Greek and Roman Gods in Symmetric-Key Crypto

Lorenzo Grassi

Eindhoven University of Technology, NL

February 2026

Table of Contents

Table of Contents

Recent Applications

Symmetric cryptography primitives may be needed in:

- secure multi-party computation (MPC),
- homomorphic encryption (HE),
- zero-knowledge proofs (ZK),

where

1. *details of the used symmetric algorithm may influence the protocols efficiency*;
2. many of such protocols are *naturally defined over* $(\mathbb{F}_p)^n$ *for a large prime integer* p (e.g., $p \approx 2^{32}$, 2^{64}, or 2^{256}).

Cost Metric of MPC-/HE-/ZK-Friendly Schemes

Demand of new *specific* symmetric primitives over *prime fields* for these new applications!

Rough Cost Metric:

- Linear/Affine functions: *almost free*;
- Non-linear functions: *expensive*.

(*Important:* the size p of the field does not impact the cost in these MPC/HE/ZK applications!)

Cost Metrics for ZK (1/2)

Focusing on Zero-Knoweldge (R1CS and AIR):

- *number of multiplications required during the verification process* as a good estimation of the complexity of a ZK-friendly scheme;
- roughly speaking, the *depth* and (slightly) the number of affine operations during the verification process impact the cost for AIR as well.

In Plonkup (Plonk + Plookup) and Binius:

- *look-up tables* are relatively cheap $\rightarrow$ different cost metric.

Cost Metrics for ZK (1/2)

Focusing on Zero-Knoweldge (R1CS and AIR):

- *number of multiplications required during the verification process* as a good estimation of the complexity of a ZK-friendly scheme;
- roughly speaking, the *depth* and (slightly) the number of affine operations during the verification process impact the cost for AIR as well.

In Plonkup (Plonk + Plookup) and Binius:

- *look-up tables* are relatively cheap $\rightarrow$ different cost metric.

Cost Metrics for ZK – Examples (2/2)

Given x and $y = x^{p-2} \equiv 1/x$ over $\mathbb{F}_p$, verified via

$$\forall x, y \neq 0 : \qquad x \cdot y = 1 \,.$$

Given x and $y = x^{1/d}$ over $\mathbb{F}_p$ s.t. $\gcd(d, p-1) = 1$, then verified via

$$y^d - x = 0 \,.$$

(*Note:* if d is small, then $1/d$ is huge! E.g., $d = 3$ and $1/d = (2p-1)/3$.)

Cost Metrics for ZK – Examples (2/2)

Given x and $y = x^{p-2} \equiv 1/x$ over $\mathbb{F}_p$, verified via

$$\forall x, y \neq 0 : \qquad x \cdot y = 1 \,.$$

Given x and $y = x^{1/d}$ over $\mathbb{F}_p$ s.t. $\gcd(d, p-1) = 1$, then verified via

$$y^d - x = 0 \,.$$

(*Note:* if d is small, then $1/d$ is huge! E.g., $d = 3$ and $1/d = (2p-1)/3$.)

The ZK-friendly Symmetric Crypto Zoo

Type 1

- Low-degree

$$y = x^d$$

- Fast in Plain
- Many rounds
- Often more constraints
- GMiMC, POSEIDON, NEPTUNE, POSEIDON2, ...

Type 2

- Low-degree equivalence

$$y = x^{1/d} \rightarrow x = y^d$$

- Slow in Plain
- Fewer rounds
- Fewer constraints
- Vision, Rescue, Grendel, GRIFFIN, Anemoi, Arion, ...

Type 3

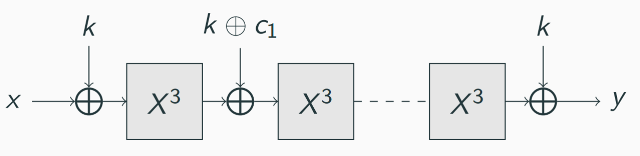
- Lookup tables

$$y = \mathcal{T}[x]$$

- Fast in Plain
- Fewer rounds
- Constraints depend on proof system
- Reinforced Concrete, Tip5, Skyscraper, ...

Table of Contents

MiMC Cipher

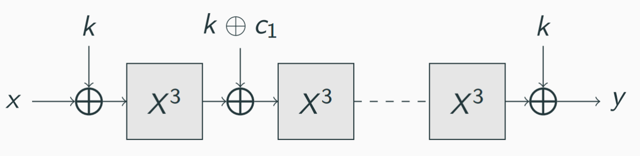


($x \mapsto x^3$ is a permutation **iff** $n = 2n' + 1$ odd and $p \equiv_3 2$)

Assuming $p \approx 2^n$, *large number of rounds*: $\lceil \log_3 p \rceil \approx \lceil n \cdot \log_3 2 \rceil$.
E.g., for $p \approx 2^{128}$:

- AES: 10 rounds and ≈ 960 (MPC) multiplications;
- MiMC: 81 rounds and 162 (MPC) multiplications.

MiMC Cipher

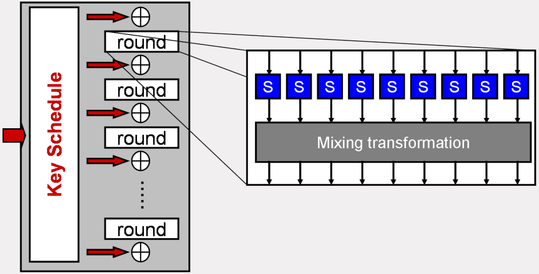


($x \mapsto x^3$ is a permutation **iff** $n = 2n' + 1$ odd and $p \equiv_3 2$)

Assuming $p \approx 2^n$, *large number of rounds*: $\lceil \log_3 p \rceil \approx \lceil n \cdot \log_3 2 \rceil$.
E.g., for $p \approx 2^{128}$:

- AES: 10 rounds and ≈ 960 (MPC) multiplications;
- MiMC: 81 rounds and 162 (MPC) multiplications.

Partial-SPN Symmetric Primitives



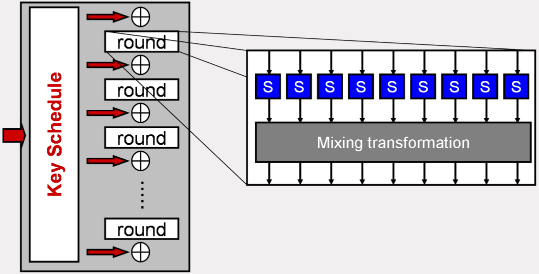
Idea: Move from *full S-Box layer*

$$S_F(x) = [S(x_1) \| S(x_2) \| \ldots \| S(x_t)]$$

to *Partial S-Box layer*

$$S_P(x) = [S(x_1) \| x_2 \| \ldots \| x_t] \,.$$

Partial-SPN Symmetric Primitives



Idea: Move from *full S-Box layer*

$$\mathcal{S}_F(x) = [S(x_1)\|S(x_2)\|\ldots\|S(x_t)]$$

to *Partial S-Box layer*

$$\mathcal{S}_P(x) = [S(x_1)\|x_2\|\ldots\|x_t]\,.$$

P-SPN versus SPN: Advantages and Disadvantages

Advantages of P-SPN:

- cheaper to compute than SPN
- one S-Box per round is sufficient for increasing the overall degree, crucial for preventing (some) algebraic attacks;

but

- guarantee security of P-SPN against statistical attacks is harder than for SPN: the "wide-trail" design strategy does not apply, and ad-hoc security argument must be provided.

Examples: attacks against the P-SPN schemes Zorro (variant of AES) and LowMC.

P-SPN versus SPN: Advantages and Disadvantages

Advantages of P-SPN:

- cheaper to compute than SPN
- one S-Box per round is sufficient for increasing the overall degree, crucial for preventing (some) algebraic attacks;

but

- guarantee security of P-SPN against statistical attacks is harder than for SPN: the "wide-trail" design strategy does not apply, and ad-hoc security argument must be provided.

Examples: attacks against the P-SPN schemes Zorro (variant of AES) and LowMC.

Recall: Wide-Trail Design Strategy (AES-Like Design)

- Design strategy for preventing differential (and linear) attacks;
- **Goal:** minimize probability of any differential characterestic $\Delta_I \to \Delta_O$:

$$\frac{|\{x \mid E_k(x + \Delta_I) - E_k(x) = \Delta_O\}|}{p^t};$$

- Remember: only the S-Boxes impact such probability;
- **Idea:** choose linear layers that active as many S-Boxes as possible, e.g., by instantiating them with "Maximum Distance Separable" (MDS) matrices.

Recall: Wide-Trail Design Strategy (AES-Like Design)

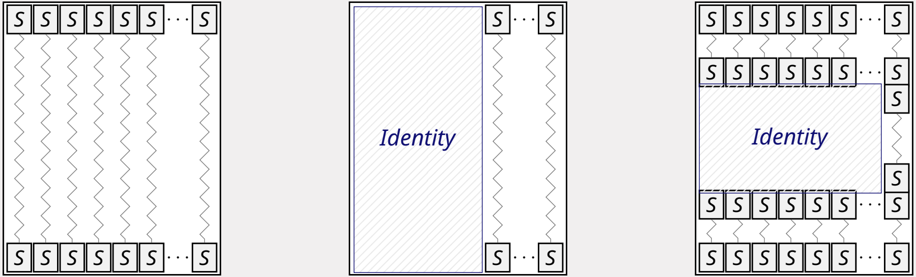
- Design strategy for preventing differential (and linear) attacks;
- **Goal:** minimize probability of any differential characterestic $\Delta_I \to \Delta_O$:

$$\frac{|\{x \mid E_k(x + \Delta_I) - E_k(x) = \Delta_O\}|}{p^t};$$

- Remember: only the S-Boxes impact such probability;
- **Idea:** choose linear layers that active as many S-Boxes as possible, e.g., by instantiating them with "Maximum Distance Separable" (MDS) matrices.

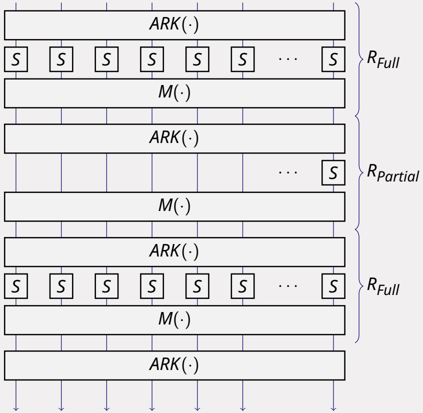
"Hades" Strategy

How to reduce number of non-linear operations & guarantee security with simple/elegant argument?



(a) SPN (b) P-SPN (c) *"Hades" strategy*

The Block Cipher HADESMiMC



- $S(x) = x^d$ where $\gcd(d, p-1) = 1$;
- Linear layer: multiplication with a MDS matrix in $\mathbb{F}_p^{t \times t}$;
- Subkeys defined via an affine map applied to the master key;
- Number of rounds ($\kappa \approx \log_2(p)$):

$$R_F = 2 \cdot R_f = 6\,,$$
$$R_P \approx \log_d(p)$$

TU/e

:

Overview of Security Analysis

- Key-guess: possible only for a single round (due to the size of the key);
- Security against differential/linear attacks: **external full rounds** only, due to Wide-Trail design strategy:
  - $\text{DP}_{\text{max}}(x \mapsto x^d) = (d-1)/p$ and $t+1$ S-Boxes active every 2 rounds;
  - each differential trail has probability $\left(\frac{d-1}{p}\right)^{r\cdot(t+1)/2} \ll 2^{-\kappa}$ for $r \geq 4$;
- Security against MitM interpolation attack: maximum degree is mostly achieved via the **internal partial rounds**;
- Security against Gröbner Basis/factorization attack: combination of internal and external rounds.

Overview of Security Analysis

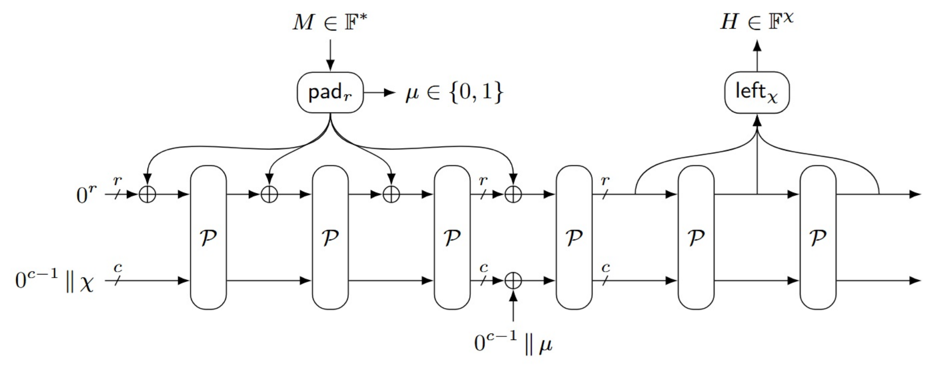
- Key-guess: possible only for a single round (due to the size of the key);
- Security against differential/linear attacks: **external full rounds** only, due to Wide-Trail design strategy:
  - $\mathrm{DP}_{\max}(x \mapsto x^d) = (d-1)/p$ and $t+1$ S-Boxes active every 2 rounds;
  - each differential trail has probability $\left(\frac{d-1}{p}\right)^{r\cdot(t+1)/2} \ll 2^{-\kappa}$ for $r \geq 4$;
- Security against MitM interpolation attack: maximum degree is mostly achieved via the **internal partial rounds**;
- Security against Gröbner Basis/factorization attack: combination of internal and external rounds.

Overview of Security Analysis

- Key-guess: possible only for a single round (due to the size of the key);
- Security against differential/linear attacks: **external full rounds** only, due to Wide-Trail design strategy:
  - $\text{DP}_{\text{max}}(x \mapsto x^d) = (d-1)/p$ and $t+1$ S-Boxes active every 2 rounds;
  - each differential trail has probability $\left(\frac{d-1}{p}\right)^{r\cdot(t+1)/2} \ll 2^{-\kappa}$ for $r \geq 4$;
- Security against MitM interpolation attack: maximum degree is mostly achieved via the **internal partial rounds**;
- Security against Gröbner Basis/factorization attack: combination of internal and external rounds.

Table of Contents

Sponge Hash Function



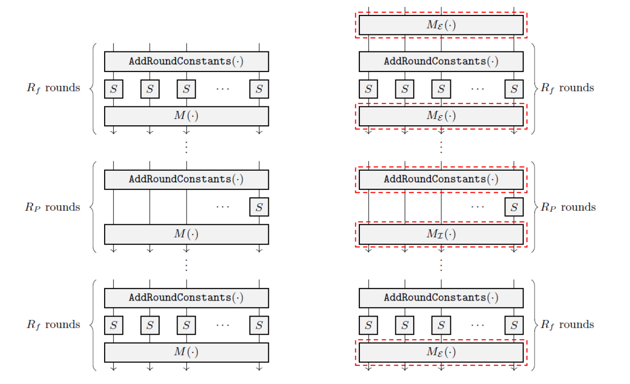
Assuming $\mathcal{P}$ over $\mathbb{F}_2^{c+r}$ is an ideal permutation: security up to $\min\{2^\chi, 2^{c/2}\}$.

Poseidon

- Poseidon is a sponge hash function instantiated by the HadesMiMC permutation (that is, round keys are replaced by round constants).
- Number of rounds for Poseidon is a bit different than the number of rounds of HadesMiMC (due to different attacks):
  - $4+4=8$ external full rounds (instead of 6);
  - partial rounds still $\approx \log_d(p)$.
- Low degree permutation: used both for evaluation and for verification.

POSEIDON2

Same number of rounds of POSEIDON, but (i) two different linear layers (one for external rounds & one for internal ones) + (ii) additional initial linear layer:



POSEIDON2: Linear Layer for Internal/Partial Rounds

- New matrix $M_{\mathcal{I}}$ in partial internal rounds:

$$\begin{bmatrix} \mu_{0,0} & 1 & 1 & \dots & 1 \\ 1 & \mu_{1,1} & 1 & \dots & 1 \\ 1 & 1 & \mu_{2,2} & \dots & 1 \\ \vdots & \vdots & & \ddots & \vdots \\ 1 & 1 & 1 & \dots & \mu_{t-1,t-1} \end{bmatrix};$$

- Values $\mu_{0,0}, \dots, \mu_{t-1,t-1} \in \mathbb{F}_p \setminus \{0\}$ chosen such that:
  - the matrix is invertible;
  - no *infinitely-long* subspace trail for the internal rounds – see

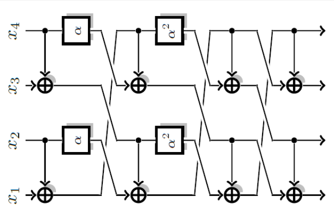
L. Grassi, C. Rechberger, M. Schofnegger: "*Proving Resistance Against Infinitely Long Subspace Trails: How to Choose the Linear Layer.*". IACR ToSC 2021

POSEIDON2: Linear Layer for External/Full Rounds

Let $t = 4 \cdot t'$ be a multiple of 4. Then $M_{\mathcal{E}} \in \mathbb{F}_p^{t \times t}$ is defined as

$$M_{\mathcal{E}} = \begin{bmatrix} 2 \cdot M_{4\times4} & M_{4\times4} & \dots & M_{4\times4} \\ M_{4\times4} & 2 \cdot M_{4\times4} & \dots & M_{4\times4} \\ \vdots & \vdots & \ddots & \vdots \\ M_{4\times4} & M_{4\times4} & \dots & 2 \cdot M_{4\times4} \end{bmatrix},$$

where $M_{4\times4} \in \mathbb{F}_p^{4\times4}$ is a MDS matrix which can be efficiently evaluated as



TU/e

Gröbner Basis + (External) Subspace Trail: POSEIDON(2)

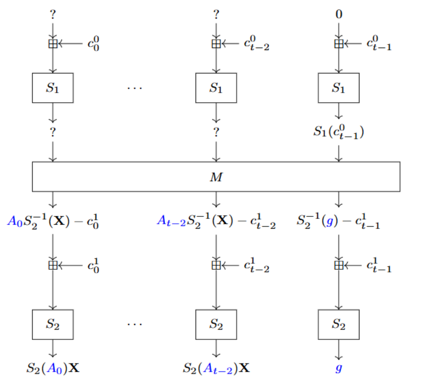


Figure: A. Bariant, C. Bouvier, G. Leurent, L. Perrin: *"Algebraic Attacks against Some Arithmetization-Oriented Primitives."* IACR ToSC 2022

- Initial invertible S-Box layer does *not* provide extra security:

$$[S(x_0), \ldots, S(x_{r-1}), S(\texttt{IV}_r), \ldots, S(\texttt{IV}_{t-1})] \rightarrow [x_0, \ldots, x_{r-1}, \texttt{IV}_r, \ldots, \texttt{IV}_{t-1}];$$

- Exploit degrees of freedom: skip extra full round (thanks also to homomorphic property of the S-Box $S(\alpha \cdot x) = S(\alpha) \cdot S(x)$).

Gröbner Basis + (Internal) Subspace Trail: POSEIDON(2) (1/2)

Exploit degrees of freedom to skip internal partial rounds:

- let $\mathcal{S}^{(\ell)}$ be

$$\mathcal{S}^{(\ell)} := \left\{ x \in \mathbb{F}^t \mid \forall i \in \{0, 1, \ldots, \ell - 1\} : [M^i \times x]_0 = 0 \right\} ;$$

- given $x \in \mathcal{S}^{(\ell)} + \sigma$, then S-Boxes are constant (= inactive) for ℓ partial rounds;
- GB attack (for $1 \leq \ell \leq r - \chi \equiv$ rate $-$ digest):

$$x \in \mathbb{F}^t \xrightarrow{R_P^r \circ R_F^4(\cdot)} \mathcal{S}^{(\ell)} \xrightarrow{R_P^\ell(\cdot)} M^{\ell-1} \times \mathcal{S}^{(\ell)} \xrightarrow{R_F^4 \circ R_P^{r'}(\cdot)} h \in \mathbb{F}^\chi$$

where $r + \ell + r' =$ number of partial rounds.

Gröbner Basis + (Internal) Subspace Trail: POSEIDON(2) (1/2)

Exploit degrees of freedom to skip internal partial rounds:

- let $\mathcal{S}^{(\ell)}$ be

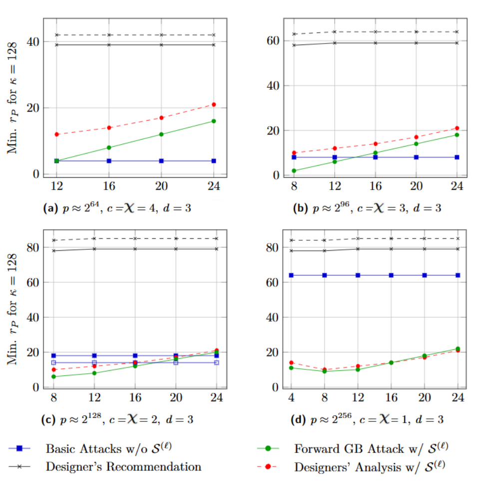
$$\mathcal{S}^{(\ell)} := \left\{x \in \mathbb{F}^t \mid \forall i \in \{0, 1, \ldots, \ell - 1\} : [M^i \times x]_0 = 0\right\} ;$$

- given $x \in \mathcal{S}^{(\ell)} + \sigma$, then S-Boxes are constant (= inactive) for ℓ partial rounds;
- GB attack (for $1 \leq \ell \leq r - \chi \equiv$ rate − digest):

$$x \in \mathbb{F}^t \xrightarrow{R_P^r \circ R_F^4(\cdot)} \mathcal{S}^{(\ell)} \xrightarrow{R_P^\ell(\cdot)} M^{\ell-1} \times \mathcal{S}^{(\ell)} \xrightarrow{R_F^4 \circ R_P^{r'}(\cdot)} h \in \mathbb{F}^\chi$$

where $r + \ell + r' =$ number of partial rounds.

Gröbner Basis + (Internal) Subspace Trail: POSEIDON(2) (2/2)



POSEIDON(2)B over Binary Fields

Versions of POSEIDON/POSEIDON2 over binary fields $\mathbb{F}_{2^n}^t$ for $n \in \{32, 64, 128\}$ targetting Binius:

- matrix $M_{\mathcal{I}}$ for internal partial rounds as in POSEIDON2;
- matrix for external full rounds:
  - MDS for POSEIDONB;
  - $M_{\mathcal{E}}$ (as in POSEIDON2) for POSEIDON2B;
- number of rounds:
  - $\approx \log_d(2^n)$ internal partial rounds;
  - 4+4 external rounds for POSEIDONB;
  - 5+5 external rounds for POSEIDON2B.

Why Extra External Full Rounds for POSEIDON2B?

Potentially, skip "several" external full rounds in a GB attack due to $M_{\mathcal{E}}$:

- the subspace

$$\mathfrak{D} = \{(\delta_0, \delta_1, \delta_2, \delta_3, -\delta_0, -\delta_1, -\delta_2, -\delta_3, 0, 0, 0, 0, \ldots, 0, 0, 0, 0) \in \mathbb{F}^t \mid \delta_0, \delta_1, \delta_2, \delta_3 \in \mathbb{F}\}$$

  is an invariant for $M_{\mathcal{E}}$ with prob. 1 as $\text{circ}(2, 1, \ldots, 1) \times [x, -x, 0, \ldots, 0]^T = [x, -x, 0, \ldots, 0]^T$;
- invariant over one full external round with probability $|\mathbb{F}|^{-4}$;
- still, possibility to exploit it together with the degrees of freedom of the hash function & homomorphic property of the S-Box to skip external full rounds.

Why Extra External Full Rounds for POSEIDON2B?

Potentially, skip "several" external full rounds in a GB attack due to $M_{\mathcal{E}}$:

- the subspace

  $$\mathfrak{D} = \{(\delta_0, \delta_1, \delta_2, \delta_3, -\delta_0, -\delta_1, -\delta_2, -\delta_3, 0, 0, 0, 0, \dots, 0, 0, 0, 0) \in \mathbb{F}^t \mid \delta_0, \delta_1, \delta_2, \delta_3 \in \mathbb{F}\}$$

  is an invariant for $M_{\mathcal{E}}$ with prob. 1 as $\text{circ}(2, 1, \dots, 1) \times [x, -x, 0, \dots, 0]^T = [x, -x, 0, \dots, 0]^T$;
- invariant over one full external round with probability $|\mathbb{F}|^{-4}$;
- still, possibility to exploit it together with the degrees of freedom of the hash function & homomorphic property of the S-Box to skip external full rounds.

Table of Contents

Reducing the Number of Multiplications

$S(x) = x^d$ can be computed with $\lfloor \log_2(d) \rfloor$ squares + $\text{hw}(d) - 1$ multiplications (total of $\lfloor \log_2(d) \rfloor + \text{hw}(d) - 1 \geq 2$ for $d \geq 3$).

$\longrightarrow$ Each external round costs $(\lfloor \log_2(d) \rfloor + \text{hw}(d) - 1) \cdot t \geq \mathbf{2 \cdot t}$ multiplications!

Goal: construct new *invertible non-linear layers* over $\mathbb{F}_p^t$ that

- cost t multiplications (e.g., of degree 2);
- "fully" non-linear (no Feistel/Lai-Massey);
- have (potentially) high-degree inverse.

Reducing the Number of Multiplications

$S(x) = x^d$ can be computed with $\lfloor \log_2(d) \rfloor$ squares + $\text{hw}(d) - 1$ multiplications (total of $\lfloor \log_2(d) \rfloor + \text{hw}(d) - 1 \geq 2$ for $d \geq 3$).

$\longrightarrow$ Each external round costs $(\lfloor \log_2(d) \rfloor + \text{hw}(d) - 1) \cdot t \geq \mathbf{2} \cdot \mathbf{t}$ multiplications!

Goal: construct new *invertible non-linear layers* over $\mathbb{F}_p^t$ that

- cost t multiplications (e.g., of degree 2);
- "fully" non-linear (no Feistel/Lai-Massey);
- have (potentially) high-degree inverse.

SI-Lifting Functions $\mathcal{S}_F$ (1/2)

Let $\mathcal{S} : \mathbb{F}_p^n \to \mathbb{F}_p^n$ be a generic non-linear function:

$$\mathcal{S}(x_0, x_1, \ldots, x_{n-1}) = y_0 \| y_1 \| \ldots \| y_{n-1} \qquad \text{where}$$
$$\forall i \in \{0, 1, \ldots, n-1\} : \qquad y_i := F_i(x_0, x_1, \ldots, x_{n-1})$$

for certain $F_i : \mathbb{F}_p^n \to \mathbb{F}_p$.

$\longrightarrow$ *Too many possible cases to analyze!*

Idea: focus on shift-invariant transformations over $\mathbb{F}_p^n$ defined by a *single local update rule* $F : \mathbb{F}_p^m \to \mathbb{F}_p$ *for* $1 \leq m \leq n$.

SI-Lifting Functions $\mathcal{S}_F$ (1/2)

Let $\mathcal{S} : \mathbb{F}_p^n \to \mathbb{F}_p^n$ be a generic non-linear function:

$$\mathcal{S}(x_0, x_1, \ldots, x_{n-1}) = y_0 \| y_1 \| \ldots \| y_{n-1} \qquad \text{where}$$
$$\forall i \in \{0, 1, \ldots, n-1\} : \qquad y_i := F_i(x_0, x_1, \ldots, x_{n-1})$$

for certain $F_i : \mathbb{F}_p^n \to \mathbb{F}_p$.

$\longrightarrow$ *Too many possible cases to analyze!*

Idea: focus on shift-invariant transformations over $\mathbb{F}_p^n$ defined by a *single local update rule* $F : \mathbb{F}_p^m \to \mathbb{F}_p$ *for* $1 \le m \le n$.

SI-Lifting Functions $\mathcal{S}_F$ (2/2)

The Shift Invariant (SI) lifting function $\mathcal{S}_F : \mathbb{F}_p^n \to \mathbb{F}_p^n$ induced by $F : \mathbb{F}_p^m \to \mathbb{F}_p$ is defined as

$$\mathcal{S}_F(x_0, x_1, \ldots, x_{n-1}) = y_0 \| y_1 \| \ldots \| y_{n-1} \qquad \text{where}$$
$$\forall i \in \{0, 1, \ldots, n-1\} : \qquad y_i := F(x_i, x_{i+1}, \ldots, x_{i+m-1})\,.$$

"Shift Invariant" property due to the fact that:

$$\Pi_i \circ \mathcal{S}_F = \mathcal{S}_F \circ \Pi_i$$

for each shift function $\Pi_i(x_0, x_1, \ldots, x_{n-1}) = x_i \| x_{i+1} \| \ldots \| x_{i+n-1}$.

SI-Lifting Functions $\mathcal{S}_F$ (2/2)

The Shift Invariant (SI) lifting function $\mathcal{S}_F : \mathbb{F}_p^n \to \mathbb{F}_p^n$ induced by $F : \mathbb{F}_p^m \to \mathbb{F}_p$ is defined as

$$\mathcal{S}_F(x_0, x_1, \dots, x_{n-1}) = y_0 \| y_1 \| \dots \| y_{n-1} \qquad \text{where}$$
$$\forall i \in \{0, 1, \dots, n-1\} : \qquad y_i := F(x_i, x_{i+1}, \dots, x_{i+m-1}) \, .$$

“Shift Invariant” property due to the fact that:

$$\Pi_i \circ \mathcal{S}_F = \mathcal{S}_F \circ \Pi_i$$

for each shift function $\Pi_i(x_0, x_1, \dots, x_{n-1}) = x_i \| x_{i+1} \| \dots \| x_{i+n-1}$.

Example of SI-Lifting Functions over $\mathbb{F}_2^n$

See Joan Daemen's PhD Thesis ("*Cipher and Hash Function Design Strategies based on linear and differential cryptanalysis*"):

- given the chi function $\chi : \mathbb{F}_2^3 \to \mathbb{F}_2$:

$$\chi(x_0, x_1, x_2) = x_0 \oplus (x_1 \oplus 1) \cdot x_2 \,,$$

  then $\mathcal{S}_\chi$ over $\mathbb{F}_2^n$ is invertible if and only if $\gcd(n, 2) = 1$;
- given $F(x_0, x_1, x_2, x_3) = x_0 \oplus (x_1 \oplus 1) \cdot x_2 \cdot x_3$, then $\mathcal{S}_F$ over $\mathbb{F}_2^n$ is invertible if and only if $\gcd(n, 3) = 1$;
- given $F(x_0, x_1, \ldots, x_5) = x_1 \oplus (x_0 \oplus 1) \cdot (x_2 \oplus 1) \cdot x_3 \cdot (x_5 \oplus 1)$, then $\mathcal{S}_F$ over $\mathbb{F}_2^n$ is invertible for each $n \geq 6$.

Example of SI-Lifting Functions over $\mathbb{F}_2^n$

See Joan Daemen's PhD Thesis ("*Cipher and Hash Function Design Strategies based on linear and differential cryptanalysis*"):

- given the chi function $\chi : \mathbb{F}_2^3 \to \mathbb{F}_2$:

$$\chi(x_0, x_1, x_2) = x_0 \oplus (x_1 \oplus 1) \cdot x_2 ,$$

  then $\mathcal{S}_\chi$ over $\mathbb{F}_2^n$ is invertible if and only if $\gcd(n, 2) = 1$;
- given $F(x_0, x_1, x_2, x_3) = x_0 \oplus (x_1 \oplus 1) \cdot x_2 \cdot x_3$, then $\mathcal{S}_F$ over $\mathbb{F}_2^n$ is invertible if and only if $\gcd(n, 3) = 1$;
- given $F(x_0, x_1, \ldots, x_5) = x_1 \oplus (x_0 \oplus 1) \cdot (x_2 \oplus 1) \cdot x_3 \cdot (x_5 \oplus 1)$, then $\mathcal{S}_F$ over $\mathbb{F}_2^n$ is invertible for each $n \geq 6$.

Our Goal

Let

- $\mathbf{p \geq 3}$;
- $F : \mathbb{F}_p^m \to \mathbb{F}_p$ **quadratic**.

Given $\mathcal{S}_F : \mathbb{F}_p^n \to \mathbb{F}_p^n$ defined as before, that is,

$$\mathcal{S}_F(x_0, x_1, \ldots, x_{n-1}) = y_0 \| y_1 \| \ldots \| y_{n-1} \qquad \text{where}$$
$$\forall i \in \{0, 1, \ldots, n-1\} : \qquad y_i := F(x_i, x_{i+1}, \ldots, x_{i+m-1}),$$

then

- is it possible to find F for which $\mathcal{S}_F$ is invertible?
- if yes, for any value of n and/or m?

Main Result for $m = 2$

Theorem

Let $p \geq 3$ be a prime, let $m = 2$, and let $n \geq 2$. Let $F : \mathbb{F}_p^2 \to \mathbb{F}_p$ be a quadratic function. Given $\mathcal{S}_F$ over $\mathbb{F}_p^n$:

- *if $n = 2$, then $\mathcal{S}_F$ is invertible if and only if*

$$F(x_0, x_1) = \gamma_0 \cdot x_0 + \gamma_1 \cdot x_1 + \gamma_2 \cdot (x_0 - x_1)^2$$

  for $\gamma_0 \neq \pm\gamma_1$;
- *if $n \geq 3$, then $\mathcal{S}_F$ is **never** invertible.*

Sketch of the Proof – Case: $m = 2$ and $n \geq 3$ (1/2)

Collisions over $\mathbb{F}_p^3$ of the form

$$\mathcal{S}_F(0, x_0, x_1) = \mathcal{S}_F(0, x_0', x_1'),$$

imply collisions over $\mathbb{F}_p^n$ for each $n \geq 3$ of the form

$$\mathcal{S}_F(0, x_0, x_1, 0, 0, \ldots, 0) = \mathcal{S}_F(0, x_0', x_1', 0, 0, \ldots, 0).$$

Indeed, both are satisfied by

$$F(0, x_0) = F(0, x_0'), \quad F(x_0, x_1) = F(x_0', x_1'), \quad F(x_1, 0) = F(x_1', 0).$$

$\longrightarrow$ We limit ourselves to $n = 3$ and $\mathcal{S}_F(0, x_0, x_1) = \mathcal{S}_F(0, x_0', x_1')$.

Sketch of the Proof – Case: $m = 2$ and $n \geq 3$ (1/2)

Collisions over $\mathbb{F}_p^3$ of the form

$$\mathcal{S}_F(0, x_0, x_1) = \mathcal{S}_F(0, x_0', x_1'),$$

imply collisions over $\mathbb{F}_p^n$ for each $n \geq 3$ of the form

$$\mathcal{S}_F(0, x_0, x_1, 0, 0, \ldots, 0) = \mathcal{S}_F(0, x_0', x_1', 0, 0, \ldots, 0).$$

Indeed, both are satisfied by

$$F(0, x_0) = F(0, x_0'), \quad F(x_0, x_1) = F(x_0', x_1'), \quad F(x_1, 0) = F(x_1', 0).$$

$\longrightarrow$ We limit ourselves to $n = 3$ and $\mathcal{S}_F(0, x_0, x_1) = \mathcal{S}_F(0, x_0', x_1')$.

Sketch of the Proof – Case: $m = 2$ and $n \geq 3$ (2/2)

Necessary requirements for invertibility of $\mathcal{S}_F$:

- $\alpha_{2,0} + \alpha_{1,1} + \alpha_{0,2} = 0$;
- $\alpha_{1,0} + \alpha_{0,1} \neq 0$.

In the paper, collisions are proposed in order to cover all the cases just given. E.g., if $\alpha_{2,0}, \alpha_{1,1} \neq 0$ with $\alpha_{2,0} + \alpha_{1,1} + \alpha_{0,2} = 0$:

$$\mathcal{S}_F\left(0, \frac{\alpha_{0,2} \cdot \alpha_{1,0}}{\alpha_{1,1} \cdot \alpha_{2,0}} - \frac{\alpha_{0,1}}{\alpha_{1,1}}, x\right) = \mathcal{S}_F\left(0, \frac{\alpha_{0,2} \cdot \alpha_{1,0}}{\alpha_{1,1} \cdot \alpha_{2,0}} - \frac{\alpha_{0,1}}{\alpha_{1,1}}, -x - \frac{\alpha_{1,0}}{\alpha_{2,0}}\right)$$

for each $x \in \mathbb{F}_p$.

Main Result for $m = 3$ and $n \geq 5$

Theorem

*Let $p \geq 3$ be a prime, let $m = 3$, and let $n \geq 5$. Let $F : \mathbb{F}_p^3 \to \mathbb{F}_p$ be **any** quadratic function. The SI-lifting function $\mathcal{S}_F$ over $\mathbb{F}_p^n$ induced by F is **never** invertible.*

- Strategy of the proof similar to the one just proposed for $m = 2$ and $n \geq 3$.
- *Different from the binary case*, for which $\mathcal{S}_F$ over $\mathbb{F}_2^n$ can be invertible depending on $F : \mathbb{F}_2^3 \to \mathbb{F}_2$ and on n (e.g., χ).

NEPTUNE's External Rounds: Non-Linear Layer

Goal: modify the external rounds for *reducing the total number of multiplications* without decreasing the security.

- Given any quadratic $F : \mathbb{F}_p^{\leq 3} \to \mathbb{F}_p$, then $\mathcal{S}_F$ over $\mathbb{F}_p^{\geq 5}$ is **not** invertible.
- Let $t = 2 \cdot t'$ even. Non-linear layer of NEPTUNE's external rounds via concatenation of S-Boxes $\mathcal{S}$ over $\mathbb{F}_p^2$, defined as

$$\mathcal{S}(x_0, x_1) = \mathcal{S}' \circ \mathcal{A} \circ \mathcal{S}'(x_0, x_1)$$

where (for $\gamma \neq 0$):

$$\mathcal{S}'(x_0, x_1) = x_0 + (x_0 - x_1)^2 \| x_1 + (x_0 - x_1)^2 \,,$$

$$\mathcal{A}(x_0, x_1) = \begin{bmatrix} \gamma \\ 0 \end{bmatrix} + \begin{bmatrix} 2 & 1 \\ 1 & 3 \end{bmatrix} \times \begin{bmatrix} x_0 \\ x_1 \end{bmatrix} .$$

NEPTUNE's External Rounds: Non-Linear Layer

Goal: modify the external rounds for *reducing the total number of multiplications* without decreasing the security.

- Given any quadratic $F : \mathbb{F}_p^{\leq 3} \to \mathbb{F}_p$, then $\mathcal{S}_F$ over $\mathbb{F}_p^{\geq 5}$ is **not** invertible.
- Let $t = 2 \cdot t'$ even. Non-linear layer of NEPTUNE's external rounds via concatenation of S-Boxes $\mathcal{S}$ over $\mathbb{F}_p^2$, defined as

$$\mathcal{S}(x_0, x_1) = \mathcal{S}' \circ \mathcal{A} \circ \mathcal{S}'(x_0, x_1)$$

where (for $\gamma \neq 0$):

$$\mathcal{S}'(x_0, x_1) = x_0 + (x_0 - x_1)^2 \| x_1 + (x_0 - x_1)^2 \,,$$

$$\mathcal{A}(x_0, x_1) = \begin{bmatrix} \gamma \\ 0 \end{bmatrix} + \begin{bmatrix} 2 & 1 \\ 1 & 3 \end{bmatrix} \times \begin{bmatrix} x_0 \\ x_1 \end{bmatrix} .$$

NEPTUNE's External Rounds: Linear Layer

Given the state as an element of $\mathbb{F}_p^{t' \times 2} \equiv \mathbb{F}_p^{t/2 \times 2}$:

- apply the S-Boxes over $\mathbb{F}_p^2$ on each row;
- multiply each column by a $t' \times t'$ MDS matrix.

Not every MDS matrix is equally good! E.g., over $\mathbb{F}_p^4$, given

$$M = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} \qquad \text{and} \qquad M' = \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix},$$

the degree grows as $4, 14, 56, \ldots$ instead of $4, 4^2 = 16, 4^3 = 64, \ldots$

$\longrightarrow$ conditions on the MDS matrices – see M. Urani and L. Grassi: "*Corrigendum to 'Invertible Quadratic Non-Linear Layers for MPC-/FHE-/ZK-Friendly Schemes over $\mathbb{F}_p^n$ – Application to Poseidon'*". IACR ToSC 2026.

NEPTUNE's External Rounds: Linear Layer

Given the state as an element of $\mathbb{F}_p^{t'\times 2} \equiv \mathbb{F}_p^{t/2\times 2}$:

- apply the S-Boxes over $\mathbb{F}_p^2$ on each row;
- multiply each column by a $t' \times t'$ MDS matrix.

Not every MDS matrix is equally good! E.g., over $\mathbb{F}_p^4$, given

$$M = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} \qquad \text{and} \qquad M' = \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix} ,$$

the degree grows as $4, 14, 56, \ldots$ instead of $4, 4^2 = 16, 4^3 = 64, \ldots$
$\longrightarrow$ conditions on the MDS matrices – see M. Urani and L. Grassi: "*Corrigendum to 'Invertible Quadratic Non-Linear Layers for MPC-/FHE-/ZK-Friendly Schemes over* $\mathbb{F}_p^n$ *– Application to Poseidon'*". IACR ToSC 2026.

NEPTUNE versus POSEIDON (with $S(x) = x^5$)

Cost of t *multiplications for computing* $\mathcal{S}$ (versus $\geq 2 \cdot t$ for power maps).

Table: Comparison of POSEIDON and NEPTUNE – both instantiated with $d = 5$ – for the case $p \approx 2^{128}$ (or bigger), $\kappa = 128$, and several values of $t \in \{4, 8, 12, 16\}$.

	t	R_F	R_P & R_I	Multiplicative Complexity
POSEIDON ($d = 5$)	4	8	60	276 (+ 21.0 %)
NEPTUNE ($d = 5$)	4	6	68	**228**
POSEIDON ($d = 5$)	8	8	60	372 (+ 40.1 %)
NEPTUNE ($d = 5$)	8	6	72	**264**
POSEIDON ($d = 5$)	12	8	61	471 (+ 53.9 %)
NEPTUNE ($d = 5$)	12	6	78	**306**
POSEIDON ($d = 5$)	16	8	61	567 (+ 64.3 %)
NEPTUNE ($d = 5$)	16	6	83	**345**

Table of Contents

What about the Non-Invertible Non-Linear Layer?

Let $p \geq 3$. Given any quadratic function $F : \mathbb{F}_p^m \to \mathbb{F}_p$, then the SI-lifting function $\mathcal{S}_F$ over $\mathbb{F}_p^n$ is **not** invertible if

- $m = 1$, $n \geq 1$;
- $m = 2$, $n \geq 3$;
- $m = 3$, $n \geq 5$.

It is trivial to find collisions for a hash function instantiated with such non-invertible quadratic functions!

Remark: *we discourage the use of low-degree non-bijective components for designing symmetric primitives in which the internal state is not obfuscated by a secret.*

What about the Non-Invertible Non-Linear Layer?

Let $p \geq 3$. Given any quadratic function $F : \mathbb{F}_p^m \to \mathbb{F}_p$, then the SI-lifting function $\mathcal{S}_F$ over $\mathbb{F}_p^n$ is **not** invertible if

- $m = 1, n \geq 1;$
- $m = 2, n \geq 3;$
- $m = 3, n \geq 5.$

It is trivial to find collisions for a hash function instantiated with such non-invertible quadratic functions!

Remark: *we discourage the use of low-degree non-bijective components for designing symmetric primitives in which the internal state is not obfuscated by a secret.*

Non-Invertible Non-Linear Layer for Ciphers (1/2)

Let's use them for instantiating a cipher! The non-linear layer

$$[x_0, x_1, \ldots, x_{n-1}] \mapsto [x_0^2, x_1^2, \ldots, x_{n-1}^2]$$

over $\mathbb{F}_p^n$ is **not** a good choice in general:

- number of collisions given by

$$\frac{(2 \cdot p - 1)^n - p^n}{p^n \cdot (p^n - 1)} \approx \frac{2^n - 1}{p^n - 1} ;$$

- *key-recovery attacks* can be potentially set up by exploiting the fact that $[x_0^2, x_1^2, \ldots, x_{n-1}^2] = [y_0^2, y_1^2, \ldots, y_{n-1}^2]$ if and only if $x_i = \pm y_i$.

Non-Invertible Non-Linear Layer for Ciphers (2/2)

Goal: Find *the quadratic function* $F : \mathbb{F}_p^2 \to \mathbb{F}_p$ such that

1. the number of collisions in $\mathcal{S}_F$ over $\mathbb{F}_p^n$ is minimized;
2. minimize the multiplicative cost of computing $\mathcal{S}_F$.

Such function is $F(x_0, x_1) = x_1^2 + x_0$ (or similar) for which

- the probability that a collision occurs at the output of $\mathcal{S}_F$ over $\mathbb{F}_p^n$ is

$$\frac{(p-1)^n}{p^n \cdot (p^n - 1)/2} \leq \frac{2}{p^n} \qquad (\ll 1 \text{ for big } p)\,;$$

- $\mathcal{S}_F(x_0, x_1, \ldots, x_{n-1}) = \mathcal{S}_F(y_0, y_1, \ldots, y_{n-1})$ implies $x_i \neq y_i$ for **all** i.

Non-Invertible Non-Linear Layer for Ciphers (2/2)

Goal: Find *the quadratic function* $F : \mathbb{F}_p^2 \to \mathbb{F}_p$ such that

1. the number of collisions in $\mathcal{S}_F$ over $\mathbb{F}_p^n$ is minimized;
2. minimize the multiplicative cost of computing $\mathcal{S}_F$.

Such function is $F(x_0, x_1) = x_1^2 + x_0$ (or similar) for which

- the probability that a collision occurs at the output of $\mathcal{S}_F$ over $\mathbb{F}_p^n$ is

$$\frac{(p-1)^n}{p^n \cdot (p^n - 1)/2} \leq \frac{2}{p^n} \qquad (\ll 1 \text{ for big } p)\,;$$

- $\mathcal{S}_F(x_0, x_1, \ldots, x_{n-1}) = \mathcal{S}_F(y_0, y_1, \ldots, y_{n-1})$ implies $x_i \neq y_i$ for **all** i.

From HadesMiMC to PLUTO

Idea: replace the non-linear layer $(x_0, x_1, \ldots, x_{t-1}) \mapsto (x_0^d, x_1^d, \ldots, x_{t-1}^d)$ in the external rounds with

$$(x_0, x_1, \ldots, x_{t-1}) \mapsto (x_1^2 + x_0, x_2^2 + x_1, \ldots, x_0^2 + x_{t-1}),$$

which costs **t** multiplications *independently of* p.

Security analogous to the one proposed for HADESMIMC. Main differences:

- collision probability at the output of PLUTO $\ll 2^{-\kappa}$;
- external rounds are not invertible, but only local inverses can be set up: we conjecture that $4 + 4 = 8$ external rounds are sufficient to prevent algebraic attacks in the backward direction.

From HadesMiMC to PLUTO

Idea: replace the non-linear layer $(x_0, x_1, \ldots, x_{t-1}) \mapsto (x_0^d, x_1^d, \ldots, x_{t-1}^d)$ in the external rounds with

$$(x_0, x_1, \ldots, x_{t-1}) \mapsto (x_1^2 + x_0, x_2^2 + x_1, \ldots, x_0^2 + x_{t-1}),$$

which costs **t** multiplications *independently of p*.

Security analogous to the one proposed for HADESMIMC. Main differences:

- collision probability at the output of PLUTO $\ll 2^{-\kappa}$;
- external rounds are not invertible, but only local inverses can be set up: we conjecture that $4 + 4 = 8$ external rounds are sufficient to prevent algebraic attacks in the backward direction.

Multiplicative Complexity (MPC): HadesMiMC versus PLUTO

Comparison between HADESMiMC (instantiated with $x \mapsto x^3$) and PLUTO for the case $p \approx 2^{128}$, $\kappa = 128$, and several values of $t \in \{4, 8, 12, 16\}$:

	t	R_F	R_P	Multiplicative Complexity
HADESMiMC ($d = 3$)	4	6	47	142 (+ 22.4 %)
PLUTO	4	8	42	**116**
HADESMiMC ($d = 3$)	8	6	48	192 (+ 24.7 %)
PLUTO	8	8	45	**154**
HADESMiMC ($d = 3$)	12	6	49	242 (+ 24.7 %)
PLUTO	12	8	49	**194**
HADESMiMC ($d = 3$)	16	6	49	290 (+ 26.1 %)
PLUTO	16	8	51	**230**

Table of Contents

Summary

- Several hash functions have been proposed for ZK: POSEIDON(2)/POSEIDON(2)B seem to be both competitive and secure;
- More cryptanalysis (especially, third-party cryptanalysis) is required to increase our confidence in the security:
  - Ethereum initiative/challenges;
- POSEIDON(2)/POSEIDON(2)B is not the end of the story: potential improvements in the design are possible!

Thanks for your attention!

Questions?

Comments?