Auld Alliance is back

Clémence Bouvier
joint work with Léo Perrin and Vesselin Velichkov

Sorbonne Université, Inria Paris, team COSMIQ, Clearmatics, London

Rump session, FSE, 2022

“The Auld Alliance”

THE AULD ALLIANCE IS BACK!

Designing Butterfly-based Hash Functions

Emerging uses in symmetric cryptography

Zero-knowledge proofs $\Rightarrow$ New primitives

designed to minimize the number of multiplications in finite fields.

"Usual" case

- operations on $\mathbb{F}_{2^\eta}$, $\eta \simeq 4, 8$.
- CPU instructions and hardware components

Arithmetization-friendly

- operations on $\mathbb{F}_\rho$, $\rho \in \{2^\eta, \pi\}$, π prime, $\pi \simeq 2^\eta, \eta \geq 64$.
- large finite-field arithmetic

Emerging uses in symmetric cryptography

Zero-knowledge proofs $\Rightarrow$ New primitives

designed to minimize the number of multiplications in finite fields.

"Usual" case

- operations on $\mathbb{F}_{2^\eta}$, $\eta \simeq 4, 8$.
- CPU instructions and hardware components

Arithmetization-friendly

- operations on $\mathbb{F}_\rho$, $\rho \in \{2^\eta, \pi\}$, π prime, $\pi \simeq 2^\eta, \eta \geq 64$.
- large finite-field arithmetic

Design goals:

- Compatibility with Various Proof Systems.
- Limited Reliance on Randomness.
- Different Algorithms for Different Purposes.
- Design Consistency.

CCZ-equivalence

Definition

$\phi : \mathbb{F}_\rho \to \mathbb{F}_\rho$ and $\psi : \mathbb{F}_\rho \to \mathbb{F}_\rho$ are **CCZ-equivalent**

$$\Gamma_\phi = \left\{ (\chi, \phi(\chi)) \mid \chi \in \mathbb{F}_\rho \right\} = \theta(\Gamma_\psi) = \left\{ \theta(\chi, \phi(\chi)) \mid \chi \in \mathbb{F}_\rho \right\},$$

where θ is an affine permutation.

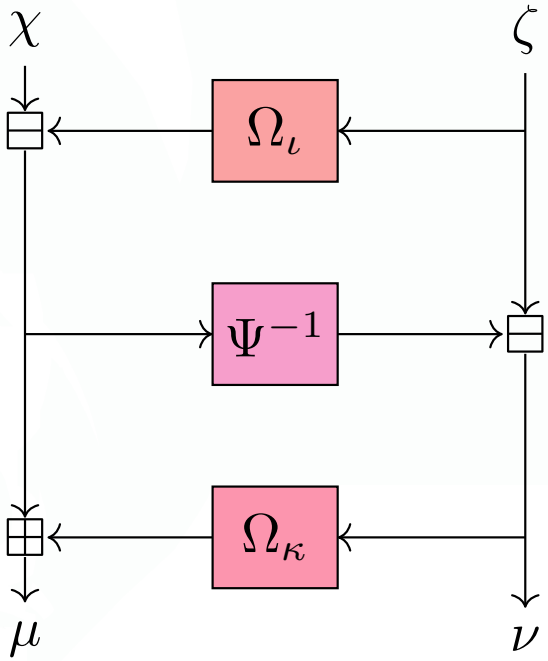
CCZ-equivalence

Definition

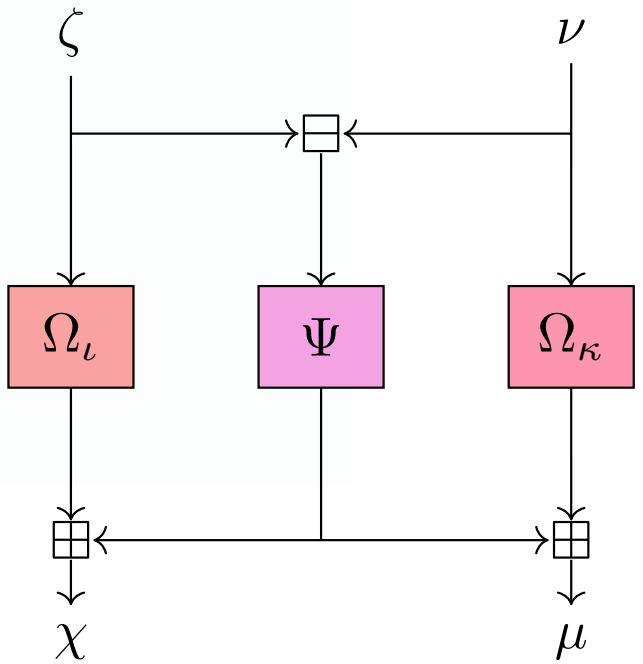
$\phi : \mathbb{F}_\rho \to \mathbb{F}_\rho$ and $\psi : \mathbb{F}_\rho \to \mathbb{F}_\rho$ are **CCZ-equivalent**

$$\Gamma_\phi = \left\{ (\chi, \phi(\chi)) \mid \chi \in \mathbb{F}_\rho \right\} = \theta(\Gamma_\psi) = \left\{ \theta(\chi, \phi(\chi)) \mid \chi \in \mathbb{F}_\rho \right\},$$

where θ is an affine permutation.



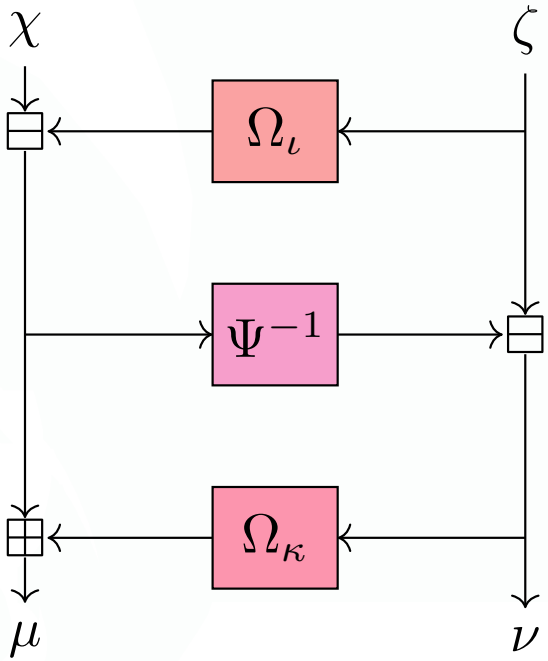
Open `Flystel`.



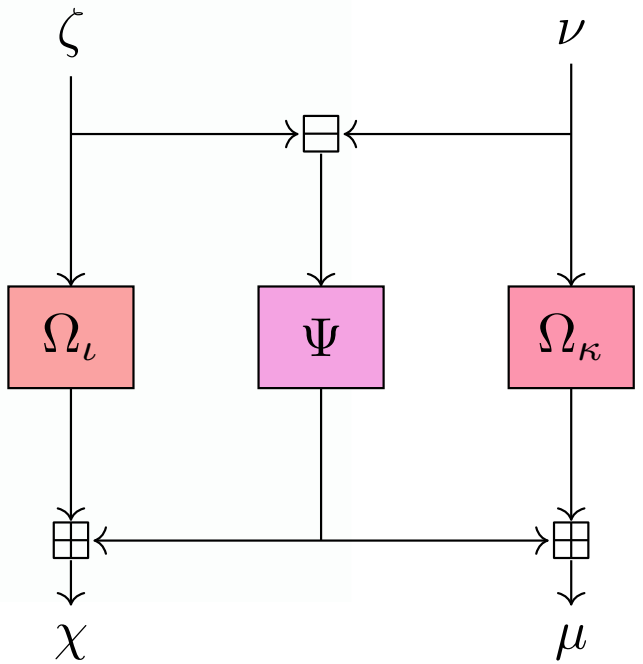
Closed `Flystel`.

CCZ-equivalence

- High Degree.
- Low Differential Uniformity.
- Low Cost Verification.
- Less Costly Evaluation.

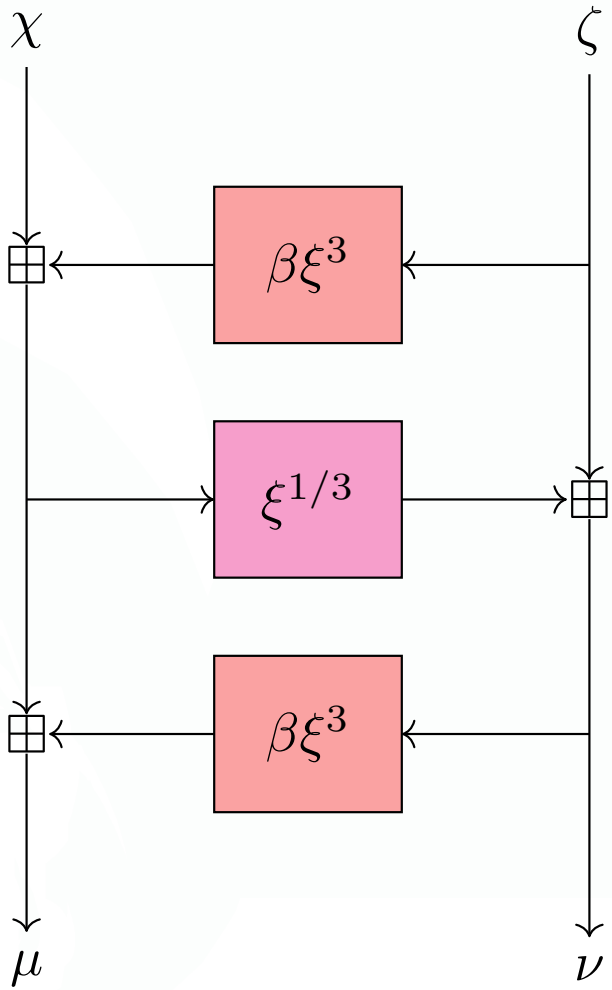


Open `Flystel`.

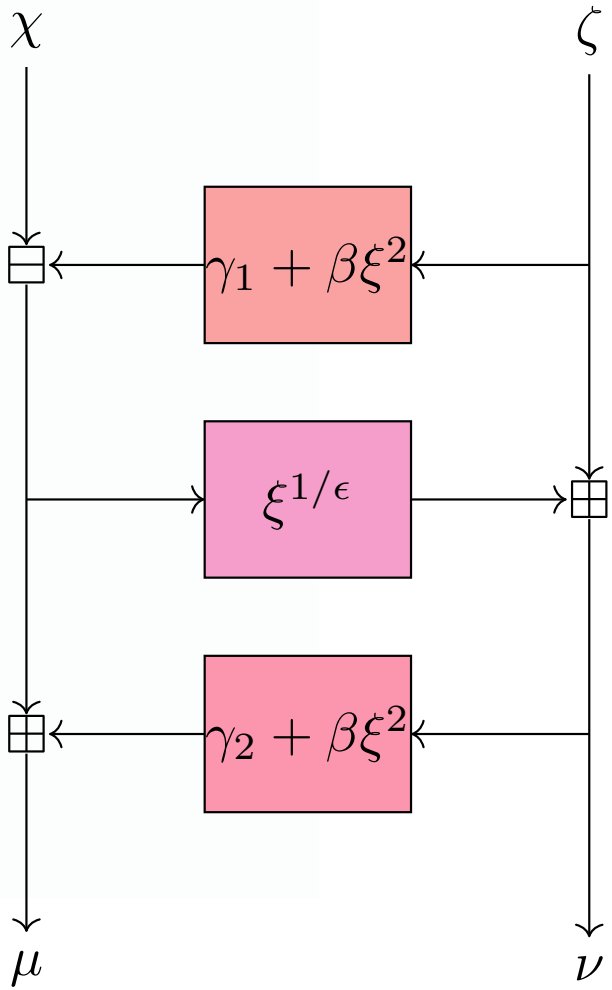


Closed `Flystel`.

Open Flystel



Flystel in $\mathbb{F}_{2^\eta}$.



Flystel in $\mathbb{F}_\pi$.

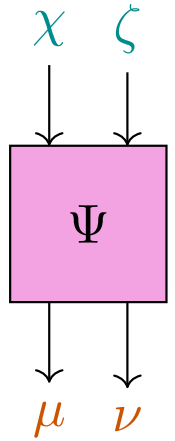
New Mode

- Random oracle replacement: `AuldRO`
- Collision resistant compression function for Merkle-trees: `AuldMC`

Dedicated mode

$$\Pi_\iota : (\chi, \zeta) \mapsto \Lambda \circ \phi(\chi + \kappa_\iota, \zeta + \omega_\iota) \ ,$$

$$(\mu, \nu) = (\Pi_{\eta-1} \circ \ldots \circ \Pi_0)(\chi, \zeta) \ ,$$



$\Rightarrow$ 2 words in 1

$$(\chi, \zeta) \mapsto \chi + \zeta + \mu + \nu \ .$$

The Conquest of Athens

Athena and Poseidon