Politecnico di Torino

Corrigendum to "Invertible Quadratic Non-Linear Layers for MPC-/FHE-/ZK-Friendly Schemes over $\mathbb{F}_p^n$ – Application to Poseidon"

SPRING 2026

10 May 2026

Lorenzo Grassi, Matilda Urani

l.grassi@tue.nl
matilda.urani@polito.it

The Context

Increasing interest in **Zero-Knowledge (ZK)** proof systems

Need for **efficient** hash functions tailored to ZK

(Some of the) Key Design Goals:

- **Low multiplicative cost:** minimize number of non-linear operations.
- **Field compatibility:** primitives defined over $\mathbb{F}_p$ with large prime p.

The Context

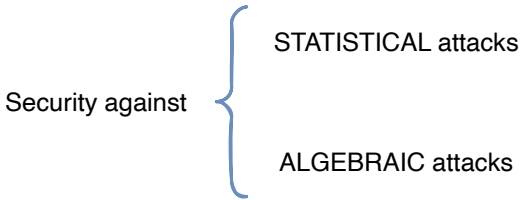
Increasing interest in **Zero-Knowledge (ZK)** proof systems

Need for **efficient** hash functions tailored to ZK

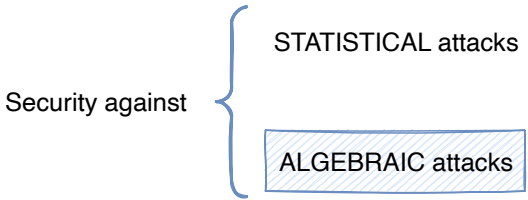
(Some of the) Key Design Goals:

- **Low multiplicative cost:** minimize number of non-linear operations.
- **Field compatibility:** primitives defined over $\mathbb{F}_p$ with large prime p.
- **Security** against malicious attackers.

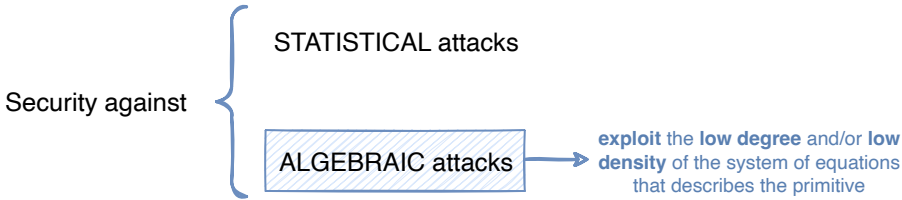
Security of ZK-Friendly Primitives



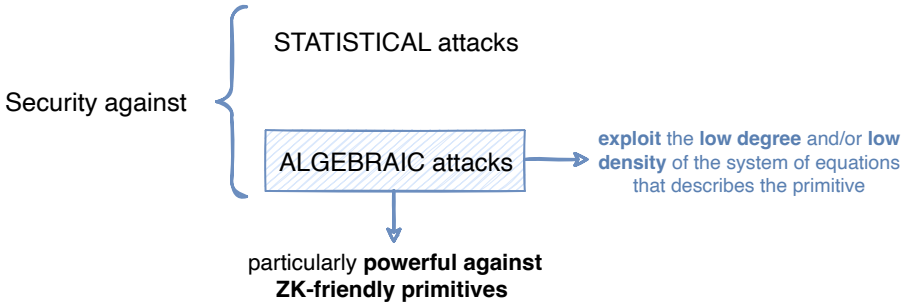
Security of ZK-Friendly Primitives



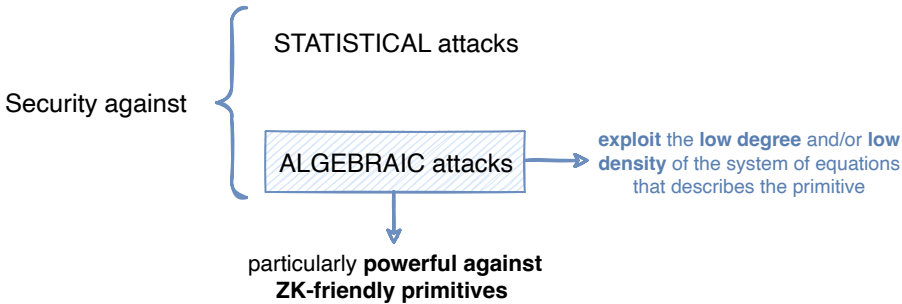
Security of ZK-Friendly Primitives



Security of ZK-Friendly Primitives



Security of ZK-Friendly Primitives



Common countermeasure: ensure that the polynomial expressing the function is of high enough (potentially maximum) degree and density.

Neptune: A ZK-friendly Hash Function

Fix a prime $p > 2^{63}$ and an even integer $t = 2t' \in \{2, 4, \ldots, 24\}$.

The NEPTUNE permutation $\mathcal{N} : \mathbb{F}_p^t \to \mathbb{F}_p^t$ is defined as

$$\mathcal{N}(\cdot) = \underbrace{\mathcal{E}^{(5)} \circ \mathcal{E}^{(4)}}_{\text{2 rounds}} \circ \underbrace{\mathcal{I}^{(\mathcal{R}_\mathcal{I}-1)} \circ \cdots \circ \mathcal{I}^{(0)}}_{\mathcal{R}_\mathcal{I} \text{ rounds}} \circ \underbrace{\mathcal{E}^{(3)} \circ \cdots \circ \mathcal{E}^{(0)}}_{\text{4 rounds}} (\mathcal{M} \times \cdot)$$

Neptune: A ZK-friendly Hash Function

Fix a prime $p > 2^{63}$ and an even integer $t = 2t' \in \{2, 4, \ldots, 24\}$.

The NEPTUNE permutation $\mathcal{N} : \mathbb{F}_p^t \to \mathbb{F}_p^t$ is defined as

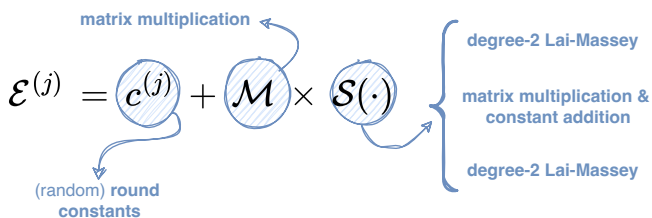
$$\mathcal{N}(\cdot) = \mathcal{E}^{(5)} \circ \mathcal{E}^{(4)} \circ \mathcal{I}^{(\mathcal{R}_\mathcal{I}-1)} \circ \cdots \circ \mathcal{I}^{(0)} \circ \mathcal{E}^{(3)} \circ \cdots \circ \mathcal{E}^{(0)}(\mathcal{M} \times \cdot)$$

Neptune: A ZK-friendly Hash Function

Fix a prime $p > 2^{63}$ and an even integer $t = 2t' \in \{2, 4, \ldots, 24\}$.

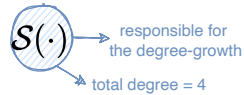
The NEPTUNE permutation $\mathcal{N} : \mathbb{F}_p^t \to \mathbb{F}_p^t$ is defined as

$$\mathcal{N}(\cdot) = \mathcal{E}^{(5)} \circ \mathcal{E}^{(4)} \circ \mathcal{I}^{(\mathcal{R}_\mathcal{I}-1)} \circ \cdots \circ \mathcal{I}^{(0)} \circ \mathcal{E}^{(3)} \circ \cdots \circ \mathcal{E}^{(0)}(\mathcal{M} \times \cdot)$$



Neptune Degree Growth

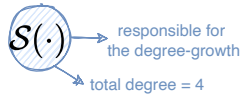
$$\mathcal{E}^{(j)} = c^{(j)} + \mathcal{M} \times \mathcal{S}(\cdot)$$



We expect that after r external rounds the degree of the composite function will be 4^r.

Neptune Degree Growth

$$\mathcal{E}^{(j)} = c^{(j)} + \mathcal{M} \times \mathcal{S}(\cdot)$$

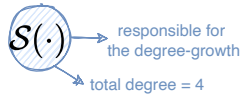


We expect that after r external rounds the degree of the composite function will be 4^r.

Is it really the case?

Neptune Degree Growth

$$\mathcal{E}^{(j)} = c^{(j)} + \mathcal{M} \times \mathcal{S}(\cdot)$$

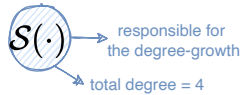


We expect that after r external rounds the degree of the composite function will be 4^r.

Is it really the case? Unfortunately, not always.

Neptune Degree Growth

$$\mathcal{E}^{(j)} = c^{(j)} + \mathcal{M} \times \mathcal{S}(\cdot)$$

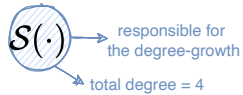


We expect that after r external rounds the degree of the composite function will be 4^r.

Is it really the case? Unfortunately, not always. *Why?*

Neptune Degree Growth

$$\mathcal{E}^{(j)} = c^{(j)} + \mathcal{M} \times \mathcal{S}(\cdot)$$



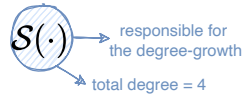
We expect that after r external rounds the degree of the composite function will be 4^r.

Is it really the case? Unfortunately, not always.

Why? Because of the linear layer $\mathcal{M}$.

Neptune Degree Growth

$$\mathcal{E}^{(j)} = c^{(j)} + \mathcal{M} \times \mathcal{S}(\cdot)$$



We expect that after r external rounds the degree of the composite function will be 4^r.

Is it really the case? Unfortunately, not always. *Why?* Because of the linear layer $\mathcal{M}$.

Fix $M', M'' \in \mathbb{F}_p^{t' \times t'}$ (MDS). We define the matrix of the linear layer $\mathcal{M} \in \mathbb{F}_p^{t \times t}$ as

$$\mathcal{M}_{i,j} = \begin{cases} M'_{i',j'} & \text{if } (i,j) = (2i',\, 2j') \\ M''_{i'',j''} & \text{if } (i,j) = (2i''+1,\, 2j''+1) \\ 0 & \text{otherwise} \end{cases}$$

Conditions on the Linear Layer

Conditions

$$M' \neq \mu \cdot M'' \quad \forall \mu \in \mathbb{F}_p$$

$$M'_{i,j} \neq M''_{i,j} \quad \forall i, j$$

Not sufficient!
Do not guarantee maximal degree growth

Conditions on the Linear Layer

Conditions

$$M' \neq \mu \cdot M'' \quad \forall \mu \in \mathbb{F}_p$$
$$M'_{i,j} \neq M''_{i,j} \quad \forall i, j$$

Not sufficient!
Do not guarantee maximal degree growth

Example.

Given $M', M'' \in \mathbb{F}_p^{2\times 2}$, for $p = 2^{64} - 2^{32} + 1$

$$M' = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} \quad M'' = \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}.$$

At round 3: $\deg = 56 \; < \; 4^3 = 64.$

Our Contribution

If the algebraic degree is lower than expected, the security analysis may not hold, increasing the **risk of successful attacks**.

Our Work

We provide **new** (sufficient) **conditions** on the **linear layer** that ensure the **maximum degree growth.**

Key idea.
Track (some specific) monomials of degree 4^r across rounds and ensure that their coefficients do not vanish.

Main Result

Notation. For $r \geq 2$

$$\begin{cases} \mu^{(1)}_{2i,j} = M'_{i,j} \\ \mu^{(r)}_{2i,j} = \sum_{k=0}^{t'-1} \mu^{(1)}_{2i,k} \left(\mu^{(r-1)}_{2k,j} - \mu^{(r-1)}_{2k+1,j}\right)^4 \end{cases} \qquad \begin{cases} \mu^{(1)}_{2i+1,j} = M''_{i,j} \\ \mu^{(r)}_{2i+1,j} = \sum_{k=0}^{t'-1} \mu^{(1)}_{2i+1,k} \left(\mu^{(r-1)}_{2k,j} - \mu^{(r-1)}_{2k+1,j}\right)^4 \end{cases}$$

Theorem (Grassi, Urani)

The degree at round r attains its maximum value (4^r) if the following conditions hold

$$\begin{aligned} \mu^{(r)}_{2i,j},\ \mu^{(r)}_{2i+1,j} &\neq 0 \\ \mu^{(r-1)}_{2i,j} - \mu^{(r-1)}_{2i+1,j} &\neq 0 \end{aligned} \qquad \text{for each } i, j = 0, \ldots, t' - 1.$$

Proof Idea

Let $x = (x_0, \ldots, x_t) \in \mathbb{F}_p^t$ be the input of the first round.

At round r, each output pair $(2i, 2i+1)$ contains monomials $(x_{2j} - x_{2j+1})^{\mathbf{4^r}}$, with coefficients evolving as

$$\mu_{2i,j}^{(r-1)},\ \mu_{2i+1,j}^{(r-1)} \xrightarrow{\mathcal{S}} (\mu_{2i,j}^{(r-1)} - \mu_{2i+1,j}^{(r-1)})^4 \xrightarrow{\mathcal{M}} \mu_{2i,j}^{(r)},\ \mu_{2i+1,j}^{(r)}.$$

Theorem (Grassi, Urani)

The degree at round r attains its maximum value (4^r) if the following conditions hold

$$\begin{aligned} \mu_{2i,j}^{(r)},\ \mu_{2i+1,j}^{(r)} &\neq 0 \\ \mu_{2i,j}^{(r-1)} - \mu_{2i+1,j}^{(r-1)} &\neq 0 \end{aligned} \qquad \text{for each } i, j = 0, \ldots, t' - 1.$$

Thank you!

Details of the Proof

Round r: propagation of coefficients

$$\boxed{x^{(r)}} \implies \boxed{y^{(r)} = S(x^{(r)})} \implies \boxed{z^{(r)} = \mathcal{M} \times y^{(r)}}$$

We **tracked the evolution** of $(x_{2i}^{(1)} - x_{2i+1}^{(1)})^{4^r}$ over the rounds.

$$y_{2i}^{(r)} = y_{2i+1}^{(r)} \cong \sum_{j=0}^{t'-1} \boldsymbol{(\mu_{2i,j}^{(r-1)} - \mu_{2i+1,j}^{(r-1)})^4} \cdot (x_{2j}^{(1)} - x_{2j+1}^{(1)})^{4^r}.$$

$$z_{2i}^{(r)} \cong \sum_{j=0}^{t'-1} \boldsymbol{\mu_{2i,j}^{(r)}} \cdot (x_{2j}^{(1)} - x_{2j+1}^{(1)})^{4^r},$$

$$z_{2i+1}^{(r)} \cong \sum_{j=0}^{t'-1} \boldsymbol{\mu_{2i+1,j}^{(r)}} \cdot (x_{2j}^{(1)} - x_{2j+1}^{(1)})^{4^r}.$$