CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Bounded Surjective Quadratic Functions over $\mathbb{F}_p^n$ for MPC-/ZK-/FHE-Friendly Symmetric Primitives

ToSC 2024, March 2024

Lorenzo Grassi
Ruhr-Universität Bochum, Germany

RUHR UNIVERSITÄT BOCHUM RUB

Gefördert durch DFG Deutsche Forschungsgemeinschaft

HORST GÖRTZ INSTITUT

Motivation

- Motivated by new applications such as secure Multi-Party Computation (MPC), Fully Homomorphic Encryption (FHE), and Zero-Knowledge proofs (ZK), many MPC-/FHE-/ZK-friendly symmetric-key primitives that minimize the number of multiplications over $\mathbb{F}_p$ have been proposed;
- For security reasons, almost all of them are instantiated via invertible components, and permutations;
- However, *invertibility is* **not** *required in many of the applications just mentioned!* (E.g., hash functions for ZK, and PRF for MPC and FHE.)

Question: *can we reduce the multiplicative complexity of existing schemes by making use of* **non-invertible** *functions, without affecting the security?*

Motivation

- Motivated by new applications such as secure Multi-Party Computation (MPC), Fully Homomorphic Encryption (FHE), and Zero-Knowledge proofs (ZK), many MPC-/FHE-/ZK-friendly symmetric-key primitives that minimize the number of multiplications over $\mathbb{F}_p$ have been proposed;

- For security reasons, almost all of them are instantiated via invertible components, and permutations;

- However, *invertibility is* **not** *required in many of the applications just mentioned!* (E.g., hash functions for ZK, and PRF for MPC and FHE.)

Question: *can we reduce the multiplicative complexity of existing schemes by making use of* **non-invertible** *functions, without affecting the security?*

Motivation

- Motivated by new applications such as secure Multi-Party Computation (MPC), Fully Homomorphic Encryption (FHE), and Zero-Knowledge proofs (ZK), many MPC-/FHE-/ZK-friendly symmetric-key primitives that minimize the number of multiplications over $\mathbb{F}_p$ have been proposed;

- For security reasons, almost all of them are instantiated via invertible components, and permutations;

- However, *invertibility is* **not** *required in many of the applications just mentioned!* (E.g., hash functions for ZK, and PRF for MPC and FHE.)

Question: *can we reduce the multiplicative complexity of existing schemes by making use of* **non-invertible** *functions, without affecting the security?*

Motivation

- Motivated by new applications such as secure Multi-Party Computation (MPC), Fully Homomorphic Encryption (FHE), and Zero-Knowledge proofs (ZK), many MPC-/FHE-/ZK-friendly symmetric-key primitives that minimize the number of multiplications over $\mathbb{F}_p$ have been proposed;
- For security reasons, almost all of them are instantiated via invertible components, and permutations;
- However, *invertibility is* **not** *required in many of the applications just mentioned!* (E.g., hash functions for ZK, and PRF for MPC and FHE.)

Question: *can we reduce the multiplicative complexity of existing schemes by making use of* ***non-invertible*** *functions, without affecting the security?*

Table of Contents

Table of Contents

Preliminary: Bounded Surjective Functions

A function $\mathcal{F} : \mathrm{X} \to \mathrm{Y}$ is **surjective** if $\forall y \in \mathrm{Y}$, there exists $x \in \mathrm{X}$ such that $\mathcal{F}(x) = y$.

Definition 1

Let $l \geq 1$ be an integer. The function $\mathcal{F}$ is **l-bounded surjective** if for any element $y \in \mathrm{Y}$, there exist **at most** l distinct elements $\mathfrak{X} = \{x_0, x_1, \dots, x_{l-1}\} \subseteq \mathrm{X}$ such that

$$\mathcal{F}(x_0) = \mathcal{F}(x_1) = \dots \mathcal{F}(x_{l-1}) = y\,, \quad \text{and} \quad \forall z \notin \mathfrak{X} : \quad \mathcal{F}(z) \neq y\,.$$

- Let $\mathcal{F} : \mathrm{X} \to \mathrm{Y}$ be $l_{\mathcal{F}}$-bounded surjective, and let $\mathcal{G} : \mathrm{Y} \to \mathrm{Z}$ be $\lambda_{\mathcal{G}}$-bounded surjective. Then $\mathcal{G} \circ \mathcal{F} : \mathrm{X} \to \mathrm{Z}$ is (at most) $(l_{\mathcal{F}} \cdot \lambda_{\mathcal{G}})$-bounded surjective.
- Let $\mathcal{F} : \mathrm{X} \to \mathrm{X}$ be a l-bounded surjective function. The probability that a collision occurs at the output of $\mathcal{F}$ is *upper bounded* by $(l-1)/(|\mathrm{X}|-1)$.

Preliminary: Bounded Surjective Functions

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

A function $\mathcal{F} : \mathsf{X} \to \mathsf{Y}$ is **surjective** if $\forall y \in \mathsf{Y}$, there exists $x \in \mathsf{X}$ such that $\mathcal{F}(x) = y$.

Definition 1

Let $l \geq 1$ be an integer. The function $\mathcal{F}$ is l-**bounded surjective** if for any element $y \in \mathsf{Y}$, there exist **at most** l distinct elements $\mathfrak{X} = \{x_0, x_1, \ldots, x_{l-1}\} \subseteq \mathsf{X}$ such that

$$\mathcal{F}(x_0) = \mathcal{F}(x_1) = \ldots \mathcal{F}(x_{l-1}) = y\,, \quad \text{and} \quad \forall z \notin \mathfrak{X} : \quad \mathcal{F}(z) \neq y\,.$$

- Let $\mathcal{F} : \mathsf{X} \to \mathsf{Y}$ be $l_{\mathcal{F}}$-bounded surjective, and let $\mathcal{G} : \mathsf{Y} \to \mathsf{Z}$ be $\lambda_{\mathcal{G}}$-bounded surjective. Then $\mathcal{G} \circ \mathcal{F} : \mathsf{X} \to \mathsf{Z}$ is (at most) $(l_{\mathcal{F}} \cdot \lambda_{\mathcal{G}})$-bounded surjective.
- Let $\mathcal{F} : \mathsf{X} \to \mathsf{X}$ be a l-bounded surjective function. The probability that a collision occurs at the output of $\mathcal{F}$ is *upper bounded* by $(l-1)/(|\mathsf{X}|-1)$.

Preliminary: Bounded Surjective Functions

A function $\mathcal{F} : \mathrm{X} \to \mathrm{Y}$ is **surjective** if $\forall y \in \mathrm{Y}$, there exists $x \in \mathrm{X}$ such that $\mathcal{F}(x) = y$.

Definition 1

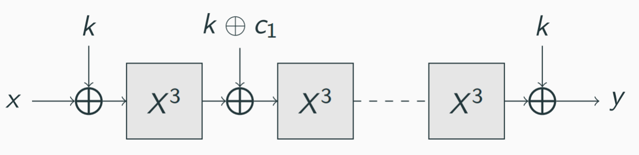
Let $l \geq 1$ be an integer. The function $\mathcal{F}$ is l-**bounded surjective** if for any element $y \in \mathrm{Y}$, there exist **at most** l distinct elements $\mathfrak{X} = \{x_0, x_1, \ldots, x_{l-1}\} \subseteq \mathrm{X}$ such that

$$\mathcal{F}(x_0) = \mathcal{F}(x_1) = \ldots \mathcal{F}(x_{l-1}) = y\,, \qquad \text{and} \quad \forall z \notin \mathfrak{X} : \quad \mathcal{F}(z) \neq y\,.$$

- Let $\mathcal{F} : \mathrm{X} \to \mathrm{Y}$ be $l_{\mathcal{F}}$-bounded surjective, and let $\mathcal{G} : \mathrm{Y} \to \mathrm{Z}$ be $\lambda_{\mathcal{G}}$-bounded surjective. Then $\mathcal{G} \circ \mathcal{F} : \mathrm{X} \to \mathrm{Z}$ is (at most) $(l_{\mathcal{F}} \cdot \lambda_{\mathcal{G}})$-bounded surjective.
- Let $\mathcal{F} : \mathrm{X} \to \mathrm{X}$ be a l-bounded surjective function. The probability that a collision occurs at the output of $\mathcal{F}$ is *upper bounded* by $(l-1)/(|\mathrm{X}|-1)$.

Table of Contents

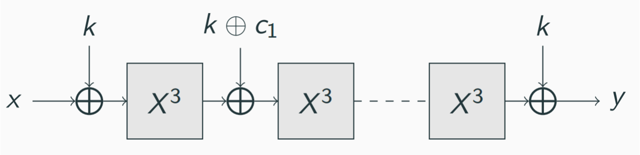
MiMC [AGR+16] (Asiacrypt'16)



- Instantiated via $x \mapsto x^d$, where $d \geq 3$ is the *smallest integer* s.t. $\gcd(d, p-1) = 1$;
- Security level $\kappa \approx \log_2(p)$ and data complexity $\leq 2^{\kappa/2} \approx \sqrt{p} \implies$ number of rounds $\approx \log_d(2^\kappa) = \kappa \cdot \log_d(2)$. E.g., 73 rounds for $d = 3$, $p \approx 2^{128}$ and $\kappa = 128$;
- Usually used in CTR-mode (due to very expensive decryption!):

$$(x, \mathrm{N}) \mapsto (x + \mathrm{MiMC}_k(\mathrm{N}), \mathrm{N}) \,.$$

MiMC [AGR+16] (Asiacrypt'16)



- Instantiated via $x \mapsto x^d$, where $d \geq 3$ is the *smallest integer* s.t. $\gcd(d, p-1) = 1$;
- Security level $\kappa \approx \log_2(p)$ and data complexity $\leq 2^{\kappa/2} \approx \sqrt{p} \implies$ number of rounds $\approx \log_d(2^\kappa) = \kappa \cdot \log_d(2)$. E.g., 73 rounds for $d = 3$, $p \approx 2^{128}$ and $\kappa = 128$;
- Usually used in CTR-mode (due to very expensive decryption!):

$$(x, \mathrm{N}) \mapsto (x + \mathrm{MiMC}_k(\mathrm{N}), \mathrm{N}) \, .$$

From MiMC to `MiMC++`

- Independently of p, the function $x \mapsto x^2$ is 2-bounded surjective;
- The PRF `MiMC++` over $\mathbb{F}_p$ corresponds to MiMC instantiated with $x \mapsto x^2$ (instead of $x \mapsto x^d$);
- Let κ be the security level (in bits). Assuming

$$p > 2^{3 \cdot \kappa}.$$

and data complexity $\leq 2^{\kappa/2}$, then number of rounds given by

$$3 + \lceil \kappa - 2 \cdot \log_2(\kappa) \rceil .$$

E.g., 117 rounds for $p \approx 2^{384}$ and $\kappa = 128$.

From MiMC to MiMC++

- Independently of p, the function $x \mapsto x^2$ is 2-bounded surjective;
- The PRF MiMC++ over $\mathbb{F}_p$ corresponds to MiMC instantiated with $x \mapsto x^2$ (instead of $x \mapsto x^d$);
- Let κ be the security level (in bits). Assuming

$$p > 2^{3\cdot\kappa}.$$

and data complexity $\leq 2^{\kappa/2}$, then number of rounds given by

$$3 + \lceil \kappa - 2 \cdot \log_2(\kappa) \rceil \ .$$

E.g., 117 rounds for $p \approx 2^{384}$ and $\kappa = 128$.

Security Analysis of `MiMC++` (1/2)

- *Security analysis analogous to the one of MiMC*: GCD is the most powerful attack;

Main Differences due to the non-invertibility:

1. About *collisions*: since R-round `MiMC++` is $\leq 2^R$-bounded surjective, the probability that a collision occurs is

$$\leq \frac{2^R - 1}{p - 1} \approx \frac{2^{3+\lceil \kappa - 2\cdot\log_2(\kappa)\rceil}}{2^{3\kappa}} \approx 2^{-2\cdot\kappa}.$$

Since $\leq 2^{\kappa/2}$ texts are available for the attack, observing a collision is unrealistic.

Security Analysis of MiMC++ (1/2)

- *Security analysis analogous to the one of MiMC*: GCD is the most powerful attack;

Main Differences due to the non-invertibility:

1. About *collisions*: since R-round MiMC++ is $\leq 2^R$-bounded surjective, the probability that a collision occurs is

$$\leq \frac{2^R - 1}{p-1} \approx \frac{2^{3+\lceil \kappa - 2\cdot \log_2(\kappa) \rceil}}{2^{3\kappa}} \approx 2^{-2\cdot\kappa}\,.$$

Since $\leq 2^{\kappa/2}$ texts are available for the attack, observing a collision is unrealistic.

Security Analysis of `MiMC++` (2/2)

2. Polynomial representation of `MiMC++`:

- forward direction: over R rounds, it is dense (as in MiMC) and has degree $\leq 2^R$;
- backward direction: $x \mapsto x^2$ is not invertible, but local inverses exist. E.g., if $p = 3 \mod 4$, the inverses of $x \mapsto x^2$ are $x \mapsto \pm x^{\frac{p+1}{4}}$. Still:
  1. such local inverses have usually high degree (as in the case of MiMC);
  2. it is difficult to *efficiently* combine/set up local inverses over multiple rounds (*open problem for future work*).

We conjecture that few rounds are sufficient to prevent algebraic attacks in the backward direction.

Security Analysis of `MiMC++` (2/2)

2. Polynomial representation of `MiMC++`:

- forward direction: over R rounds, it is dense (as in MiMC) and has degree $\leq 2^R$;
- backward direction: $x \mapsto x^2$ is not invertible, but local inverses exist. E.g., if $p = 3 \mod 4$, the inverses of $x \mapsto x^2$ are $x \mapsto \pm x^{\frac{p+1}{4}}$. Still:
  1. such local inverses have usually high degree (as in the case of MiMC);
  2. it is difficult to *efficiently* combine/set up local inverses over multiple rounds (*open problem for future work*).

We conjecture that few rounds are sufficient to prevent algebraic attacks in the backward direction.

Security Analysis of `MiMC++` (2/2)

2. Polynomial representation of `MiMC++`:

- forward direction: over R rounds, it is dense (as in MiMC) and has degree $\leq 2^R$;
- backward direction: $x \mapsto x^2$ is not invertible, but local inverses exist. E.g., if $p = 3 \mod 4$, the inverses of $x \mapsto x^2$ are $x \mapsto \pm x^{\frac{p+1}{4}}$. Still:
    1. such local inverses have usually high degree (as in the case of MiMC);
    2. it is difficult to *efficiently* combine/set up local inverses over multiple rounds (*open problem for future work*).

We conjecture that few rounds are sufficient to prevent algebraic attacks in the backward direction.

Multiplicative Complexity (MPC): MiMC versus `MiMC++`

Multiplicative Complexity of MiMC and `MiMC++` in the case of MPC applications:

PRF	$(\log_2 p,\ \kappa)$	# Rounds	# Multiplications
`MiMC++`	(**384**, 128)	117	117
MiMC ($d = 3$)	(128, 128)	73	146 (+**24.8**%)
MiMC ($d = 5$)	(128, 128)	51	153 (+**30.8**%)
MiMC ($d = 7$)	(128, 128)	42	168 (+**43.6**%)

(See the paper for a more detailed comparison!)

(**Remark:** *The size of p does* **not** *impact the performance of the MPC application*)

Table of Contents

First Observation

Working over $\mathbb{F}_p^n$, the non-linear layer

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

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 collisions are of the form*

$$[x_0^2, x_1^2, \dots, x_{n-1}^2] = [y_0^2, y_1^2, \dots, y_{n-1}^2] \qquad \Longleftrightarrow \qquad x_i = \pm y_i \, .$$

Starting Point: SI-Lifting Functions $\mathcal{S}_F$

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

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

Theorem 2 ([GOPS22])

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

- *if $m = 2$, then $\mathcal{S}_F$ is* **never** *invertible for each $n \geq 3$;*
- *if $m = 3$, then $\mathcal{S}_F$ is* **never** *invertible for each $n \geq 5$.*

Starting Point: SI-Lifting Functions $\mathcal{S}_F$

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

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

Theorem 2 ([GOPS22])

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

- *if $m = 2$, then $\mathcal{S}_F$ is* **never** *invertible for each $n \geq 3$;*
- *if $m = 3$, then $\mathcal{S}_F$ is* **never** *invertible for each $n \geq 5$.*

Goal and Main Result

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

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

- a (non-trivial) collision $\mathcal{S}_F(x_0, x_1, \ldots, x_{n-1}) = \mathcal{S}_F(y_0, y_1, \ldots, y_{n-1})$ implies $x_i \neq y_i$ for **all** $i \in \{0, 1, 2, \ldots, n-1\}$;
- the corresponding *function $\mathcal{S}_F$ is 2^n-bounded surjective.*

Goal and Main Result

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 $\mathcal{S}_F$.

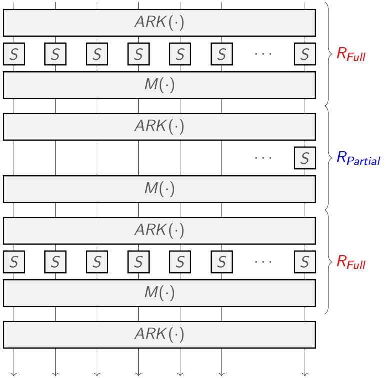
Such function is $F(x_0, x_1) = x_1^2 + x_0$ (or similar) for which

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

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

- a (non-trivial) collision $\mathcal{S}_F(x_0, x_1, \ldots, x_{n-1}) = \mathcal{S}_F(y_0, y_1, \ldots, y_{n-1})$ implies $x_i \neq y_i$ for **all** $i \in \{0, 1, 2, \ldots, n-1\}$;
- the corresponding *function* $\mathcal{S}_F$ *is* 2^n*-bounded surjective*.

Table of Contents



- $S(x) = x^d$ where $\gcd(d, p-1) = 1$;
- Linear layer: multiplication with MDS matrix $\in \mathbb{F}_p^{n \times n}$ (for which **no** arbitrary long subspace trail in internal rounds exists);
- Number of rounds ($\kappa \approx \log_2(p)$):

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

- Used in CTR mode.

From HadesMiMC to Pluto (1/2)

- *Multiplicative cost* of each external/full round:

$$(\lfloor \log_2(d) \rfloor + \text{hw}(d) - 1) \cdot n \geq \mathbf{2} \cdot \mathbf{n} \, ;$$

- External/Full Rounds crucial for
  - "masking" the internal rounds;
  - simple security argument against statistical attacks (e.g., via wide-trail design strategy);

- **Idea**: replace

$$(x_0, x_1, \ldots, x_{n-1}) \mapsto (x_0^d, x_1^d, \ldots, x_{n-1}^d)$$

with

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

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

From HadesMiMC to Pluto (1/2)

- *Multiplicative cost* of each external/full round:

$$(\lfloor \log_2(d) \rfloor + \mathrm{hw}(d) - 1) \cdot n \geq \mathbf{2} \cdot \mathbf{n}\,;$$

- External/Full Rounds crucial for
  - "masking" the internal rounds;
  - simple security argument against statistical attacks (e.g., via wide-trail design strategy);

- **Idea**: replace

$$(x_0, x_1, \ldots, x_{n-1}) \mapsto (x_0^d, x_1^d, \ldots, x_{n-1}^d)$$

with

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

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

From HadesMiMC to PLUTO (2/2)

- Internal rounds instantiated with the degree-4 Lai-Massey scheme proposed for HYDRA [GØS+22] (besides linear layer for destroying invariant subspace trails);

- *Security analogous to the one proposed for HadesMiMC*. Main differences:
  - Collision probability at the output of PLUTO (assuming invertible internal rounds):

$$\leq \frac{2^{8\cdot n}-1}{p^n-1} \approx \left(\frac{2^8}{p}\right)^n \leq 2^{-2\cdot\kappa} \qquad \text{(assuming } \kappa \leq \frac{n}{2}\cdot(\log_2(p)-8)\text{)};$$

  - The external rounds are not invertible, and only local inverses can be set up (similarly to `MiMC++`): *we conjecture that* $4+4=8$ *external rounds are sufficient to frustrate algebraic attacks in the backward direction.*

From HadesMiMC to PLUTO (2/2)

- Internal rounds instantiated with the degree-4 Lai-Massey scheme proposed for HYDRA [GØS+22] (besides linear layer for destroying invariant subspace trails);
- *Security analogous to the one proposed for HadesMiMC*. Main differences:
  - Collision probability at the output of PLUTO (assuming invertible internal rounds):

$$\leq \frac{2^{8\cdot n}-1}{p^n-1} \approx \left(\frac{2^8}{p}\right)^n \leq 2^{-2\cdot\kappa} \qquad \text{(assuming } \kappa \leq \frac{n}{2}\cdot(\log_2(p)-8)\text{)};$$

  - The external rounds are not invertible, and only local inverses can be set up (similarly to `MiMC++`): *we conjecture that* $4+4=8$ *external rounds are sufficient to frustrate 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 $n \in \{4, 8, 12, 16\}$:

	n	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 and Open Problems

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

- We showed that the multiplicative complexity of several MPC-/FHE-/ZK-friendly schemes can be improved by making use of non-invertible non-linear layers;
- Several **open problems**: understand in a better way how to exploit the *local inverses* to set up MitM algebraic attacks!
- 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 (e.g., a secret key)!

Summary and Open Problems

- We showed that the multiplicative complexity of several MPC-/FHE-/ZK-friendly schemes can be improved by making use of non-invertible non-linear layers;

- Several **open problems**: understand in a better way how to exploit the *local inverses* to set up MitM algebraic attacks!

- 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 (e.g., a secret key)!

Thanks for your attention!

Questions?

Comments?

About Number of Collisions of $\mathcal{S}_F$ via $F(x_0, x_1) = x_1^2 + x_0$

The collision $\mathcal{S}_F(x_0, x_1, \ldots, x_{n-1}) = \mathcal{S}_F(x'_0, x'_1, \ldots, x'_{n-1})$ corresponds to

$$\begin{bmatrix} 0 & d_1 & 0 & \ldots & 0 \\ 0 & 0 & d_2 & \ldots & 0 \\ \vdots & & & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & d_{n-1} \\ d_0 & 0 & 0 & \ldots & 0 \end{bmatrix} \times \begin{bmatrix} s_0 \\ s_1 \\ \ldots \\ s_{n-2} \\ s_{n-1} \end{bmatrix} = - \begin{bmatrix} d_0 \\ d_1 \\ \ldots \\ d_{n-2} \\ d_{n-1} \end{bmatrix}$$

where $d_i := x_i - x'_i$ and $s_i := x_i + x'_i$ for each i.

Hence, a collision exists *only* for $(d_0, d_1, \ldots, d_{n-1}) \in \mathbb{F}_p^n$ such that

$$\forall i \in \{0, 1, \ldots, n-1\} : \qquad d_i \neq 0 \,,$$

that is, $(p-1)^n$ values.

About Number of Collisions of $\mathcal{S}_F$ via $F(x_0, x_1) = x_1^2 + x_0$

The collision $\mathcal{S}_F(x_0, x_1, \ldots, x_{n-1}) = \mathcal{S}_F(x_0', x_1', \ldots, x_{n-1}')$ corresponds to

$$\begin{bmatrix} 0 & d_1 & 0 & \ldots & 0 \\ 0 & 0 & d_2 & \ldots & 0 \\ \vdots & & & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & d_{n-1} \\ d_0 & 0 & 0 & \ldots & 0 \end{bmatrix} \times \begin{bmatrix} s_0 \\ s_1 \\ \ldots \\ s_{n-2} \\ s_{n-1} \end{bmatrix} = - \begin{bmatrix} d_0 \\ d_1 \\ \ldots \\ d_{n-2} \\ d_{n-1} \end{bmatrix}$$

where $d_i := x_i - x_i'$ and $s_i := x_i + x_i'$ for each i.

Hence, a collision exists *only* for $(d_0, d_1, \ldots, d_{n-1}) \in \mathbb{F}_p^n$ such that

$$\forall i \in \{0, 1, \ldots, n-1\} : \qquad d_i \neq 0 \,,$$

that is, $(p-1)^n$ values.

About 2^n-Bounded Surjective of $\mathcal{S}_F$ via $F(x_0, x_1) = x_1^2 + x_0$

Goal: each output y of $\mathcal{S}_F$ over $\mathbb{F}_p^n$ admits at most 2^n pre-images.

- Given $y_i = x_{i+1}^2 + x_i$, then $x_i = G_{y_i}(x_{i+1}) := y_i - x_{i+1}^2$, where G_y *quadratic*;
- Working iteratively:

$$\begin{aligned} x_0 = G_{y_0}(x_1) = G_{y_0} \circ G_{y_1}(x_2) = \ldots = G_{y_0} \circ G_{y_1} \circ \ldots \circ G_{y_{n-1}}(x_0) \\ \Longrightarrow \qquad G_{y_0} \circ G_{y_1} \circ \ldots \circ G_{y_{n-1}}(x_0) - x_0 = 0 \end{aligned}$$

  where $\deg(G_{y_0} \circ G_{y_1} \circ \ldots \circ G_{y_{n-1}}) = 2^n$;
- The previous equation admits at most 2^n solutions in x_0. For each x_0, it is possible to find the other variables via $x_i = G_{y_i}(x_{i+1})$.

About 2^n-Bounded Surjective of $\mathcal{S}_F$ via $F(x_0, x_1) = x_1^2 + x_0$

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Goal: each output y of $\mathcal{S}_F$ over $\mathbb{F}_p^n$ admits at most 2^n pre-images.

- Given $y_i = x_{i+1}^2 + x_i$, then $x_i = G_{y_i}(x_{i+1}) := y_i - x_{i+1}^2$, where G_y *quadratic*;
- Working iteratively:

$$\begin{aligned} x_0 = G_{y_0}(x_1) = G_{y_0} \circ G_{y_1}(x_2) = \ldots = G_{y_0} \circ G_{y_1} \circ \ldots \circ G_{y_{n-1}}(x_0) \\ \Longrightarrow \qquad G_{y_0} \circ G_{y_1} \circ \ldots \circ G_{y_{n-1}}(x_0) - x_0 = 0 \end{aligned}$$

  where $\deg(G_{y_0} \circ G_{y_1} \circ \ldots \circ G_{y_{n-1}}) = 2^n$;
- The previous equation admits at most 2^n solutions in x_0. For each x_0, it is possible to find the other variables via $x_i = G_{y_i}(x_{i+1})$.

About 2^n-Bounded Surjective of $\mathcal{S}_F$ via $F(x_0, x_1) = x_1^2 + x_0$

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Goal: each output y of $\mathcal{S}_F$ over $\mathbb{F}_p^n$ admits at most 2^n pre-images.

- Given $y_i = x_{i+1}^2 + x_i$, then $x_i = G_{y_i}(x_{i+1}) := y_i - x_{i+1}^2$, where G_y *quadratic*;
- Working iteratively:

$$x_0 = G_{y_0}(x_1) = G_{y_0} \circ G_{y_1}(x_2) = \ldots = G_{y_0} \circ G_{y_1} \circ \ldots \circ G_{y_{n-1}}(x_0)$$
$$\Longrightarrow \qquad G_{y_0} \circ G_{y_1} \circ \ldots \circ G_{y_{n-1}}(x_0) - x_0 = 0$$

where $\deg(G_{y_0} \circ G_{y_1} \circ \ldots \circ G_{y_{n-1}}) = 2^n$;

- The previous equation admits at most 2^n solutions in x_0. For each x_0, it is possible to find the other variables via $x_i = G_{y_i}(x_{i+1})$.

About 2^n-Bounded Surjective of $\mathcal{S}_F$ via $F(x_0, x_1) = x_1^2 + x_0$

Goal: each output y of $\mathcal{S}_F$ over $\mathbb{F}_p^n$ admits at most 2^n pre-images.

- Given $y_i = x_{i+1}^2 + x_i$, then $x_i = G_{y_i}(x_{i+1}) := y_i - x_{i+1}^2$, where G_y *quadratic*;
- Working iteratively:

$$\begin{aligned} x_0 = G_{y_0}(x_1) = G_{y_0} \circ G_{y_1}(x_2) = \ldots = G_{y_0} \circ G_{y_1} \circ \ldots \circ G_{y_{n-1}}(x_0) \\ \Longrightarrow \qquad G_{y_0} \circ G_{y_1} \circ \ldots \circ G_{y_{n-1}}(x_0) - x_0 = 0 \end{aligned}$$

  where $\deg(G_{y_0} \circ G_{y_1} \circ \ldots \circ G_{y_{n-1}}) = 2^n$;
- The previous equation admits at most 2^n solutions in x_0. For each x_0, it is possible to find the other variables via $x_i = G_{y_i}(x_{i+1})$.

From HadesMiMC to Pluto: Internal Rounds

- Internal rounds instantiated with the same degree-4 Lai-Massey scheme used in Hydra [GØS+22] (besides linear layer for destroying invariant subspace trails):

$$(x_0, x_1, \ldots, x_{n-1}) \mapsto (x_0 + z, x_1 + z, \ldots, x_{n-1} + z)$$

where

$$z := \Big(\big(\sum_i \gamma_i^{(0)} \cdot x_i\big)^2 + \sum_i \gamma_i^{(1)} \cdot x_i\Big)^2$$

such that $[\gamma_0^{(0)}, \gamma_1^{(0)}, \ldots, \gamma_{n-1}^{(0)}]$ and $[\gamma_0^{(1)}, \gamma_1^{(1)}, \ldots, \gamma_{n-1}^{(1)}]$ are linearly independent;

- Cost of each internal round: 2 multiplications *independently of p*.

References I

- M.R. Albrecht, L. Grassi, C. Rechberger, A. Roy and T. Tiessen
  MiMC: Efficient Encryption and Cryptographic Hashing with Minimal Multiplicative Complexity.
  ASIACRYPT 2016
- L. Grassi, D. Khovratovich, A. Roy, C. Rechberger and M. Schofnegger
  Poseidon: A New Hash Function for Zero-Knowledge Proof Systems.
  USENIX 2021
- L. Grassi, R. Lüftenegger, C. Rechberger, D. Rotaru and M. Schofnegger
  On a Generalization of Substitution-Permutation Networks: The HADES Design Strategy.
  EUROCRYPT 2020

References II

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

L. Grassi, M. Øygarden, M. Schofnegger and R. Walch
From Farfalle to Megafono via Ciminion: The PRF Hydra for MPC Applications.
EUROCRYPT 2022