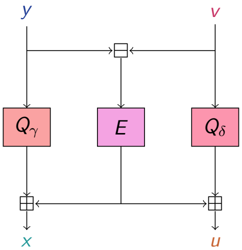
A 3-round Feistel-network with
$Q_\gamma : \mathbb{F}_q \to \mathbb{F}_q$ and $Q_\delta : \mathbb{F}_q \to \mathbb{F}_q$ two quadratic functions, and $E : \mathbb{F}_q \to \mathbb{F}_q$ a permutation

High-degree permutation



Open Flystel $\mathcal{H}$.

Low-degree function



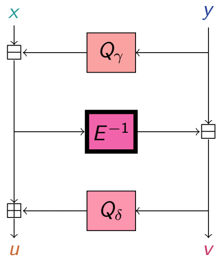
Closed Flystel $\mathcal{V}$.

$$\Gamma_{\mathcal{H}} = \mathcal{L}(\Gamma_{\mathcal{V}}) \quad \text{s.t.} \quad ((x, y), (u, v)) = \mathcal{L}\left(((v, y), (x, u)) \right)$$

Advantage of CCZ-equivalence

⋆ High Degree Evaluation.

High-degree
permutation



Open Flystel $\mathcal{H}$.

Ex: 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

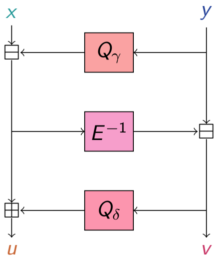
$$5^{-1} = \texttt{0x2e5f0fbadd72321ce14a56699d73f002}$$
$$\texttt{217f0e679998f19933333332cccccccd}$$

Advantage of CCZ-equivalence

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

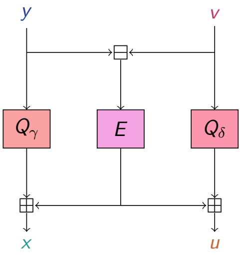
$$(u, v) == \mathcal{H}(x, y) \Leftrightarrow (x, u) == \mathcal{V}(y, v)$$

High-degree permutation



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

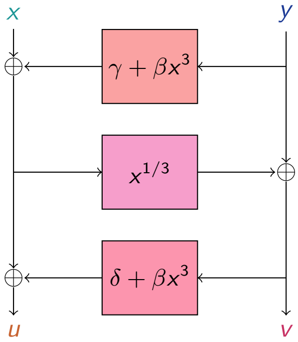
Low-degree function



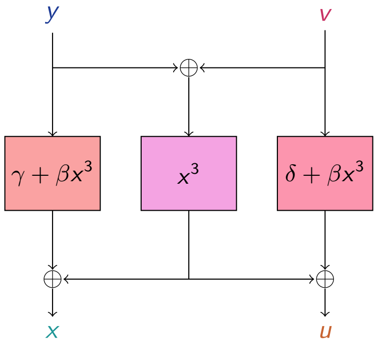
Closed `Flystel` $\mathcal{V}$.

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

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

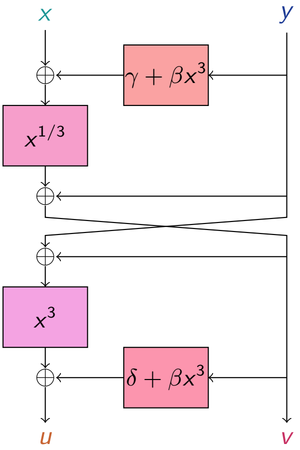


Open `Flystel`$_2$.



Closed `Flystel`$_2$.

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



Degenerated Butterfly.

Introduced by [Perrin et al. 2016].

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

- Differential properties

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

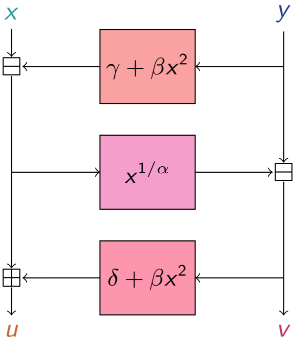
- Linear properties

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

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

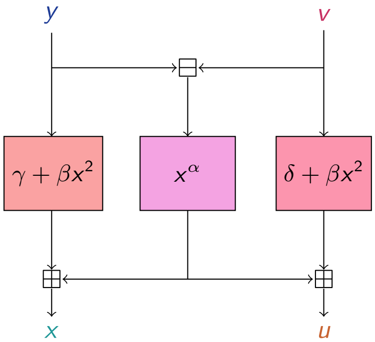
Flystel in $\mathbb{F}_p$

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



Open Flystel$_p$.

usually
$\alpha = 3$ or 5.

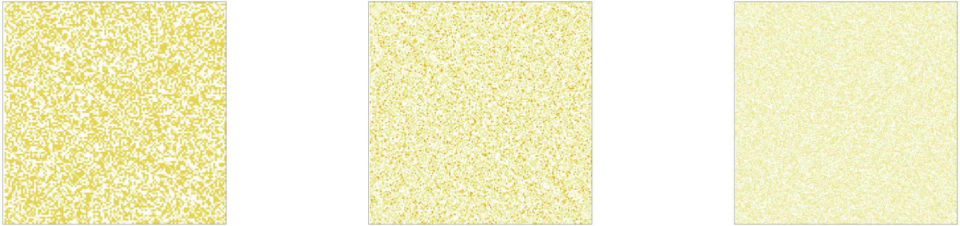


Closed Flystel$_p$.

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

- Differential properties
  $\texttt{Flystel}_p$ has a differential uniformity:

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



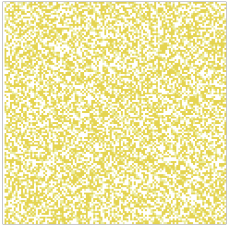
(a) *If $p = 11$ and $\alpha = 3$.* (b) *If $p = 13$ and $\alpha = 5$.* (c) *If $p = 17$ and $\alpha = 3$.*

DDT of $\texttt{Flystel}_p$.

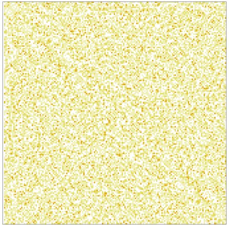
Properties of Flystel in $\mathbb{F}_p$

- Differential properties
  $\texttt{Flystel}_p$ has a differential uniformity:

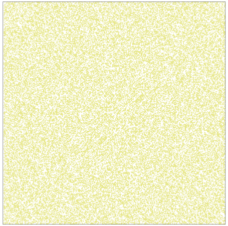
$$\delta_{\mathcal{H}} = \max_{a \neq 0, b} |\{x \in \mathbb{F}_p^2, \mathcal{H}(x+a) - \mathcal{H}(x) = b\}| \leq \alpha - 1$$



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



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



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

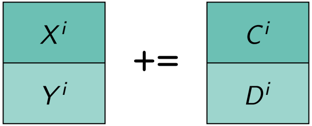
DDT of $\texttt{Flystel}_p$.

Solving the open problem of finding an APN permutation over $\mathbb{F}_p^2$

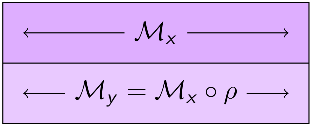
The SPN Structure

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

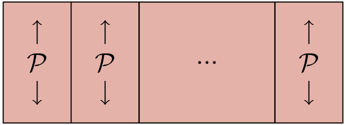
(a) *Internal state.*



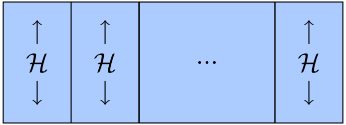
(b) *The constant addition.*



(c) *The diffusion layer.*

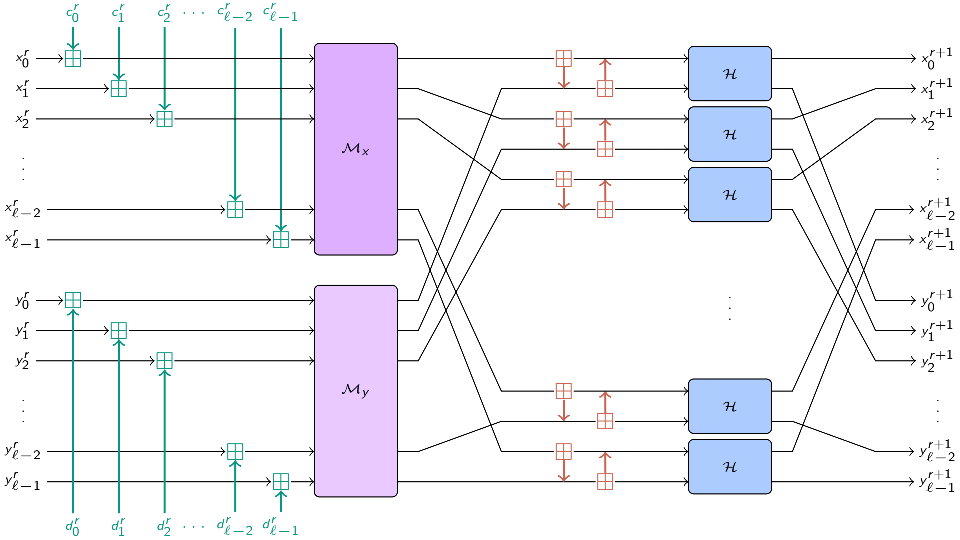


(d) *The PHT.*



(e) *The S-box layer.*

The SPN Structure



Number of rounds

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

- Choosing the number of rounds

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

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

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

Purposes of Anemoi

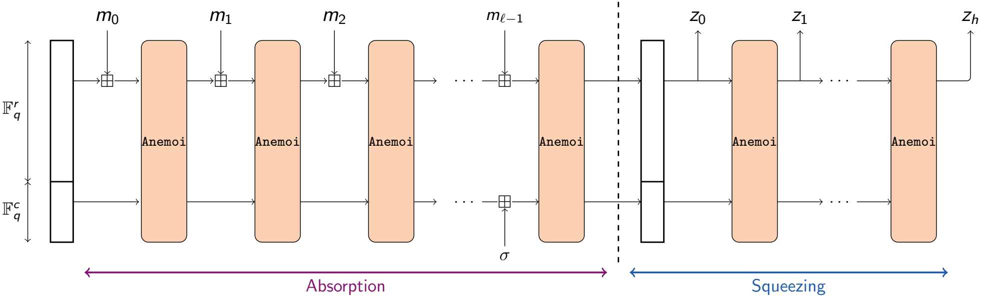
The 2 purposes of Anemoi:

- ⋆ a hash function to emulate a random oracle
- ⋆ a compression function within a Merkle-tree

Using different functions for the different purposes

Sponge construction

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

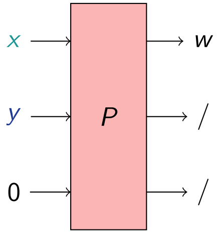


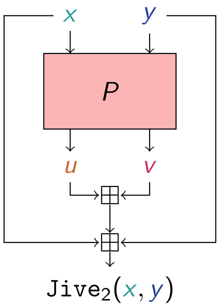
New Mode: Jive

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

Dedicated mode: 2 words in 1

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



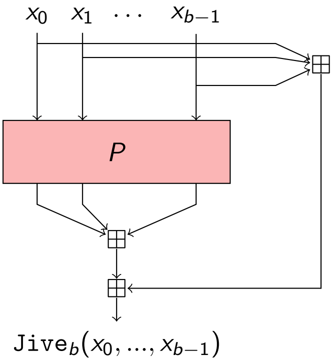


New Mode: Jive

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

Dedicated mode: b words in 1

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



Some Benchmarks

	m	*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* $\alpha = 3$

	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	-	**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* $\alpha = 5$

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

[1] *Rescue* [Aly, Ashur, Ben-Sasson, Dhooghe and Szepieniec, ToSC20]
[2] Poseidon [Grassi, Khovratovich, Rechberger, Roy and Schofnegger, USENIX21]
[3] Griffin [Grassi, Hao, Rechberger, Schofnegger, Walch and Wang, CRYPTO23] (next session)

Conclusions

Anemoi: A new family of ZK-friendly hash functions

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

Conclusions

Anemoi: A new family of ZK-friendly hash functions

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

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

Anemoi: A new family of ZK-friendly hash functions

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

Related works

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

☞ More details on eprint.iacr.org/2022/840 or on anemoi-hash.github.io

Conclusions

Anemoi: A new family of ZK-friendly hash functions

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

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]

☞ More details on eprint.iacr.org/2022/840 or on anemoi-hash.github.io

Thanks for your attention!

More benchmarks and

Cryptanalysis

Comparison for Plonk (with optimizations)

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

(a) *With 3 wires.*

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

(b) *With 4 wires.*

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

Comparison for Plonk (with optimizations)

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

(a) *With 3 wires.*

	m	Constraints
Poseidon	3 2	98 82
Reinforced Concrete	3 2	267 174
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

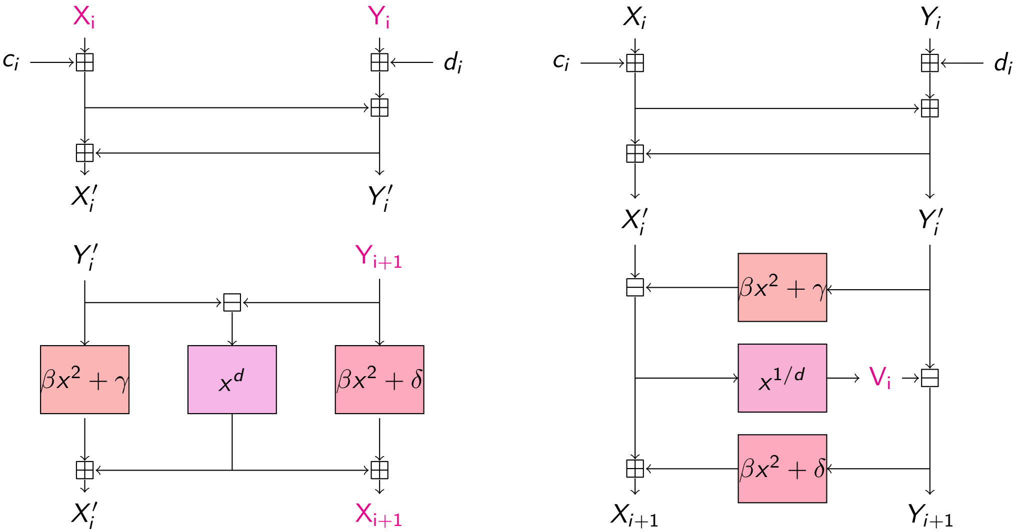
Rescue-12	*Rescue*-8	Poseidon-12	Poseidon-8	Griffin-12	Griffin-8	Anemoi-8
15.67 μs	9.13 μs	5.87 μs	2.69 μs	2.87 μs	**2.59 μs**	4.21 μs

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 BLS12 − 381, Rescue, Poseidon, Anemoi with state size of 2, Griffin of 3 ($s = 128$).

Algebraic attacks: 2 modelings

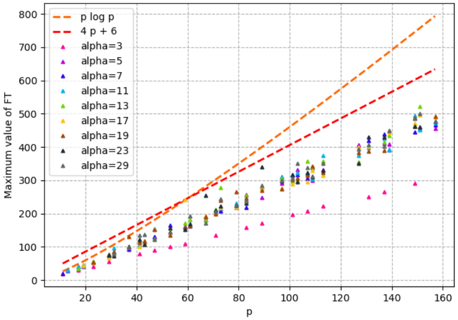


(a) *Model 1.* (b) *Model 2.*

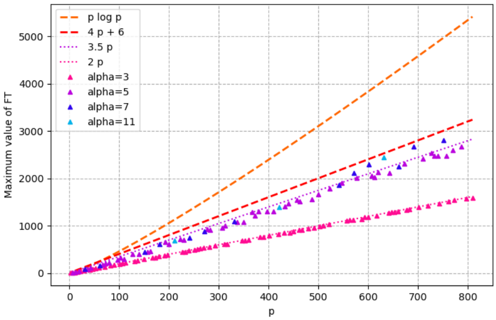
Properties of Flystel in $\mathbb{F}_p$

- Linear properties

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



(a) *For different α.*



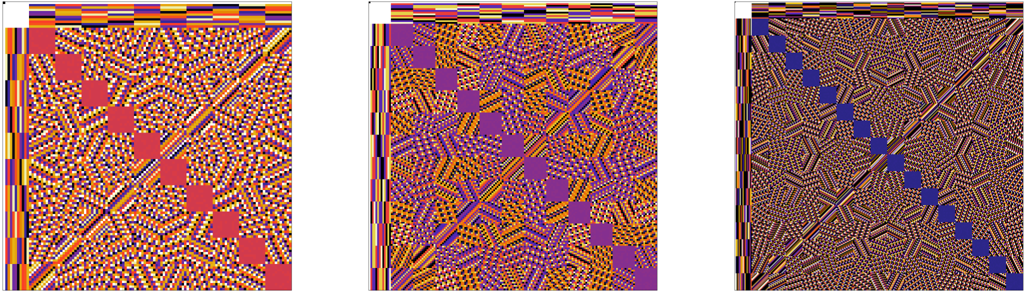
(b) *For the smallest α.*

Conjecture for the linearity.

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

- Linear properties

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



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

LAT of $\texttt{Flystel}_p$.