Invertible Quadratic Non-Linear Functions over $\mathbb{F}_p^n$ via Multiple Local Maps

Young Researchers Algebra Conference 2023

Ginevra Giordani, Lorenzo Grassi, Silvia Onofri and Marco Pedicini

July 26th, 2023

INdAM Istituto Nazionale di Alta Matematica GNSAGA
Università degli Studi di Napoli Federico II
Dipartimento di Matematica e Applicazioni "Renato Caccioppoli"
UNIVERSITÀ DEGLI STUDI DELL'AQUILA
DISIM Dipartimento di Ingegneria e Scienze dell'Informazione e Matematica

Low-Multiplicative Non-Linear Invertible Functions

A low-multiplicative non-linear function is a function that requires a small number of non-linear operations (multiplications).
These functions over prime fields $\mathbb{F}_p$ for $p \geq 3$ prime are very relevant for symmetric encryption schemes like

- Multi Party Computation (MPC);
- Zero-Knowledge proofs (ZK);
- Fully Homomorphic Encryption (FHE).

Motivation

Low-Multiplicative Non-Linear Invertible Functions

A low-multiplicative non-linear function is a function that requires a small number of non-linear operations (multiplications).

These functions over prime fields $\mathbb{F}_p$ for $p \geq 3$ prime are very relevant for symmetric encryption schemes like

- Multi Party Computation (MPC);
- Zero-Knowledge proofs (ZK);
- Fully Homomorphic Encryption (FHE).

Low-Multiplicative Non-Linear Invertible Functions

A low-multiplicative non-linear function is a function that requires a small number of non-linear operations (multiplications).
These functions over prime fields $\mathbb{F}_p$ for $p \geq 3$ prime are very relevant for symmetric encryption schemes like

- Multi Party Computation (MPC);
- Zero-Knowledge proofs (ZK);
- Fully Homomorphic Encryption (FHE).

Low-Multiplicative Non-Linear Invertible Functions

A low-multiplicative non-linear function is a function that requires a small number of non-linear operations (multiplications).
These functions over prime fields $\mathbb{F}_p$ for $p \geq 3$ prime are very relevant for symmetric encryption schemes like

- Multi Party Computation (MPC);
- Zero-Knowledge proofs (ZK);
- Fully Homomorphic Encryption (FHE).

Motivation

Low-Multiplicative Non-Linear Invertible Functions

A low-multiplicative non-linear function is a function that requires a small number of non-linear operations (multiplications).
These functions over prime fields $\mathbb{F}_p$ for $p \geq 3$ prime are very relevant for symmetric encryption schemes like

- Multi Party Computation (MPC);
- Zero-Knowledge proofs (ZK);
- Fully Homomorphic Encryption (FHE).

Motivation

Low-Multiplicative Non-Linear Invertible Functions

A low-multiplicative non-linear function is a function that requires a small number of non-linear operations (multiplications).
These functions over prime fields $\mathbb{F}_p$ for $p \geq 3$ prime are very relevant for symmetric encryption schemes like

- Multi Party Computation (MPC);
- Zero-Knowledge proofs (ZK);
- Fully Homomorphic Encryption (FHE).

Motivation

These MPC-/FHE-/ZK-friendly symmetric primitives are characterized by the following:

- they are usually defined over prime fields $\mathbb{F}_p^t$ for a huge prime $p \approx 2^{128}$ or more;
- they can be described via a simple algebraic expression over their natural field.

Goal: find invertible quadratic low-multiplicative functions over $\mathbb{F}_p^n$ for $p \geq 3$.

Motivation

These MPC-/FHE-/ZK-friendly symmetric primitives are characterized by the following:

- they are usually defined over prime fields $\mathbb{F}_p^t$ for a huge prime $p \approx 2^{128}$ or more;
- they can be described via a simple algebraic expression over their natural field.

Goal: find invertible quadratic low-multiplicative functions over $\mathbb{F}_p^n$ for $p \geq 3$.

Motivation

These MPC-/FHE-/ZK-friendly symmetric primitives are characterized by the following:

- they are usually defined over prime fields $\mathbb{F}_p^t$ for a huge prime $p \approx 2^{128}$ or more;
- they can be described via a simple algebraic expression over their natural field.

Goal: find invertible quadratic low-multiplicative functions over $\mathbb{F}_p^n$ for $p \geq 3$.

Motivation

These MPC-/FHE-/ZK-friendly symmetric primitives are characterized by the following:

- they are usually defined over prime fields $\mathbb{F}_p^t$ for a huge prime $p \approx 2^{128}$ or more;
- they can be described via a simple algebraic expression over their natural field.

Goal: find invertible quadratic low-multiplicative functions over $\mathbb{F}_p^n$ for $p \geq 3$.

Motivation

These MPC-/FHE-/ZK-friendly symmetric primitives are characterized by the following:

- they are usually defined over prime fields $\mathbb{F}_p^t$ for a huge prime $p \approx 2^{128}$ or more;
- they can be described via a simple algebraic expression over their natural field.

Goal: find invertible quadratic low-multiplicative functions over $\mathbb{F}_p^n$ for $p \geq 3$.

Low-Multiplicative Non-Linear Functions

Some examples of this kind of functions over prime fields are known, but their efficiency for the schemes mentioned before is not clear.
Another approach is inspired from

Daemen, J
Cipher and Hash Function Design, Strategies Based on Linear and Differential Cryptanalysis
PhD Thesis. K.U.Leuven (1995), http//jda.noekeon.org/.

where are introduced *shift-invariant* functions, i.e.,

Definition [Shift-Invariant Map]

A map S is called **shift-invariant** if

$$S \circ \Pi = \Pi \circ S$$

for every Π shifting of the arguments.

Low-Multiplicative Non-Linear Functions

Some examples of this kind of functions over prime fields are known, but their efficiency for the schemes mentioned before is not clear.

Another approach is inspired from

Daemen, J
Cipher and Hash Function Design, Strategies Based on Linear and Differential Cryptanalysis
PhD Thesis. K.U.Leuven (1995), http//jda.noekeon.org/.

where are introduced *shift-invariant* functions, i.e.,

Definition [Shift-Invariant Map]

A map S is called **shift-invariant** if

$$S \circ \Pi = \Pi \circ S$$

for every Π shifting of the arguments.

Low-Multiplicative Non-Linear Functions

Some examples of this kind of functions over prime fields are known, but their efficiency for the schemes mentioned before is not clear.
Another approach is inspired from

Daemen, J
Cipher and Hash Function Design, Strategies Based on Linear and Differential Cryptanalysis
PhD Thesis. K.U.Leuven (1995), http//jda.noekeon.org/.

where are introduced *shift-invariant* functions, i.e.,

Definition [Shift-Invariant Map]

A map $\mathcal{S}$ is called **shift-invariant** if

$$\mathcal{S} \circ \Pi = \Pi \circ \mathcal{S}$$

for every Π shifting of the arguments.

Low-Multiplicative Non-Linear Functions

Some examples of this kind of functions over prime fields are known, but their efficiency for the schemes mentioned before is not clear.
Another approach is inspired from

Daemen, J
Cipher and Hash Function Design, Strategies Based on Linear and Differential Cryptanalysis
PhD Thesis. K.U.Leuven (1995), http//jda.noekeon.org/.

where are introduced *shift-invariant* functions, i.e.,

Definition [Shift-Invariant Map]

A map $\mathcal{S}$ is called **shift-invariant** if

$$\mathcal{S} \circ \Pi = \Pi \circ \mathcal{S}$$

for every Π shifting of the arguments.

Low-Multiplicative Non-Linear Functions

Some examples of this kind of functions over prime fields are known, but their efficiency for the schemes mentioned before is not clear.
Another approach is inspired from

Daemen, J
Cipher and Hash Function Design, Strategies Based on Linear and Differential Cryptanalysis
PhD Thesis. K.U.Leuven (1995), http//jda.noekeon.org/.

where are introduced *shift-invariant* functions, i.e.,

Definition [Shift-Invariant Map]

A map $\mathcal{S}$ is called **shift-invariant** if

$$\mathcal{S} \circ \Pi = \Pi \circ \mathcal{S}$$

for every Π shifting of the arguments.

Low-Multiplicative Non-Linear Functions

Some examples of this kind of functions over prime fields are known, but their efficiency for the schemes mentioned before is not clear.
Another approach is inspired from

Daemen, J
Cipher and Hash Function Design, Strategies Based on Linear and Differential Cryptanalysis
PhD Thesis. K.U.Leuven (1995), http//jda.noekeon.org/.

where are introduced *shift-invariant* functions, i.e.,

Definition [Shift-Invariant Map]

A map $\mathcal{S}$ is called **shift-invariant** if

$$\mathcal{S} \circ \Pi = \Pi \circ \mathcal{S}$$

for every Π shifting of the arguments.

Shift-Invariant Liftings

In

L. Grassi, S. Onofri, M. Pedicini, L. Sozzi
Invertible Quadratic Non-Linear Layers for MPC-/FHE-/ZK-Friendly Schemes over $\mathbb{F}_p^n$ - Application to Poseidon
IACR Trans. Symmetric Cryptol. 2022(3), 20-72 (2022).

the authors studied the invertibility of *shift-invariant lifting functions*

Definition [Shift-Invariant lifting]

Let $p \geq 3$ be a prime integer, and let $1 \leq m \leq n$. Let $F : \mathbb{F}_p^m \to \mathbb{F}_p$ be a local map. The *shift-invariant lifting* (SI–lifting) function $\mathcal{S}_F$ over $\mathbb{F}_p^n$ induced by the local map F is defined as

$$\mathcal{S}_F(x_0, \ldots, x_{n-1}) = y_0 \| y_1 \| \ldots \| y_{n-1} \quad \text{such that} \quad y_i = F(x_i, \ldots, x_{i+m-1})$$

where indices i of x_i are taken modulo n.

where $\mathcal{S}_F$ is induced over $\mathbb{F}_p^n$ by a *quadratic* local map.

Related Works

Shift-Invariant Liftings

In

L. Grassi, S. Onofri, M. Pedicini, L. Sozzi
Invertible Quadratic Non-Linear Layers for MPC-/FHE-/ZK-Friendly Schemes over $\mathbb{F}_p^n$ - Application to Poseidon
IACR Trans. Symmetric Cryptol. 2022(3), 20-72 (2022).

the authors studied the invertibility of *shift-invariant lifting functions*

Definition [Shift-Invariant lifting]

Let $p \geq 3$ be a prime integer, and let $1 \leq m \leq n$. Let $F : \mathbb{F}_p^m \to \mathbb{F}_p$ be a local map. The *shift-invariant lifting* (SI–lifting) function $\mathcal{S}_F$ over $\mathbb{F}_p^n$ induced by the local map F is defined as

$$\mathcal{S}_F(x_0, \ldots, x_{n-1}) = y_0 \| y_1 \| \ldots \| y_{n-1} \quad \text{such that} \quad y_i = F(x_i, \ldots, x_{i+m-1})$$

where indices i of x_i are taken modulo n.

where $\mathcal{S}_F$ is induced over $\mathbb{F}_p^n$ by a *quadratic* local map.

Related Works

Shift-Invariant Liftings

In

L. Grassi, S. Onofri, M. Pedicini, L. Sozzi
Invertible Quadratic Non-Linear Layers for MPC-/FHE-/ZK-Friendly Schemes over $\mathbb{F}_p^n$ - Application to Poseidon
IACR Trans. Symmetric Cryptol. 2022(3), 20-72 (2022).

the authors studied the invertibility of *shift-invariant lifting functions*

Definition [Shift-Invariant lifting]

Let $p \geq 3$ be a prime integer, and let $1 \leq m \leq n$. Let $F : \mathbb{F}_p^m \to \mathbb{F}_p$ be a local map. The *shift-invariant lifting* (SI–lifting) function $\mathcal{S}_F$ over $\mathbb{F}_p^n$ induced by the local map F is defined as

$$\mathcal{S}_F(x_0, \ldots, x_{n-1}) = y_0 \| y_1 \| \ldots \| y_{n-1} \quad \text{such that} \quad y_i = F(x_i, \ldots, x_{i+m-1})$$

where indices i of x_i are taken modulo n.

where $\mathcal{S}_F$ is induced over $\mathbb{F}_p^n$ by a *quadratic* local map.

Shift-Invariant Liftings

In

L. Grassi, S. Onofri, M. Pedicini, L. Sozzi
Invertible Quadratic Non-Linear Layers for MPC-/FHE-/ZK-Friendly Schemes over $\mathbb{F}_p^n$ - Application to Poseidon
IACR Trans. Symmetric Cryptol. 2022(3), 20-72 (2022).

the authors studied the invertibility of *shift-invariant lifting functions*

Definition [Shift-Invariant lifting]

Let $p \geq 3$ be a prime integer, and let $1 \leq m \leq n$. Let $F : \mathbb{F}_p^m \to \mathbb{F}_p$ be a local map. The *shift-invariant lifting* (SI–lifting) function $\mathcal{S}_F$ over $\mathbb{F}_p^n$ induced by the local map F is defined as

$$\mathcal{S}_F(x_0, \ldots, x_{n-1}) = y_0 \| y_1 \| \ldots \| y_{n-1} \quad \text{such that} \quad y_i = F(x_i, \ldots, x_{i+m-1})$$

where indices i of x_i are taken modulo n.

where $\mathcal{S}_F$ is induced over $\mathbb{F}_p^n$ by a *quadratic* local map.

Related Works

Their result is

Theorem [Th 2-3]

Let $p \geq 3$ be a prime integer, and let $1 \leq m \leq n$. Given $F : \mathbb{F}_p^m \to \mathbb{F}_p$ a quadratic local map, then the SI–lifting function $\mathcal{S}_F$ induced by F over $\mathbb{F}_p^n$ is not invertible neither if $m = 2$ and $n \geq 3$ nor if $m = 3$ and $n \geq 5$.

Related Works

Their result is

Theorem [Th 2-3]

Let $p \geq 3$ be a prime integer, and let $1 \leq m \leq n$. Given $F : \mathbb{F}_p^m \to \mathbb{F}_p$ a quadratic local map, then the SI–lifting function $\mathcal{S}_F$ induced by F over $\mathbb{F}_p^n$ is not invertible neither if $m = 2$ and $n \geq 3$ nor if $m = 3$ and $n \geq 5$.

Their result is

Theorem [Th 2-3]

Let $p \geq 3$ be a prime integer, and let $1 \leq m \leq n$. Given $F : \mathbb{F}_p^m \to \mathbb{F}_p$ a quadratic local map, then the SI–lifting function $\mathcal{S}_F$ induced by F over $\mathbb{F}_p^n$ is not invertible neither if $m = 2$ and $n \geq 3$ nor if $m = 3$ and $n \geq 5$.

Multiple Local Maps

We analyzed the possibility to set up invertible quadratic functions over $\mathbb{F}_p^n$ via shift-invariant functions induced by multiple local maps.

The general scheme is

Definition[Cyclic (Alternating) Shift-Invariant Lifting]

Let $p \geq 3$ be a prime integer and let $1 \leq m, h \leq n$. For each $i \in \{0, 1, \ldots, h-1\}$, let $F_i : \mathbb{F}_p^m \to \mathbb{F}_p$ be a local map. The *cyclic (or alternating) shift-invariant lifting* (CSI-lifting or ASI-lifting) function $\mathcal{S}_{F_0, F_1, \ldots, F_{h-1}}$ induced by the family of local maps $(F_0, \ldots, F_{h-1})$ over $\mathbb{F}_p^n$ is defined as

$$\mathcal{S}(x_0, x_1, \ldots, x_{n-1}) = y_0 \| y_1 \| \ldots \| y_{n-1} \qquad \text{where}$$
$$y_i := F_{i \bmod h}(x_i, x_{i+1}, \ldots, x_{i+m-1})$$

for each $i \in \{0, 1, \ldots, n-1\}$, where the sub-indices are taken modulo n.

Our Contribution

Multiple Local Maps

We analyzed the possibility to set up invertible quadratic functions over $\mathbb{F}_p^n$ via shift-invariant functions induced by multiple local maps.
The general scheme is

Definition[Cyclic (Alternating) Shift-Invariant Lifting]

Let $p \geq 3$ be a prime integer and let $1 \leq m, h \leq n$. For each $i \in \{0, 1, \ldots, h-1\}$, let $F_i : \mathbb{F}_p^m \to \mathbb{F}_p$ be a local map. The *cyclic (or alternating) shift-invariant lifting* (CSI-lifting or ASI-lifting) function $\mathcal{S}_{F_0, F_1, \ldots, F_{h-1}}$ induced by the family of local maps $(F_0, \ldots, F_{h-1})$ over $\mathbb{F}_p^n$ is defined as

$$\mathcal{S}(x_0, x_1, \ldots, x_{n-1}) = y_0 || y_1 || \ldots || y_{n-1} \qquad \text{where}$$
$$y_i := F_{i \bmod h}(x_i, x_{i+1}, \ldots, x_{i+m-1})$$

for each $i \in \{0, 1, \ldots, n-1\}$, where the sub-indices are taken modulo n.

Our Contribution

Multiple Local Maps

We analyzed the possibility to set up invertible quadratic functions over $\mathbb{F}_p^n$ via shift-invariant functions induced by multiple local maps.
The general scheme is

Definition[Cyclic (Alternating) Shift-Invariant Lifting]

Let $p \geq 3$ be a prime integer and let $1 \leq m, h \leq n$. For each $i \in \{0, 1, \ldots, h-1\}$, let $F_i : \mathbb{F}_p^m \to \mathbb{F}_p$ be a local map. The *cyclic (or alternating) shift-invariant lifting* (CSI-lifting or ASI-lifting) function $\mathcal{S}_{F_0, F_1, \ldots, F_{h-1}}$ induced by the family of local maps $(F_0, \ldots, F_{h-1})$ over $\mathbb{F}_p^n$ is defined as

$$\mathcal{S}(x_0, x_1, \ldots, x_{n-1}) = y_0 \| y_1 \| \ldots \| y_{n-1} \qquad \text{where}$$
$$y_i := F_{i \bmod h}(x_i, x_{i+1}, \ldots, x_{i+m-1})$$

for each $i \in \{0, 1, \ldots, n-1\}$, where the sub-indices are taken modulo n.

Our Contribution

Multiple Local Maps

We analyzed the possibility to set up invertible quadratic functions over $\mathbb{F}_p^n$ via shift-invariant functions induced by multiple local maps.
The general scheme is

Definition[Cyclic (Alternating) Shift-Invariant Lifting]

Let $p \geq 3$ be a prime integer and let $1 \leq m, h \leq n$. For each $i \in \{0, 1, \ldots, h-1\}$, let $F_i : \mathbb{F}_p^m \to \mathbb{F}_p$ be a local map. The *cyclic (or alternating) shift-invariant lifting* (CSI-lifting or ASI-lifting) function $\mathcal{S}_{F_0, F_1, \ldots, F_{h-1}}$ induced by the family of local maps $(F_0, \ldots, F_{h-1})$ over $\mathbb{F}_p^n$ is defined as

$$\mathcal{S}(x_0, x_1, \ldots, x_{n-1}) = y_0 \| y_1 \| \ldots \| y_{n-1} \qquad \text{where}$$
$$y_i := F_{i \bmod h}(x_i, x_{i+1}, \ldots, x_{i+m-1})$$

for each $i \in \{0, 1, \ldots, n-1\}$, where the sub-indices are taken modulo n.

We limited ourselves to consider the case $h = 2$ (ASI), i.e., functions $\mathcal{S}_{F_0,F_1}(x_0, x_1, \dots, x_{n-1}) = y_0 \| y_1 \| \dots \| y_{n-1}$ where

$$y_i = \begin{cases} F_0(x_i, x_{i+1}, \dots, x_{i+m-1}) & \text{if } i \text{ is even} \\ F_1(x_i, x_{i+1}, \dots, x_{i+m-1}) & \text{if } i \text{ is odd} \end{cases} \quad (1)$$

for each $i \in \{0, 1, \dots, n-1\}$, where the sub-indices of x_i are taken modulo n.

Notation

We denote with $\alpha_{i_0,i_1;j}$ the coefficient of the monomial of degree i_0 in x_0 and i_1 in x_1 of F_j with $j \in \{0, 1\}$.

We limited ourselves to consider the case $h = 2$ (ASI), i.e., functions $\mathcal{S}_{F_0,F_1}(x_0, x_1, \ldots, x_{n-1}) = y_0 \| y_1 \| \ldots \| y_{n-1}$ where

$$y_i = \begin{cases} F_0(x_i, x_{i+1}, \ldots, x_{i+m-1}) & \text{if } i \text{ is even} \\ F_1(x_i, x_{i+1}, \ldots, x_{i+m-1}) & \text{if } i \text{ is odd} \end{cases} \tag{1}$$

for each $i \in \{0, 1, \ldots, n-1\}$, where the sub-indices of x_i are taken modulo n.

Notation

We denote with $\alpha_{i_0,i_1;j}$ the coefficient of the monomial of degree i_0 in x_0 and i_1 in x_1 of F_j with $j \in \{0, 1\}$.

Our Contribution

We limited ourselves to consider the case $h = 2$ (ASI), i.e., functions $\mathcal{S}_{F_0,F_1}(x_0, x_1, \ldots, x_{n-1}) = y_0 \| y_1 \| \ldots \| y_{n-1}$ where

$$y_i = \begin{cases} F_0(x_i, x_{i+1}, \ldots, x_{i+m-1}) & \text{if } i \text{ is even} \\ F_1(x_i, x_{i+1}, \ldots, x_{i+m-1}) & \text{if } i \text{ is odd} \end{cases} \tag{1}$$

for each $i \in \{0, 1, \ldots, n-1\}$, where the sub-indices of x_i are taken modulo n.

Notation

We denote with $\alpha_{i_0,i_1;j}$ the coefficient of the monomial of degree i_0 in x_0 and i_1 in x_1 of F_j with $j \in \{0, 1\}$.

Result of Our Study

Our result is the following

Theorem pt.1

Let $p \geq 3$ be a prime integer, and let $n \geq 3$. Let $F_0, F_1 : \mathbb{F}_p^2 \to \mathbb{F}_p$ be two functions. Let $\mathcal{S}_{F_0,F_1} : \mathbb{F}_p^n \to \mathbb{F}_p$ be defined as $\mathcal{S}_{F_0,F_1}(x_0, x_1, \ldots, x_{n-1}) := y_0\|y_1\|\ldots\|y_{n-1}$ where

$$y_i = F_{i \bmod 2}(x_i, x_{i+1}, \ldots, x_{i+m-1}) \qquad \text{for each } i \in \{0, 1, \ldots, n-1\}.$$

Then:

- if F_0 and F_1 are both of degree 2, then $\mathcal{S}_{F_0,F_1}$ is never invertible;
- if F_0 is linear and F_1 is quadratic (or vice-versa), then $\mathcal{S}_{F_0,F_1}$ is invertible for $n \geq 4$ if and only if it is a Feistel Type-II function, e.g.,

$$y_i = \begin{cases} x_{i-1} & \text{if } i \text{ odd} \\ x_{i-1} + x_{i-2}^2 & \text{if } i \text{ even.} \end{cases}$$

Result of Our Study

Our result is the following

Theorem pt.1

Let $p \geq 3$ be a prime integer, and let $n \geq 3$. Let $F_0, F_1 : \mathbb{F}_p^2 \to \mathbb{F}_p$ be two functions. Let $\mathcal{S}_{F_0,F_1} : \mathbb{F}_p^n \to \mathbb{F}_p$ be defined as $\mathcal{S}_{F_0,F_1}(x_0, x_1, \ldots, x_{n-1}) := y_0 \| y_1 \| \ldots \| y_{n-1}$ where

$$y_i = F_{i \bmod 2}(x_i, x_{i+1}, \ldots, x_{i+m-1}) \qquad \text{for each } i \in \{0, 1, \ldots, n-1\}.$$

Then:

- if F_0 and F_1 are both of degree 2, then $\mathcal{S}_{F_0,F_1}$ is never invertible;
- if F_0 is linear and F_1 is quadratic (or vice-versa), then $\mathcal{S}_{F_0,F_1}$ is invertible for $n \geq 4$ if and only if it is a Feistel Type-II function, e.g.,

$$y_i = \begin{cases} x_{i-1} & \text{if } i \text{ odd} \\ x_{i-1} + x_{i-2}^2 & \text{if } i \text{ even.} \end{cases}$$

Our Result

Result of Our Study

Our result is the following

Theorem pt.1

Let $p \geq 3$ be a prime integer, and let $n \geq 3$. Let $F_0, F_1 : \mathbb{F}_p^2 \to \mathbb{F}_p$ be two functions. Let $\mathcal{S}_{F_0,F_1} : \mathbb{F}_p^n \to \mathbb{F}_p$ be defined as $\mathcal{S}_{F_0,F_1}(x_0, x_1, \ldots, x_{n-1}) := y_0 \| y_1 \| \ldots \| y_{n-1}$ where

$$y_i = F_{i \bmod 2}(x_i, x_{i+1}, \ldots, x_{i+m-1}) \qquad \text{for each } i \in \{0, 1, \ldots, n-1\}.$$

Then:

- if F_0 and F_1 are both of degree 2, then $\mathcal{S}_{F_0,F_1}$ is never invertible;
- if F_0 is linear and F_1 is quadratic (or vice-versa), then $\mathcal{S}_{F_0,F_1}$ is invertible for $n \geq 4$ if and only if it is a Feistel Type-II function, e.g.,

$$y_i = \begin{cases} x_{i-1} & \text{if } i \text{ odd} \\ x_{i-1} + x_{i-2}^2 & \text{if } i \text{ even.} \end{cases}$$

Result of Our Study

Our result is the following

Theorem pt.1

Let $p \geq 3$ be a prime integer, and let $n \geq 3$. Let $F_0, F_1 : \mathbb{F}_p^2 \to \mathbb{F}_p$ be two functions. Let $\mathcal{S}_{F_0,F_1} : \mathbb{F}_p^n \to \mathbb{F}_p$ be defined as $\mathcal{S}_{F_0,F_1}(x_0, x_1, \ldots, x_{n-1}) := y_0\|y_1\|\ldots\|y_{n-1}$ where

$$y_i = F_{i \bmod 2}(x_i, x_{i+1}, \ldots, x_{i+m-1}) \qquad \text{for each } i \in \{0, 1, \ldots, n-1\}.$$

Then:

- if F_0 and F_1 are both of degree 2, then $\mathcal{S}_{F_0,F_1}$ is never invertible;
- if F_0 is linear and F_1 is quadratic (or vice-versa), then $\mathcal{S}_{F_0,F_1}$ is invertible for $n \geq 4$ if and only if it is a Feistel Type-II function, e.g.,

$$y_i = \begin{cases} x_{i-1} & \text{if } i \text{ odd} \\ x_{i-1} + x_{i-2}^2 & \text{if } i \text{ even.} \end{cases}$$

Our Result

Theorem pt.2

If $n = 3$, $\mathcal{S}_{F_0,F_1}$ is invertible *also* in the case in which F_0 is a linear function of the form $F_0(x_0, x_1) = \alpha_{1,0;0} \cdot x_0 + \alpha_{0,1;0} \cdot x_1$ with $\alpha_{1,0;0}, \alpha_{0,1;0} \neq 0$, and F_1 is a quadratic function of the form

$F_1(x_0, x_1) = \gamma \cdot \left(\frac{\alpha_{0,1;0}}{\alpha_{1,0;0}} \cdot x_0 - \frac{\alpha_{1,0;0}}{\alpha_{0,1;0}} \cdot x_1 \right)^2 + \alpha_{1,0;1} \cdot x_0 + \alpha_{0,1;1} \cdot x_1$, where $\gamma \in \mathbb{F}_p$ and $\alpha_{1,0;1} \cdot \alpha_{1,0;0}^2 \neq -\alpha_{0,1;1} \cdot \alpha_{0,1;0}^2$.

Our Result

Theorem pt.2

If $n = 3$, $\mathcal{S}_{F_0,F_1}$ is invertible *also* in the case in which F_0 is a linear function of the form $F_0(x_0, x_1) = \alpha_{1,0;0} \cdot x_0 + \alpha_{0,1;0} \cdot x_1$ with $\alpha_{1,0;0}, \alpha_{0,1;0} \neq 0$, and F_1 is a quadratic function of the form
$F_1(x_0, x_1) = \gamma \cdot \left(\frac{\alpha_{0,1;0}}{\alpha_{1,0;0}} \cdot x_0 - \frac{\alpha_{1,0;0}}{\alpha_{0,1;0}} \cdot x_1 \right)^2 + \alpha_{1,0;1} \cdot x_0 + \alpha_{0,1;1} \cdot x_1$, where $\gamma \in \mathbb{F}_p$ and $\alpha_{1,0;1} \cdot \alpha_{1,0;0}^2 \neq -\alpha_{0,1;1} \cdot \alpha_{0,1;0}^2$.

Tools for the Proof

The main tools we used to prove the theorem are the following:

- The shift invariance;
- The concept of *collision*: the proof is by finding collisions

Definition [Collision]

Let $\mathbb{F}$ be a generic field, and let $\mathcal{F}$ be a function defined over $\mathbb{F}^n$ for $n \geq 1$. A pair $x, y \in \mathbb{F}_p^n$ is a collision for $\mathcal{F}$ if and only if $\mathcal{F}(x) = \mathcal{F}(y)$ and $x \neq y$.

- The following lemma

Lemma

Let $p \geq 3$ be a prime integer, and let $n \geq 2$ be an integer. Let $F_0, F_1, \ldots, F_{h-1} : \mathbb{F}_p^2 \to \mathbb{F}_p$ be $1 \leq h \leq n$ quadratic functions. If there exists $l \leq h$ such that the quadratic function F_l depends on a single variable, then the cyclic SI-lifting $\mathcal{S}_{F_0,F_1,\ldots,F_{h-1}}$ defined over $\mathbb{F}_p^n$ for $n \geq 3$ is **not** invertible.

Tools for the Proof

The main tools we used to prove the theorem are the following:

- The shift invariance;
- The concept of *collision*: the proof is by finding collisions

Definition [Collision]

Let $\mathbb{F}$ be a generic field, and let $\mathcal{F}$ be a function defined over $\mathbb{F}^n$ for $n \geq 1$. A pair $x, y \in \mathbb{F}_p^n$ is a collision for $\mathcal{F}$ if and only if $\mathcal{F}(x) = \mathcal{F}(y)$ and $x \neq y$.

- The following lemma

Lemma

Let $p \geq 3$ be a prime integer, and let $n \geq 2$ be an integer. Let $F_0, F_1, \ldots, F_{h-1} : \mathbb{F}_p^2 \to \mathbb{F}_p$ be $1 \leq h \leq n$ quadratic functions. If there exists $l \leq h$ such that the quadratic function F_l depends on a single variable, then the cyclic SI-lifting $\mathcal{S}_{F_0, F_1, \ldots, F_{h-1}}$ defined over $\mathbb{F}_p^n$ for $n \geq 3$ is **not** invertible.

The main tools we used to prove the theorem are the following:

- The shift invariance;
- The concept of *collision*: the proof is by finding collisions

Definition [Collision]

Let $\mathbb{F}$ be a generic field, and let $\mathcal{F}$ be a function defined over $\mathbb{F}^n$ for $n \geq 1$. A pair $x, y \in \mathbb{F}_p^n$ is a collision for $\mathcal{F}$ if and only if $\mathcal{F}(x) = \mathcal{F}(y)$ and $x \neq y$.

- The following lemma

Lemma

Let $p \geq 3$ be a prime integer, and let $n \geq 2$ be an integer. Let $F_0, F_1, \ldots, F_{h-1} : \mathbb{F}_p^2 \to \mathbb{F}_p$ be $1 \leq h \leq n$ quadratic functions. If there exists $l \leq h$ such that the quadratic function F_l depends on a single variable, then the cyclic SI-lifting $\mathcal{S}_{F_0,F_1,\ldots,F_{h-1}}$ defined over $\mathbb{F}_p^n$ for $n \geq 3$ is **not** invertible.

Tools for the Proof

The main tools we used to prove the theorem are the following:

- The shift invariance;
- The concept of *collision*: the proof is by finding collisions

Definition [Collision]

Let $\mathbb{F}$ be a generic field, and let $\mathcal{F}$ be a function defined over $\mathbb{F}^n$ for $n \geq 1$. A pair $x, y \in \mathbb{F}_p^n$ is a collision for $\mathcal{F}$ if and only if $\mathcal{F}(x) = \mathcal{F}(y)$ and $x \neq y$.

- The following lemma

Lemma

Let $p \geq 3$ be a prime integer, and let $n \geq 2$ be an integer. Let $F_0, F_1, \ldots, F_{h-1} : \mathbb{F}_p^2 \rightarrow \mathbb{F}_p$ be $1 \leq h \leq n$ quadratic functions. If there exists $l \leq h$ such that the quadratic function F_l depends on a single variable, then the cyclic SI-lifting $\mathcal{S}_{F_0,F_1,\ldots,F_{h-1}}$ defined over $\mathbb{F}_p^n$ for $n \geq 3$ is **not** invertible.

Tools for the Proof

The main tools we used to prove the theorem are the following:

- The shift invariance;
- The concept of *collision*: the proof is by finding collisions

Definition [Collision]

Let $\mathbb{F}$ be a generic field, and let $\mathcal{F}$ be a function defined over $\mathbb{F}^n$ for $n \geq 1$. A pair $x, y \in \mathbb{F}_p^n$ is a collision for $\mathcal{F}$ if and only if $\mathcal{F}(x) = \mathcal{F}(y)$ and $x \neq y$.

- The following lemma

Lemma

Let $p \geq 3$ be a prime integer, and let $n \geq 2$ be an integer. Let $F_0, F_1, \ldots, F_{h-1} : \mathbb{F}_p^2 \to \mathbb{F}_p$ be $1 \leq h \leq n$ quadratic functions. If there exists $l \leq h$ such that the quadratic function F_l depends on a single variable, then the cyclic SI-lifting $\mathcal{S}_{F_0, F_1, \ldots, F_{h-1}}$ defined over $\mathbb{F}_p^n$ for $n \geq 3$ is **not** invertible.

Proof by finding collisions

Lemma

Consider the case with F_0, F_1 two quadratic functions such that $\alpha_{1,1;0} \neq 0$, $\alpha_{1,1;1} \neq 0$ and $n \geq 4$ even number. Then $\mathcal{S}_{F_0,F_1}$ over $\mathbb{F}_p^n$ is not invertible.

Proof: Inputs $(x_0, x_1, x_2, x_3, \dots x_{n-1})$ and $(y_0, y_1, y_2, y_3, \dots, y_{n-1}) = (x_0, x_1, y_2, x_3, \dots, x_{n-1})$, $y_2 \neq x_2$.

$\implies \mathcal{S}_{F_0,F_1}(x_0, x_1, x_2, x_3, \dots, x_{n-1}) = \mathcal{S}_{F_0,F_1}(x_0, x_1, y_2, x_3, \dots, x_{n-1})$ reduces to the two equations $F_1(x_1, x_2) = F_1(x_1, y_2)$ and $F_0(x_2, x_3) = F_0(y_2, x_3)$.

These two equations are:

$$\alpha_{0,2;1} \cdot d_2 \cdot s_2 + \frac{\alpha_{1,1;1}}{2} \cdot d_2 \cdot s_1 + \alpha_{0,1;1} \cdot d_2 = 0,$$

$$\alpha_{2,0;0} \cdot d_2 \cdot s_2 + \frac{\alpha_{1,1;0}}{2} \cdot d_2 \cdot s_3 + \alpha_{1,0;0} \cdot d_2 = 0,$$

where $d_i = x_i - y_i$ and $s_i = x_i + y_i$.

Proof by finding collisions

Lemma

Consider the case with F_0, F_1 two quadratic functions such that $\alpha_{1,1;0} \neq 0$, $\alpha_{1,1;1} \neq 0$ and $n \geq 4$ even number. Then $\mathcal{S}_{F_0,F_1}$ over $\mathbb{F}_p^n$ is not invertible.

Proof: Inputs $(x_0, x_1, x_2, x_3, \ldots x_{n-1})$ and $(y_0, y_1, y_2, y_3, \ldots, y_{n-1}) = (x_0, x_1, y_2, x_3, \ldots, x_{n-1})$, $y_2 \neq x_2$.

$\implies \mathcal{S}_{F_0,F_1}(x_0, x_1, x_2, x_3, \ldots, x_{n-1}) = \mathcal{S}_{F_0,F_1}(x_0, x_1, y_2, x_3, \ldots, x_{n-1})$ reduces to the two equations $F_1(x_1, x_2) = F_1(x_1, y_2)$ and $F_0(x_2, x_3) = F_0(y_2, x_3)$.

These two equations are:

$$\alpha_{0,2;1} \cdot d_2 \cdot s_2 + \frac{\alpha_{1,1;1}}{2} \cdot d_2 \cdot s_1 + \alpha_{0,1;1} \cdot d_2 = 0,$$

$$\alpha_{2,0;0} \cdot d_2 \cdot s_2 + \frac{\alpha_{1,1;0}}{2} \cdot d_2 \cdot s_3 + \alpha_{1,0;0} \cdot d_2 = 0,$$

where $d_i = x_i - y_i$ and $s_i = x_i + y_i$.

Lemma

Consider the case with F_0, F_1 two quadratic functions such that $\alpha_{1,1;0} \neq 0$, $\alpha_{1,1;1} \neq 0$ and $n \geq 4$ even number. Then $\mathcal{S}_{F_0,F_1}$ over $\mathbb{F}_p^n$ is not invertible.

Proof: Inputs $(x_0, x_1, x_2, x_3, \ldots x_{n-1})$ and $(y_0, y_1, y_2, y_3, \ldots, y_{n-1}) = (x_0, x_1, y_2, x_3, \ldots, x_{n-1})$, $y_2 \neq x_2$.

$\implies \mathcal{S}_{F_0,F_1}(x_0, x_1, x_2, x_3, \ldots, x_{n-1}) = \mathcal{S}_{F_0,F_1}(x_0, x_1, y_2, x_3, \ldots, x_{n-1})$ reduces to the two equations $F_1(x_1, x_2) = F_1(x_1, y_2)$ and $F_0(x_2, x_3) = F_0(y_2, x_3)$.

These two equations are:

$$\alpha_{0,2;1} \cdot d_2 \cdot s_2 + \frac{\alpha_{1,1;1}}{2} \cdot d_2 \cdot s_1 + \alpha_{0,1;1} \cdot d_2 = 0,$$

$$\alpha_{2,0;0} \cdot d_2 \cdot s_2 + \frac{\alpha_{1,1;0}}{2} \cdot d_2 \cdot s_3 + \alpha_{1,0;0} \cdot d_2 = 0,$$

where $d_i = x_i - y_i$ and $s_i = x_i + y_i$.

Proof by finding collisions

Lemma

Consider the case with F_0, F_1 two quadratic functions such that $\alpha_{1,1;0} \neq 0$, $\alpha_{1,1;1} \neq 0$ and $n \geq 4$ even number. Then $\mathcal{S}_{F_0,F_1}$ over $\mathbb{F}_p^n$ is not invertible.

Proof: Inputs $(x_0, x_1, x_2, x_3, \dots x_{n-1})$ and $(y_0, y_1, y_2, y_3, \dots, y_{n-1}) = (x_0, x_1, y_2, x_3, \dots, x_{n-1})$, $y_2 \neq x_2$.

$\implies \mathcal{S}_{F_0,F_1}(x_0, x_1, x_2, x_3, \dots, x_{n-1}) = \mathcal{S}_{F_0,F_1}(x_0, x_1, y_2, x_3, \dots, x_{n-1})$ reduces to the two equations $F_1(x_1, x_2) = F_1(x_1, y_2)$ and $F_0(x_2, x_3) = F_0(y_2, x_3)$.

These two equations are:

$$\alpha_{0,2;1} \cdot d_2 \cdot s_2 + \frac{\alpha_{1,1;1}}{2} \cdot d_2 \cdot s_1 + \alpha_{0,1;1} \cdot d_2 = 0,$$

$$\alpha_{2,0;0} \cdot d_2 \cdot s_2 + \frac{\alpha_{1,1;0}}{2} \cdot d_2 \cdot s_3 + \alpha_{1,0;0} \cdot d_2 = 0,$$

where $d_i = x_i - y_i$ and $s_i = x_i + y_i$.

Proof by finding collisions

Lemma

Consider the case with F_0, F_1 two quadratic functions such that $\alpha_{1,1;0} \neq 0$, $\alpha_{1,1;1} \neq 0$ and $n \geq 4$ even number. Then $\mathcal{S}_{F_0,F_1}$ over $\mathbb{F}_p^n$ is not invertible.

Proof: Inputs $(x_0, x_1, x_2, x_3, \ldots x_{n-1})$ and $(y_0, y_1, y_2, y_3, \ldots, y_{n-1}) = (x_0, x_1, y_2, x_3, \ldots, x_{n-1})$, $y_2 \neq x_2$.

$\implies \mathcal{S}_{F_0,F_1}(x_0, x_1, x_2, x_3, \ldots, x_{n-1}) = \mathcal{S}_{F_0,F_1}(x_0, x_1, y_2, x_3, \ldots, x_{n-1})$ reduces to the two equations $F_1(x_1, x_2) = F_1(x_1, y_2)$ and $F_0(x_2, x_3) = F_0(y_2, x_3)$.

These two equations are:

$$\alpha_{0,2;1} \cdot d_2 \cdot s_2 + \frac{\alpha_{1,1;1}}{2} \cdot d_2 \cdot s_1 + \alpha_{0,1;1} \cdot d_2 = 0,$$

$$\alpha_{2,0;0} \cdot d_2 \cdot s_2 + \frac{\alpha_{1,1;0}}{2} \cdot d_2 \cdot s_3 + \alpha_{1,0;0} \cdot d_2 = 0,$$

where $d_i = x_i - y_i$ and $s_i = x_i + y_i$.

Proof by finding collisions

Since $d_2 \neq 0$, the system can be written as

$$\begin{pmatrix} \frac{\alpha_{1,1;1}}{2} & 0 \\ 0 & \frac{\alpha_{1,1;0}}{2} \end{pmatrix} \times \begin{pmatrix} s_1 \\ s_3 \end{pmatrix} = - \begin{pmatrix} \alpha_{0,2;1} \cdot s_2 + \alpha_{0,1;1} \\ \alpha_{2,0;0} \cdot s_2 + \alpha_{1,0;0} \end{pmatrix}.$$

We can see that the determinant is never zero in this case, so the system is compatible. But this means that there is a collision. □

Proof by finding collisions

Since $d_2 \neq 0$, the system can be written as

$$\begin{pmatrix} \frac{\alpha_{1,1;1}}{2} & 0 \\ 0 & \frac{\alpha_{1,1;0}}{2} \end{pmatrix} \times \begin{pmatrix} s_1 \\ s_3 \end{pmatrix} = - \begin{pmatrix} \alpha_{0,2;1} \cdot s_2 + \alpha_{0,1;1} \\ \alpha_{2,0;0} \cdot s_2 + \alpha_{1,0;0} \end{pmatrix}.$$

We can see that the determinant is never zero in this case, so the system is compatible. But this means that there is a collision. □

Proof by finding collisions

Since $d_2 \neq 0$, the system can be written as

$$\begin{pmatrix} \frac{\alpha_{1,1;1}}{2} & 0 \\ 0 & \frac{\alpha_{1,1;0}}{2} \end{pmatrix} \times \begin{pmatrix} s_1 \\ s_3 \end{pmatrix} = - \begin{pmatrix} \alpha_{0,2;1} \cdot s_2 + \alpha_{0,1;1} \\ \alpha_{2,0;0} \cdot s_2 + \alpha_{1,0;0} \end{pmatrix}.$$

We can see that the determinant is never zero in this case, so the system is compatible. But this means that there is a collision. □

Considerations

- Due to the definition of the ASI-lifting, we needed to prove separately the case with n even and n odd, because if n is odd, the numbers of the repetitions of F_0 and F_1 are different;
- CAREFUL: When n is odd, we considered both the cases with F_0 linear and F_1 quadratic and vice versa, because these cases are NOT equivalent
- We have basically an impossibility result, with few exceptions: if we relax the conditions over the two functions to a linear one and a quadratic one, we get
  1. for $n \geq 4$ the already known Type-II Feistel schemes;
  2. for $n = 3$ and if F_0 is the linear function, one more type of invertible ASI-lifting.

Considerations

Considerations

- Due to the definition of the ASI-lifting, we needed to prove separately the case with n even and n odd, because if n is odd, the numbers of the repetitions of F_0 and F_1 are different;
- CAREFUL: When n is odd, we considered both the cases with F_0 linear and F_1 quadratic and vice versa, because these cases are NOT equivalent
- We have basically an impossibility result, with few exceptions: if we relax the conditions over the two functions to a linear one and a quadratic one, we get
  1. for $n \geq 4$ the already known Type-II Feistel schemes;
  2. for $n = 3$ and if F_0 is the linear function, one more type of invertible ASI-lifting.

Considerations

- Due to the definition of the ASI-lifting, we needed to prove separately the case with n even and n odd, because if n is odd, the numbers of the repetitions of F_0 and F_1 are different;
- CAREFUL: When n is odd, we considered both the cases with F_0 linear and F_1 quadratic and vice versa, because these cases are NOT equivalent
- We have basically an impossibility result, with few exceptions: if we relax the conditions over the two functions to a linear one and a quadratic one, we get
  1. for $n \geq 4$ the already known Type-II Feistel schemes;
  2. for $n = 3$ and if F_0 is the linear function, one more type of invertible ASI-lifting.

Considerations

- Due to the definition of the ASI-lifting, we needed to prove separately the case with n even and n odd, because if n is odd, the numbers of the repetitions of F_0 and F_1 are different;
- CAREFUL: When n is odd, we considered both the cases with F_0 linear and F_1 quadratic and vice versa, because these cases are NOT equivalent
- We have basically an impossibility result, with few exceptions: if we relax the conditions over the two functions to a linear one and a quadratic one, we get
  1. for $n \geq 4$ the already known Type-II Feistel schemes;
  2. for $n = 3$ and if F_0 is the linear function, one more type of invertible ASI-lifting.

Considerations

- Due to the definition of the ASI-lifting, we needed to prove separately the case with n even and n odd, because if n is odd, the numbers of the repetitions of F_0 and F_1 are different;
- CAREFUL: When n is odd, we considered both the cases with F_0 linear and F_1 quadratic and vice versa, because these cases are NOT equivalent
- We have basically an impossibility result, with few exceptions:
  if we relax the conditions over the two functions to a linear one and a quadratic one, we get
  1. for $n \geq 4$ the already known Type-II Feistel schemes;
  2. for $n = 3$ and if F_0 is the linear function, one more type of invertible ASI-lifting.

Possible Generalizations

There are two main ways in which this work can be generalized:

- by considering local maps $F_0, F_1, \ldots, F_{h-1} : \mathbb{F}_p^m \to \mathbb{F}_p$ defined over a larger input domain by taking $m \geq 3$;
- In the current definition, the function F takes in input consecutive elements $x_i, x_{i+1}, \ldots, x_{i+m-1}$. A possible way to generalize such definition consists of allowing for non-consecutive inputs.

Possible Generalizations

There are two main ways in which this work can be generalized:

- by considering local maps $F_0, F_1, \ldots, F_{h-1} : \mathbb{F}_p^m \to \mathbb{F}_p$ defined over a larger input domain by taking $m \geq 3$;
- In the current definition, the function F takes in input consecutive elements $x_i, x_{i+1}, \ldots, x_{i+m-1}$. A possible way to generalize such definition consists of allowing for non-consecutive inputs.

Possible Generalizations

There are two main ways in which this work can be generalized:

- by considering local maps $F_0, F_1, \ldots, F_{h-1} : \mathbb{F}_p^m \to \mathbb{F}_p$ defined over a larger input domain by taking $m \geq 3$;
- In the current definition, the function F takes in input consecutive elements $x_i, x_{i+1}, \ldots, x_{i+m-1}$. A possible way to generalize such definition consists of allowing for non-consecutive inputs.

Possible Generalizations

There are two main ways in which this work can be generalized:

- by considering local maps $F_0, F_1, \ldots, F_{h-1} : \mathbb{F}_p^m \to \mathbb{F}_p$ defined over a larger input domain by taking $m \geq 3$;
- In the current definition, the function F takes in input consecutive elements $x_i, x_{i+1}, \ldots, x_{i+m-1}$. A possible way to generalize such definition consists of allowing for non-consecutive inputs.

References

J. Daemen
Cipher and Hash Function Design, Strategies Based on Linear and Differential Cryptanalysis
PhD Thesis. K.U.Leuven (1995), http//jda.noekeon.org/

L. Grassi, S. Onofri, M. Pedicini, L. Sozzi
Invertible Quadratic Non-Linear Layers for MPC-/FHE-/ZK-Friendly Schemes over $\mathbb{F}_p^n$ - Application to Poseidon
IACR Trans. Symmetric Cryptol. 2022(3), 20-72 (2022)

K. Nyberg
Generalized Feistel networks
Advances in Cryptology - ASIACRYPT '96. Springer (1996)

S. Wolfram
Cryptography with Cellular Automata
Advances in Cryptology - CRYPTO '85 Proceedings. Springer (1996)

Y. Zheng, T. Matsumoto, H. Imai
On the Construction of Block Ciphers Provably Secure and Not Relying on Any Unproved Hypotheses
Advances in Cryptology - CRYPTO '89. LNCS, vol. 435, pp. 461–480 (1989)

Thanks

Thank you for your attention!!!