Invertible Quadratic Non-Linear Layers for MPC-/FHE-/ZK-Friendly Schemes over $\mathbb{F}_p^n$

Application to Poseidon

Lorenzo Grassi, Silvia Onofri, Marco Pedicini, Luca Sozzi

Radboud University, Nijmegen, the Netherlands
Scuola Normale Superiore di Pisa, Pisa, Italy
Università Roma Tre, Roma, Italy
Università degli Studi di Milano, Milano, Italy

Motivation

Symmetric Primitives for MPC/FHE/ZK Applications

New applications including

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

require symmetric-key primitives that

(1) *are naturally defined over* $(\mathbb{F}_p)^n$ *for a* **large** *prime integer* p (usually, $p \approx 2^{128}$ or 2^{256});

(2) *minimize their multiplicative complexity*, that is, the number of multiplications ($=$ non-linear operations) required to compute and/or verify them.

Invertible Non-Linear Operations over $\mathbb{F}_p^n$

Due to the size of p, the non-linear operations

- cannot be pre-computed and stored (no look-up tables);
- they must admit a simple algebraic expression.

Current known invertible non-linear operations:

- power map $x \mapsto x^d$ over $\mathbb{F}_p$ where $\gcd(d, p-1) = 1$;
- Dickson polynomial $x \mapsto D_{d,\alpha}(x) = \sum_{i=0}^{\lfloor d/2 \rfloor} \frac{d}{d-i} \binom{d-i}{i} \cdot (-\alpha)^i \cdot x^{d-2i}$ over $\mathbb{F}_p$ where $\gcd(d, p^2-1) = 1$;
- non-linear functions over $\mathbb{F}_p$ via Legendre function $x \mapsto L_p(x) = x^{\frac{p-1}{2}} \in \{-1, 0, 1\}$ or/and $x \mapsto (-1)^x$ operator;
- non-linear layers over $\mathbb{F}_p^n$ instantiated via Feistel and/or Lai-Massey schemes, e.g., $(x_0, x_1) \mapsto (x_1, x_1^2 + x_0)$.

Invertible Non-Linear Operations over $\mathbb{F}_p^n$

Due to the size of p, the non-linear operations

- cannot be pre-computed and stored (no look-up tables);
- they must admit a simple algebraic expression.

Current known invertible non-linear operations:

- power map $x \mapsto x^d$ over $\mathbb{F}_p$ where $\gcd(d, p-1) = 1$;
- Dickson polynomial $x \mapsto D_{d,\alpha}(x) = \sum_{i=0}^{\lfloor d/2 \rfloor} \frac{d}{d-i} \binom{d-i}{i} \cdot (-\alpha)^i \cdot x^{d-2i}$ over $\mathbb{F}_p$ where $\gcd(d, p^2-1) = 1$;
- non-linear functions over $\mathbb{F}_p$ via Legendre function $x \mapsto L_p(x) = x^{\frac{p-1}{2}} \in \{-1, 0, 1\}$ or/and $x \mapsto (-1)^x$ operator;
- non-linear layers over $\mathbb{F}_p^n$ instantiated via Feistel and/or Lai-Massey schemes, e.g., $(x_0, x_1) \mapsto (x_1, x_1^2 + x_0)$.

Goals

- Changing d in base of p (e.g., $\gcd(d, p-1) = 1$) is not desirable:
  - potentially harder (algebraic) security analysis which must be adapted depending on p and so on d (e.g., density of the polynomial representation);
  - efficiency could depend on the choice of d.
- Feistel and/or Lai-Massey schemes are "partially linear" (do not provide "full non-linearity").

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

- cost n multiplications (e.g., of degree 2);
- have (potentially) high-degree inverse.

Goals

- Changing d in base of p (e.g., $\gcd(d, p-1) = 1$) is not desirable:
  - potentially harder (algebraic) security analysis which must be adapted depending on p and so on d (e.g., density of the polynomial representation);
  - efficiency could depend on the choice of d.
- Feistel and/or Lai-Massey schemes are "partially linear" (do not provide "full non-linearity").

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

- cost n multiplications (e.g., of degree 2);
- have (potentially) high-degree inverse.

Shift Invariant Lifting Functions $\mathcal{S}_F$ over $\mathbb{F}_p^n$ Induced by a Local Map $F : \mathbb{F}_p^m \to \mathbb{F}_p$

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

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

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

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

Idea: *define $\mathcal{S}$ as a Cellular Automata (CA)*, that is, a shift-invariant transformation over a $\mathbb{F}_p^n$–array of cells defined by a *single local* update rule $F : \mathbb{F}_p^m \to \mathbb{F}_p$ for $1 \leq m \leq n$.

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: *define $\mathcal{S}$ as a Cellular Automata (CA)*, that is, a shift-invariant transformation over a $\mathbb{F}_p^n$–array of cells 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 $\mathcal{S}_F$ (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 Π_i over $\mathbb{F}_p^n$ defined as

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

for $i \in \{0, 1, \ldots, n-1\}$.

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

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

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

for $i \in \{0, 1, \ldots, n-1\}$.

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 the function

$$F(x_0, x_1, x_2, x_3) = x_0 \oplus (x_1 \oplus 1) \cdot x_2 \cdot x_3 \,,$$

  then $\mathcal{S}_F$ over $\mathbb{F}_2^n$ is invertible if and only if $\gcd(n, 3) = 1$;

- given the function

$$F(x_0, x_1, \ldots, x_5) = x_1 \oplus (x_0 \oplus 1) \cdot (x_2 \oplus 1) \cdot x_3 \cdot (x_5 \oplus 1) \,,$$

  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 the function

$$F(x_0, x_1, x_2, x_3) = x_0 \oplus (x_1 \oplus 1) \cdot x_2 \cdot x_3 \,,$$

  then $\mathcal{S}_F$ over $\mathbb{F}_2^n$ is invertible if and only if $\gcd(n, 3) = 1$;
- given the function

$$F(x_0, x_1, \ldots, x_5) = x_1 \oplus (x_0 \oplus 1) \cdot (x_2 \oplus 1) \cdot x_3 \cdot (x_5 \oplus 1) \,,$$

  then $\mathcal{S}_F$ over $\mathbb{F}_2^n$ is invertible for each $n \geq 6$.

Our Goal

Let

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

SI-Lifting Functions $\mathcal{S}_F$ over $\mathbb{F}_p^n$ via Quadratic $F : \mathbb{F}_p^m \to \mathbb{F}_p$: Results for $m \in \{2, 3\}$

Necessary Conditions for Inveritibility

Let $F : \mathbb{F}_p^m \to \mathbb{F}_p$ be a quadratic function:

$$F(x_0, x_1, \ldots, x_{m-1}) := \sum_{0 \le i_0+i_1+\ldots+i_{m-1} \le 2} \alpha_{i_0,i_1,\ldots,i_{m-1}} \cdot x_0^{i_0} \cdot x_1^{i_1} \cdot \ldots \cdot x_{m-1}^{i_{m-1}} .$$

Let $\alpha^{(d)}$ be the sum of the coefficients of the degree-d monomials:

$$\alpha^{(d)} := \sum_{i_0+i_1+\ldots+i_{m-1}=d} \alpha_{i_0,i_1,\ldots,i_{m-1}} .$$

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

$$\alpha^{(2)} = 0 \quad \text{and} \quad \alpha^{(1)} \neq 0 .$$

- If $\alpha^{(2)} = \alpha^{(1)} = 0$: $F(x, x, \ldots, x) = F(0, 0, \ldots, 0)$;
- If $\alpha^{(2)} \neq 0$: $F(x, x, \ldots, x) = \alpha^{(2)} \cdot x^2 + \alpha^{(1)} \cdot x + \alpha_{0,0,\ldots,0}$, hence collisions $\mathcal{S}_F(x', x', \ldots, x') = \mathcal{S}_F(\hat{x}, \hat{x}, \ldots, \hat{x})$.

Let $F : \mathbb{F}_p^m \to \mathbb{F}_p$ be a quadratic function:

$$F(x_0, x_1, \ldots, x_{m-1}) := \sum_{0 \le i_0 + i_1 + \ldots + i_{m-1} \le 2} \alpha_{i_0, i_1, \ldots, i_{m-1}} \cdot x_0^{i_0} \cdot x_1^{i_1} \cdot \ldots \cdot x_{m-1}^{i_{m-1}} .$$

Let $\alpha^{(d)}$ be the sum of the coefficients of the degree-d monomials:

$$\alpha^{(d)} := \sum_{i_0 + i_1 + \ldots + i_{m-1} = d} \alpha_{i_0, i_1, \ldots, i_{m-1}} .$$

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

$$\alpha^{(2)} = 0 \quad \text{and} \quad \alpha^{(1)} \neq 0 .$$

- If $\alpha^{(2)} = \alpha^{(1)} = 0$: $F(x, x, \ldots, x) = F(0, 0, \ldots, 0)$;
- If $\alpha^{(2)} \neq 0$: $F(x, x, \ldots, x) = \alpha^{(2)} \cdot x^2 + \alpha^{(1)} \cdot x + \alpha_{0,0,\ldots,0}$, hence collisions $\mathcal{S}_F(x', x', \ldots, x') = \mathcal{S}_F(\hat{x}, \hat{x}, \ldots, \hat{x})$.

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:

$$F(x_0, x_1) = \alpha_{2,0} \cdot x_0^2 + \alpha_{1,1} \cdot x_0 \cdot x_1 + \alpha_{0,2} \cdot x_1^2 + \alpha_{1,0} \cdot x_0 + \alpha_{0,1} \cdot x_1 \,.$$

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

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

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

Examples of Invertible SI-Lifting Functions $\mathcal{S}_F$ for $m = 3$ and $n \in \{3, 4\}$

- *Case $n = m = 3$:* given
$$F(x_0, x_1, x_2) = \sum_{i=0}^{2} \mu_i \cdot x_i + (x_0 - x_1)^2 + (x_1 - x_2)^2 + (x_0 - x_2)^2 \, ,$$
such that $\text{circ}(\mu_0, \mu_1, \mu_2) \in \mathbb{F}_p^{3\times 3}$ is invertible, then $\mathcal{S}_F$ over $\mathbb{F}_p^3$ is invertible.

- *Case $n = 3$ and $m = 4$:* given
$$F(x_0, x_1, x_2) = \alpha \cdot (x_0 + x_2) + \beta \cdot x_1 + (x_0 - x_2)^2 \, ,$$
such that $\alpha \neq \pm\beta/2$, then $\mathcal{S}_F$ over $\mathbb{F}_p^4$ is invertible.

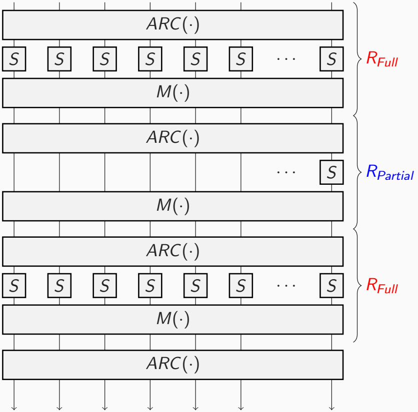
- Other examples given in the paper.

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).

The Sponge Hash Function Neptune



- $S(x) = x^d$ where $d \geq 3$ s.t. $\gcd(d, p-1) = 1$;
- Linear layer: multiplication with a MDS matrix in $\mathbb{F}_p^{t \times t}$ (that prevents infinitely long subspace trails);
- Random constants addition in $\mathbb{F}_p^t$.
- Number of rounds ($\kappa \approx \log_2(p)$):

$$R_F = 2 \cdot R_f = 8\,,$$
$$R_P \approx \log_d(p)$$

From Poseidon to Neptune

- Internal partial rounds are crucial for increasing the degree of the permutation, and so preventing algebraic attacks. Cost of

$$\underbrace{(\text{Hw}(d) + \lfloor \log_2(d) \rfloor - 1)}_{\geq 2} \cdot \underbrace{R_P}_{\approx \log_d(p)}$$

multiplications, which is *independent of t*;

- External full rounds guarantee security against statistical attacks, including differential, linear, and so on. Cost of

$$\underbrace{(\text{Hw}(d) + \lfloor \log_2(d) \rfloor - 1) \cdot R_F}_{\geq \mathbf{16}} \cdot \mathbf{t}$$

multiplications, which *depends on t*;

- **Goal**: modify the external rounds for *reducing the total number of multiplications (= factor that multiplies t)* without decreasing the security.

- Internal partial rounds are crucial for increasing the degree of the permutation, and so preventing algebraic attacks. Cost of

$$\underbrace{(\text{Hw}(d) + \lfloor \log_2(d) \rfloor - 1)}_{\geq 2} \cdot \underbrace{R_P}_{\approx \log_d(p)}$$

multiplications, which is *independent of t*;

- External full rounds guarantee security against statistical attacks, including differential, linear, and so on. Cost of

$$\underbrace{(\text{Hw}(d) + \lfloor \log_2(d) \rfloor - 1) \cdot R_F}_{\geq \mathbf{16}} \cdot \mathbf{t}$$

multiplications, which *depends on t*;

- **Goal**: modify the external rounds for *reducing the total number of multiplications (= factor that multiplies t)* without decreasing the security.

Neptune's External Rounds: Non-Linear Layer

- 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 $\gamma \neq 0$):

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

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

- Differential property of $\mathcal{S}$: $\mathrm{DP}_{\max} = p^{-1}$;
- Cost of t *multiplications for computing* $\mathcal{S}$ (versus $\geq 2 \cdot t$ for power maps).

Neptune's External Rounds: Non-Linear Layer

- 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 $\gamma \neq 0$):

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

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

- Differential property of $\mathcal{S}$: $\mathrm{DP}_{\max} = p^{-1}$;
- Cost of t *multiplications for computing* $\mathcal{S}$ (versus $\geq 2 \cdot t$ for power maps).

Neptune versus Poseidon – $S(x) = x^5$

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**

(See the paper for more details about Neptune' specification.)

Summary and Open Problems

- 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
  - $m = 1$, $n \geq 1$;
  - $m = 2$, $n \geq 3$;
  - $m = 3$, $n \geq 5$.
- **Open Conjecture:** Given F as before, $\mathcal{S}_F$ is **never** invertible if $n \geq 2 \cdot m - 1$;
- **Open Problem:** Construct invertible non-linear functions over $\mathbb{F}_p^n$ with minimal multiplicative complexity;
- Exploit them when designing future MPC-/ZK-/FHE-friendly symmetric schemes!

Summary and Open Problems

- 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
  - $m = 1$, $n \geq 1$;
  - $m = 2$, $n \geq 3$;
  - $m = 3$, $n \geq 5$.
- **Open Conjecture:** Given F as before, $\mathcal{S}_F$ is **never** invertible if $n \geq 2 \cdot m - 1$;
- **Open Problem:** Construct invertible non-linear functions over $\mathbb{F}_p^n$ with minimal multiplicative complexity;
- Exploit them when designing future MPC-/ZK-/FHE-friendly symmetric schemes!

Thanks for your attention!

Questions?

Comments?

Lai-Massey Schemes: Example of SI-Lifting Functions for $m = n$

Let $\text{circ}(\mu_0, \mu_1, \ldots, \mu_{n-1}) \in \mathbb{F}_p^{n\times n}$ be an invertible circulant matrix. Given an invertible even function $H : \mathbb{F}_p \to \mathbb{F}_p$ (i.e., $H(z) = H(-z)$), let

$$F(x_0, x_1, \ldots, x_{n-1}) = \sum_{i=0}^{n-1} \mu_i \cdot x_i + H\left(\sum_{i=0}^{n-1} (-1)^i \cdot x_i\right) .$$

If $n = 2n'$ is even, then $\mathcal{S}_F$ over $\mathbb{F}_p^n$ is invertible.

Proof. Given $\mathcal{S}_F(x_0, x_1, \ldots, x_{n-1}) = y_0 \| y_1 \| \ldots \| y_{n-1}$:

- if $\text{circ}(\mu_0, \mu_1, \ldots, \mu_{n-1}) = \text{circ}(1, 0, \ldots, 0)$, then $\sum_{i=0}^{n-1} (-1)^i \cdot x_i = \sum_{i=0}^{n-1} (-1)^i \cdot y_i$;
- otherwise, work with $z \in \mathbb{F}_p^n$ defined as $z = \text{circ}^{-1}(\mu_0, \mu_1, \ldots, \mu_{n-1}) \times y$.

(Other examples in the paper.)

Another Necessary Conditions for Inveritibility

Definition. A function $F : \mathbb{F}_p^m \to \mathbb{F}_p$ is balanced if and only if

$$\forall y \in \mathbb{F}_p : \qquad \left|\{x \in \mathbb{F}_p^m \mid F(x) = y\}\right| = p^{m-1} \, .$$

Lemma. If F is not balanced, then $\mathcal{S}_F$ is **not** invertible.

Example. Let $p \geq 2$ be a prime, and let $F : \mathbb{F}_p^2 \to \mathbb{F}_p$ be

$$F(x_0, x_1) = \alpha_{2,0} \cdot x_0^2 + \alpha_{1,1} \cdot x_0 \cdot x_1 + \alpha_{0,2} \cdot x_1^2 + \alpha_{1,0} \cdot x_0 + \alpha_{0,1} \cdot x_1 \, .$$

If $\alpha_{2,0} = \alpha_{0,2} = 0$, then F is **not** a balanced function.

Neptune's External Rounds: Linear Layer

Given $M', M'' \in \mathbb{F}_p^{t' \times t'}$ two MDS matrices, linear layer $M \in \mathbb{F}_p^{t \times t}$ of NEPTUNE's external rounds defined as

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

that is,

$$M = \begin{bmatrix} M'_{0,0} & 0 & M'_{0,1} & 0 & \dots & M'_{0,t'-1} & 0 \\ 0 & M''_{0,0} & 0 & M''_{0,1} & \dots & 0 & M''_{0,t'-1} \\ M'_{1,0} & 0 & M'_{1,1} & 0 & \dots & M'_{1,t'-1} & 0 \\ 0 & M''_{1,0} & 0 & M''_{1,1} & \dots & 0 & M''_{1,t'-1} \\ \vdots & & & & \ddots & & \vdots \\ M'_{t'-1,0} & 0 & M'_{t'-1,1} & 0 & \dots & M'_{t'-1,t'-1} & 0 \\ 0 & M''_{t'-1,0} & 0 & M''_{t'-1,1} & \dots & 0 & M''_{t'-1,t'-1} \end{bmatrix}.$$

References i

G. Bertoni, J. Daemen, M. Peeters, G. Van Assche
On the Indifferentiability of the Sponge Construction.
EUROCRYPT 2008

J. Daemen and V. Rijmen
The Wide Trail Design Strategy.
IMACC 2001

J. Daemen
Cipher and hash function design, strategies based on linear and differential cryptanalysis.
PhD Thesis (1995)

References ii

- L. Grassi
  Bounded Surjective Quadratic Functions over $\mathbb{F}_p^n$ for MPC-/ZK-/FHE-Friendly Symmetric Primitives.
  IACR ePrint 2022
- L. Grassi, D. Khovratovich, S. Rønjom, M. Schofnegger
  The Legendre Symbol and the Modulo-2 Operator in Symmetric Schemes over $\mathbb{F}_p^n$ Preimage Attack on Full Grendel.
  FSE/ToSC 2021/2022

- L. Grassi, D. Khovratovich, A. Roy, C. Rechberger, M. Schofnegger
  Poseidon: A New Hash Function for Zero-Knowledge Proof Systems.
  USENIX 2021
- L. Grassi, R. Lüftenegger, C. Rechberger, D. Rotaru, M. Schofnegger
  On a Generalization of Substitution-Permutation Networks: The HADES Design Strategy.
  EUROCRYPT 2020

L. Grassi, S. Onofri, M. Pedicini, L. Sozzi
Invertible Quadratic Non-Linear Layers for MPC-/FHE-/ZK-Friendly Schemes over $\mathbb{F}_p^n$.
FSE/ToSC 2022/2023

L. Grassi, C. Rechberger, M. Schofnegger
Proving Resistance Against Infinitely Long Subspace Trails: How to Choose the Linear Layer.
FSE/ToSC 2021/2022